



**Installation and Upgrade Guide
for
OmniVista 2500 NMS
Version 4.9R2**

May 2025

Revision B

Part Number 060957-00

READ THIS DOCUMENT

OmniVista 2500 NMS

for

VMware ESXi: 6.5, 6.7, 7.0.2, 8.0

MS Hyper-V: 2012 R2, 2016, 2019, 2022

**MS Hyper-V on Windows 10
Professional**

Linux KVM/Ubuntu 22.04

ALE USA Inc.
2000 Corporate Center Drive
Thousand Oaks, CA 91320
+1 (818) 880-3500

Table of Contents

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide	1
Installing OmniVista 2500 NMS 4.9R2	3
Required Minimum System Configurations	4
Standalone and High-Availability Installations	6
Deploying OmniVista on a Virtual Appliance.....	6
Deploying the Virtual Appliance on VMware ESXi	6
Deploying the Virtual Appliance on Hyper-V	14
Deploying the Virtual Appliance on Linux KVM/Ubuntu 22.04	19
Completing the OmniVista Installation	29
Converting to a High-Availability Installation	35
Layer 2 Configuration.....	38
Converting Node 1 to Cluster Mode.....	38
Joining Node 2 to the Cluster.....	44
Verifying the Conversion	46
Logging into the OmniVista UI	47
Layer 3 Configuration.....	48
Converting Node 1 to Cluster Mode.....	48
Joining Node 2 to the Cluster.....	51
Verifying the Conversion	53
Logging into the OmniVista UI	54
Upgrading from 4.9R1 to 4.9R2	55
Upgrading from 4.9R1 Standalone to 4.9R2 Standalone.....	55
Launching the OmniVista UI	60
Upgrading from 4.9R1 HA to 4.9R2 HA	61
L2 High-Availability Upgrade Workflow	62
Launching the OmniVista UI	77
L3 High-Availability Upgrade Workflow	77
Launching the OmniVista UI	94
Upgrading from 4.8R2 to 4.9R1	95
Upgrading from 4.8R2 Standalone to 4.9R1 Standalone.....	95
Launching the OmniVista UI	100
Upgrading from 4.8R2 HA to 4.9R1 HA	100
High-Availability Upgrade Workflow	101
Launching the OmniVista UI	115
Upgrading from 4.8R1 to 4.8R2	116
Upgrading from 4.8R1 Standalone to 4.8R2 Standalone.....	116
Launching the OmniVista UI	121
Upgrading from 4.8R1 HA to 4.8R2 HA	122
High-Availability Upgrade Workflow	123
Launching the OmniVista UI	137
Upgrading from 4.7R1 to 4.7R1 Patch 2 to 4.8R1.....	138
Upgrading from 4.7R1 Standalone to 4.7R1 Patch 2 Standalone to 4.8R1 Standalone ...	138
Standalone Upgrade Workflow	139
Launching the OmniVista UI	148
Upgrading from 4.7R1 HA to 4.7R1 Patch 2 to 4.8R1 HA.....	148
High-Availability Upgrade Workflow	149
Launching the OmniVista UI	171
Upgrading from 4.6R2 to 4.7R1	172

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Upgrading from 4.6R2 Standalone to 4.7R1 Standalone	172
Launching the OmniVista UI	177
Upgrading from 4.6R2 HA to 4.7R1 HA	178
High-Availability Upgrade Workflow	179
Launching the OmniVista UI	189
Upgrading from 4.6R1 to 4.6R2	190
Upgrading from 4.6R1 Standalone to 4.6R2 Standalone	190
Launching the OmniVista UI	195
Upgrading from 4.6R1 HA to 4.6R2 HA	195
High-Availability Upgrade Workflow	197
Launching the OmniVista UI	207
Upgrading from 4.5R3 to 4.6R1	207
Upgrading from 4.5R3 Standalone to 4.6R1 Standalone	207
Launching the OmniVista UI	212
Upgrading from 4.5R3 HA to 4.6R1 HA	212
High-Availability Upgrade Workflow	213
Launching the OmniVista UI	224
Upgrading from 4.5R2 to 4.5R3	224
Upgrading from 4.5R2 Standalone to 4.5R3 Standalone	224
Launching the OmniVista UI	229
Upgrading from 4.5R2 HA to 4.5R3HA	229
High-Availability Upgrade Workflow	230
Launching the OmniVista UI	241
Upgrading from 4.5R1 to 4.5R2	241
Upgrading from 4.5R1 Standalone to 4.5R2 Standalone	241
Launching the OmniVista UI	246
Upgrading from 4.5R1 HA to 4.5R2 HA	247
High-Availability Upgrade Workflow	248
Launching the OmniVista UI	266
Appendix A – Using the Virtual Appliance Menu	1
Help	2
Configure the Virtual Appliance	2
Help	3
Display Current Configuration	3
Configure IPs and Ports	3
Configure Default Gateway	5
Configure Hostname	5
Configure DNS Server	6
Configure Timezone	6
Configure Route	7
Configure Network Size	8
Configure Keyboard Layout	9
Update OmniVista Web Server SSL Certificate	11
Enable/Disable AP SSL Authentication	12
Enable/Disable Admin SSH	12
Configure NTP Client	12
Configure Proxy	13
Change Screen Resolution	13
Configure the Other Network Cards	14
Exit	15

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Run Watchdog Command	15
Upgrade/Backup/Restore VA	16
Change Password	19
Logging	19
Login Authentication Server	20
Power Off	21
Reboot.....	21
Advanced Mode	21
Set Up Optional Tools	22
Convert to Cluster	22
Join Cluster	23
Troubleshoot	23
Log Out	23
Appendix B – Using the HA Virtual Appliance Menu.....	1
Help.....	2
Show OV Cluster Status	2
Configure Cluster	2
Help.....	3
Display Cluster Configuration.....	3
Configure Cluster IP.....	4
Configure Captive Portal Virtual IP	4
Configure Captive Portal Virtual IPv6.....	5
Configure Additional OV Web Virtual IP.....	5
Remove Peer Node From Cluster	5
Configure OV Web Ports.....	6
Configure Portal Web Ports	6
Configure OV SSL Certificate	6
Enable/Disable AP SSL Authentication.....	7
Configure FTP Password	7
Configure Login Authentication Server	7
Preferred Active Node.....	8
Manual Failover.....	8
Cluster Error Check.....	8
Configure Peer Node’s Information	9
Enable Maintenance Mode	9
Exit	9
Configure Current Node	9
Help.....	10
Display Current Node Configuration	10
Configure Default Gateway	11
Configure DNS Server	12
Configure Timezone.....	12
Configure Route	13
Configure Keyboard Layout	14
Configure NTP Client	15
Configure Proxy	16
Change Screen Resolution	16
Configure “cliadmin” Password	17
Configure “root” Secret Text.....	17
Enable/Disable Admin SSH	17

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Configure MongoDB Password	17
Configure IPs and Ports	17
Configure Hostname	18
Extend Data Partitions	18
Configure Network Size	20
Troubleshoot	20
Configure Another NIC(s).....	20
Configure “admin” Password for UI	21
Exit	21
Run Watchdog Command	21
Upgrade/Backup/Restore VA	22
Logging	25
Set Up Optional Tools	26
Advanced Mode	26
Power Off	27
Reboot.....	27
Log Out	28
Appendix C – Generating an Evaluation License	1

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

This document details the OmniVista 2500 NMS 4.9R2 (OV 2500 NMS 4.9R2) installation/upgrade process. OV 2500 NMS 4.9R2 can be installed as a [fresh installation](#) from a download file available on the Customer Support website; or you can [upgrade directly from OV 2500 NMS 4.9R1 to 4.9R2](#) using the Virtual Appliance Menu.

Note: If you are using release 4.7R1:

1. Upgrade to the 4.7R1 Patch 2 release.
2. Upgrade to 4.8R1.
3. Upgrade to 4.8R2.
4. Upgrade to 4.9R1. Refer to [Upgrading from 4.8R2 to 4.9R1](#) in this guide for more information.
5. Upgrade to 4.9R2. Refer to [Upgrading from 4.9R1 to 4.9R2](#) in this guide for more information.

The Upgrade Matrix below shows the upgrade paths that must be followed to get to OV 2500 NMS 4.9R2.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Upgrade Matrix for OV 4.9R2

From	To OV 4.9R2
OV4.5R1	Step 1: Automatic Upgrade to 4.5R2 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.5R3 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.6R1 (Standalone/HA) From VA Menu Step 4: Automatic Upgrade to 4.6R2 (Standalone/HA) From VA Menu Step 5: Automatic Upgrade to 4.7R1 (Standalone/HA) From VA Menu Step 6: Automatic Upgrade to 4.7R1 Patch 2 (Standalone/HA) From VA Menu via Custom Repository Step 7: Automatic Upgrade to 4.8R1 (Standalone/HA) From VA Menu Step 8: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 9: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 10: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV4.5R2	Step 1: Automatic Upgrade to 4.5R3 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.6R1 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.6R2 (Standalone/HA) From VA Menu Step 4: Automatic Upgrade to 4.7R1 (Standalone/HA) From VA Menu Step 5: Automatic Upgrade to 4.7R1 Patch 2 (Standalone/HA) From VA Menu via Custom Repository Step 6: Automatic Upgrade to 4.8R1 (Standalone/HA) From VA Menu Step 7: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 8: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 9: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV4.5R3	Step 1: Automatic Upgrade to 4.6R1 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.6R2 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.7R1 (Standalone/HA) From VA Menu Step 4: Automatic Upgrade to 4.7R1 Patch 2 (Standalone/HA) From VA Menu via Custom Repository Step 5: Automatic Upgrade to 4.8R1 (Standalone/HA) From VA Menu Step 6: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 7: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 8: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV4.6R1	Step 1: Automatic Upgrade to 4.6R2 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.7R1 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.7R1 Patch 2 (Standalone/HA) From VA Menu via Custom Repository Step 4: Automatic Upgrade to 4.8R1 (Standalone/HA) From VA Menu Step 5: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 6: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 7: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV 46R2	Step 1: Automatic Upgrade to 4.7R1 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.7R1 Patch 2 (Standalone/HA) From VA Menu via Custom Repository Step 3: Automatic Upgrade to 4.8R1 (Standalone/HA) From VA Menu Step 4: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 5: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 6: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV 4.7R1	Step 1: Automatic Upgrade to 4.7R1 Patch 2 (Standalone/HA) From VA Menu via Custom Repository Step 2: Automatic Upgrade to 4.8R1 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 4: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 5: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV 4.8R1	Step 1: Automatic Upgrade to 4.8R2 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV 4.8R2	Step 1: Automatic Upgrade to 4.9R1 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu
OV 4.9R1	Step 1: Automatic Upgrade to 4.9R2 (Standalone/HA) From VA Menu

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: If your OmniVista is currently running a release older than 4.5R1, the sequential upgrade to the latest OmniVista release will take a very long time. Therefore, it is recommended that you take a backup of your existing OmniVista installation and start with a fresh installation of the latest OmniVista release. After the installation, you will need to add/discover devices and redo the configurations (Profiles, Templates, SSID etc.). It should be quicker. You will lose historical statistics (like traps, statistics etc.). If retaining historical statistics is important, you can export statistics from the old installation.

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

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

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

Note: Never simply power off the VM during any maintenance operation by shutting off the Hypervisor (e.g., hardware upgrade). Always shut down the VM first from the OmniVista Virtual Appliance Menu (Power Off option).

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

Installing OmniVista 2500 NMS 4.9R2

OV 2500 NMS 4.9R2 is distributed as a Virtual Appliance only. There are no other standalone installers (e.g., Windows/Linux). OV 2500 NMS 4.9R2 is installed as a Virtual Appliance, and can be deployed on the following hypervisors:

- VMware ESXi: 6.5, 6.7 and 7.0.2, 8.0
- MS Hyper-V: 2012 R2, 2016, 2019, and 2022
- MS Hyper-V on Windows 10 Professional
- Linux KVM/Ubuntu 22.04.

The sections below detail each of the steps required to deploy OV 2500 NMS 4.9R2 as Virtual Appliance on [VMware](#), [Hyper-V](#), and [Linux KVM/Ubuntu 22.04](#).

Important Note: Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. Insufficient memory or disk space for the chosen network size may cause OV instability. OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 20GB of memory

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to [Required System Configurations](#) for details.

Required Minimum System Configurations

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

Configuration	Network Size*			
	Low	Medium	High	Very High
Total Number of Managed Devices (AOS, Third-Party, and Stellar APs)	500	2,000	5,000**	10,000**
Stellar AP Devices	500	2,000	4,000	4,000
Stellar AP Client Association	50,000	200,000	200,000	200,000
Authenticated UPAM Clients	20,000	50,000	75,000	100,000
Hypervisor Processor	2.4 GHz 8 Logical Processors	2.4 GHz 8 Logical Processors	2.4 GHz 12 Logical Processors	2.4 GHz 12 Logical Processors
Minimum Reserved OmniVista VA RAM for Standalone	20GB	36GB	64GB	64GB
Minimum Reserved OmniVista VA RAM for HA	N/A***	40GB	64GB	64GB
Storage Provisioning****	Partition 1: 50GB (50GB Disk 1) Partition 2: 512GB (512GB Disk 2)	Partition 1: 50GB (50GB Disk 1) Partition 2: 1TB (0.5TB Disk 2 + 0.5TB Additional Disks)	Partition 1: 50GB (50GB Disk 1) Partition 2: 2TB (0.5TB Disk 2 + 1.5TB Additional Disks)	Partition 1: 50GB (50GB Disk 1) Partition 2: 2TB (0.5TB Disk 2 + 1.5TB Additional Disks)
Minimum Storage Read/Write Speed	100 MB/s	150 MB/s	200 MB/s	200 MB/s

*OmniVista allocates memory based on the network size selected during installation.

**If there are 4,000 Stellar APs in a “High” network size, up to 500 AOS switches can be supported. If there are 4,000 Stellar APs in a “Very High” network size, up to 1,000 AOS switches can be supported. If there are 4,000 Stellar APs in an HA “Very High” network size, up to 1500 AOS switches can be supported.

***An HA installation should be done on a “Medium” or higher size VA.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

****Partition can be based on multiple virtual disks. To extend a partition, add new virtual disks from the hypervisor and then use the "Extend Data Partition" option from the OmniVista VA menu. Note that editing the size of existing virtual disks is not supported.

For detailed instructions on extending the data partition on Standalone Installations, see [Configure Network Size](#) (Option 4 – Extend Data Partition). For detailed instructions on extending the data partition on High-Availability Installations, see [Extend Data Partitions](#).

Notes:

- When deploying the OmniVista VA for the first time, do not add the new disks in the hypervisor until after OmniVista is configured and rebooted.
- When provisioning RAM for a new VM for OmniVista, never allocate more memory than is available on the Host Server. For example, if you are running a Host Server with 128GB of memory and have already allocated 96GB of memory to your existing VMs, accounting for the Host Server's own memory use, you are not left with enough memory to run OmniVista without incident. VM RAM is configured from the Hypervisor.
- Allocate the recommended amount of RAM for the OmniVista VM based on your network size as shown in the above table. In addition, it is recommended that you **reserve** that RAM for the OmniVista VM to prevent performance issues.
- Set CPU Shares to "High".
- Do not exceed the number of Logical Processors recommended for your network size as shown in the above table. Hypervisor Processors are configured from the Hypervisor.
 - HDD Provisioning is configured from the VA Menu. By default, OV 2500 NMS 4.8R2 is partitioned as follows: HDD1:50GB and HDD2:512GB. If you are managing more than 500 devices, it is recommended that you go to the Virtual Appliance Menu on the VA to increase the OmniVista disk space. For a **Standalone** Installation, use the "Extend Data Partition" option under [Configure Network Size](#) in the Configure The Virtual Appliance Menu (Configure The Virtual Appliance Menu – Configure Network Size – Extend Data Partition). For a **High-Availability** Installation, use the "[Extend Data Partition](#)" option under Configure Current Node in The HA Virtual Appliance Menu (The HA Virtual Appliance Menu - Configure Current Node - Extend Partitions).
 - OmniVista can be configured to use SNMPv3 to communicate with devices. When editing this configuration, you can specify which algorithms should be used. A recommended algorithm is AES ("Advanced Encryption Standard"). To get the best performance from your hypervisor, we recommend that you use Intel processors with the AES-NI instruction set enabled.
 - AES-NI was introduced by Intel in 2010 in its Westmere family of processors and allows your hypervisor and its VMs to manage AES-related workloads natively. To realize the full benefits of AES-NI, you need to ensure that it is made available to the VM running OmniVista. To do this:
 - Your hypervisor's CPUs must be newer CPUs (> 2010)
 - AES-NI must be enabled in your hypervisor's BIOS
 - The AES-NI feature must not be "masked" by your hypervisor.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- By default, VMWare and Hyper-V are "pass-through" meaning that OmniVista's VM will be able to use AES acceleration.
- The High-Availability Feature supports up to 4,000 devices.

Standalone and High-Availability Installations

OV 2500 NMS 4.9R2 can be installed in a Standalone or High-Availability configuration. A High-Availability Installation consists of two VMs (Node 1 and Node 2), with one node acting as the Active OV Server (Node 1) and the other as a Standby OV Server (Node 2). If Node 1 fails, OmniVista will automatically failover to Node 2.

Deploying OmniVista on a Virtual Appliance

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

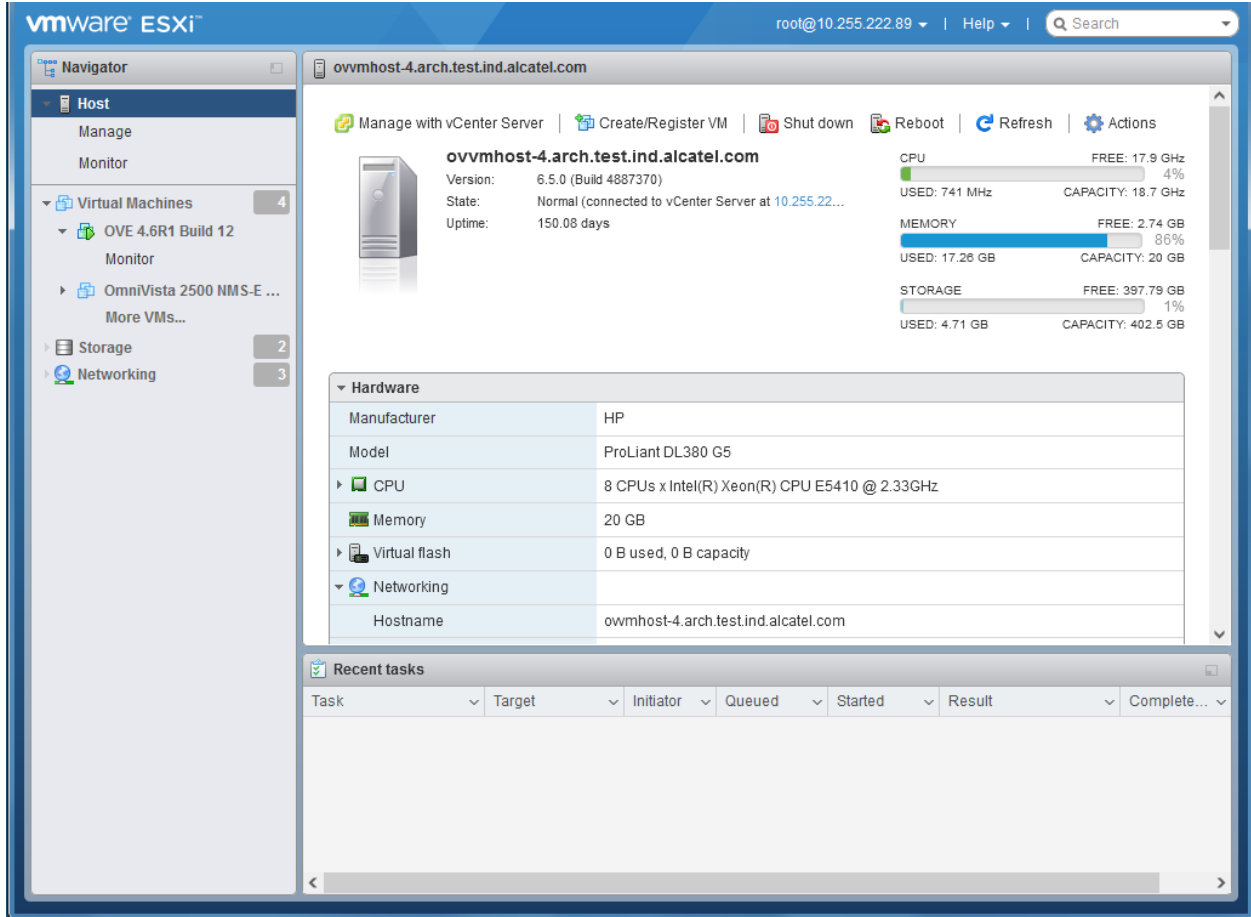
Note: The High-Availability Feature supports up to 4,000 devices.

Deploying the Virtual Appliance on VMware ESXi

Note that in the instructions below, the screens are for demonstration purposes. Some of the screens shown may depict an older OmniVista Release.

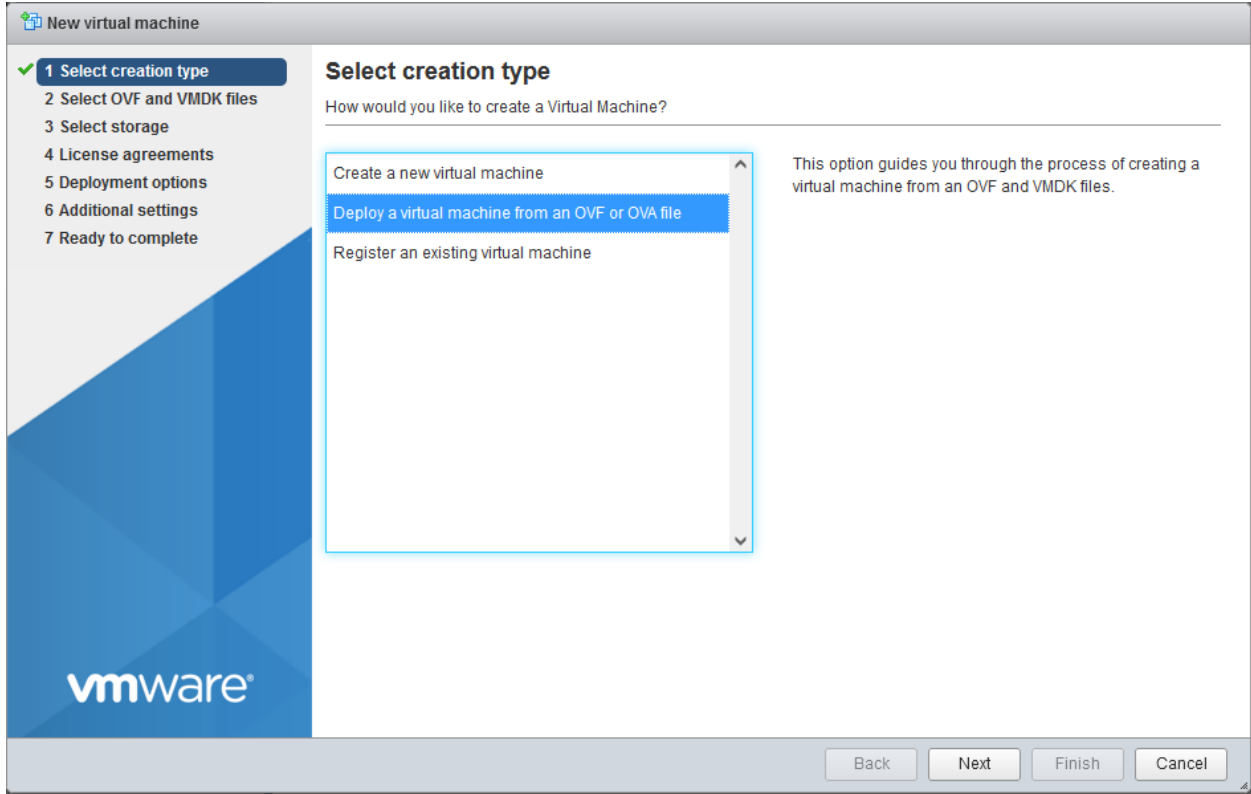
1. Download and unzip the OVF package. You will be using the OVF File and **both** VMDK Files (disk 1 and disk 2) for the installation. **The Zip file also contains an *.mf File. You will not use it and can delete it.**
2. Log into VMware ESXi.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

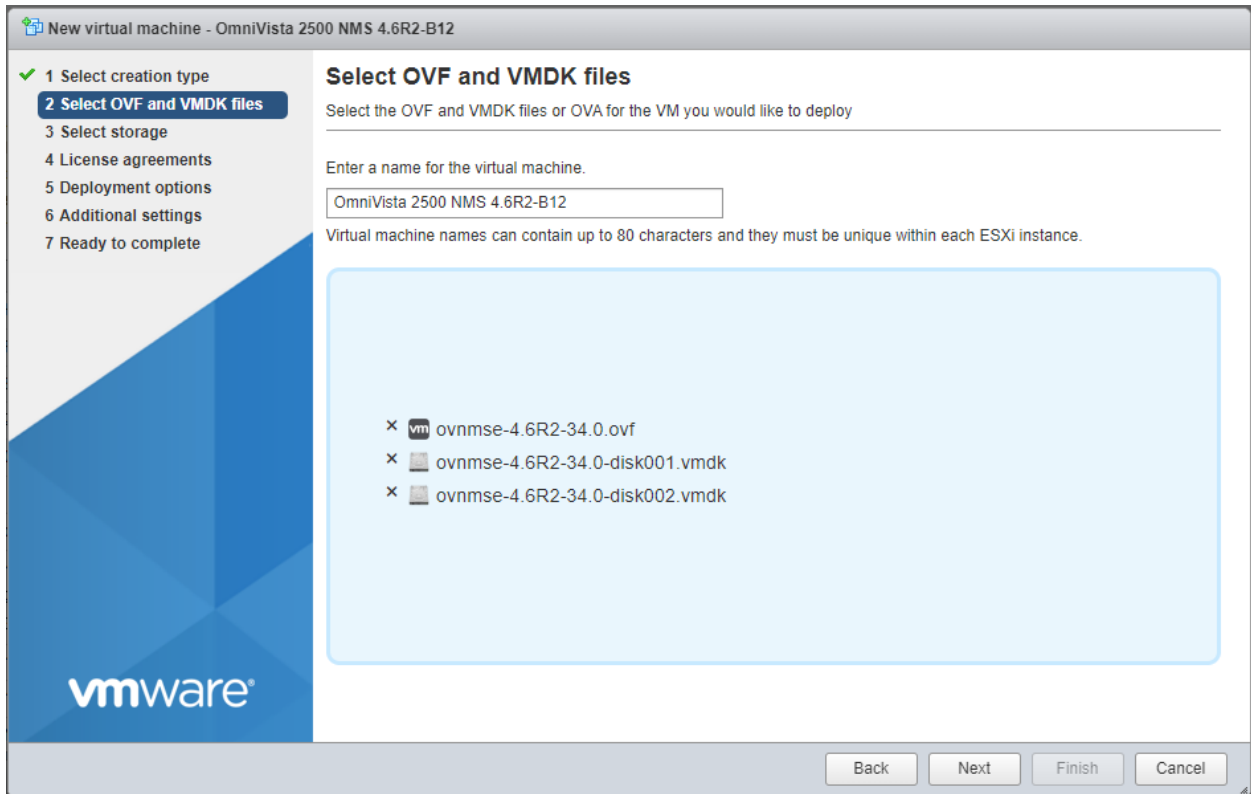


3. Select the Host on which you want to install OV 2500 NMS 4.9R2 and click on **Create/Register VM**. The first screen of the New Virtual Machine Wizard appears.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

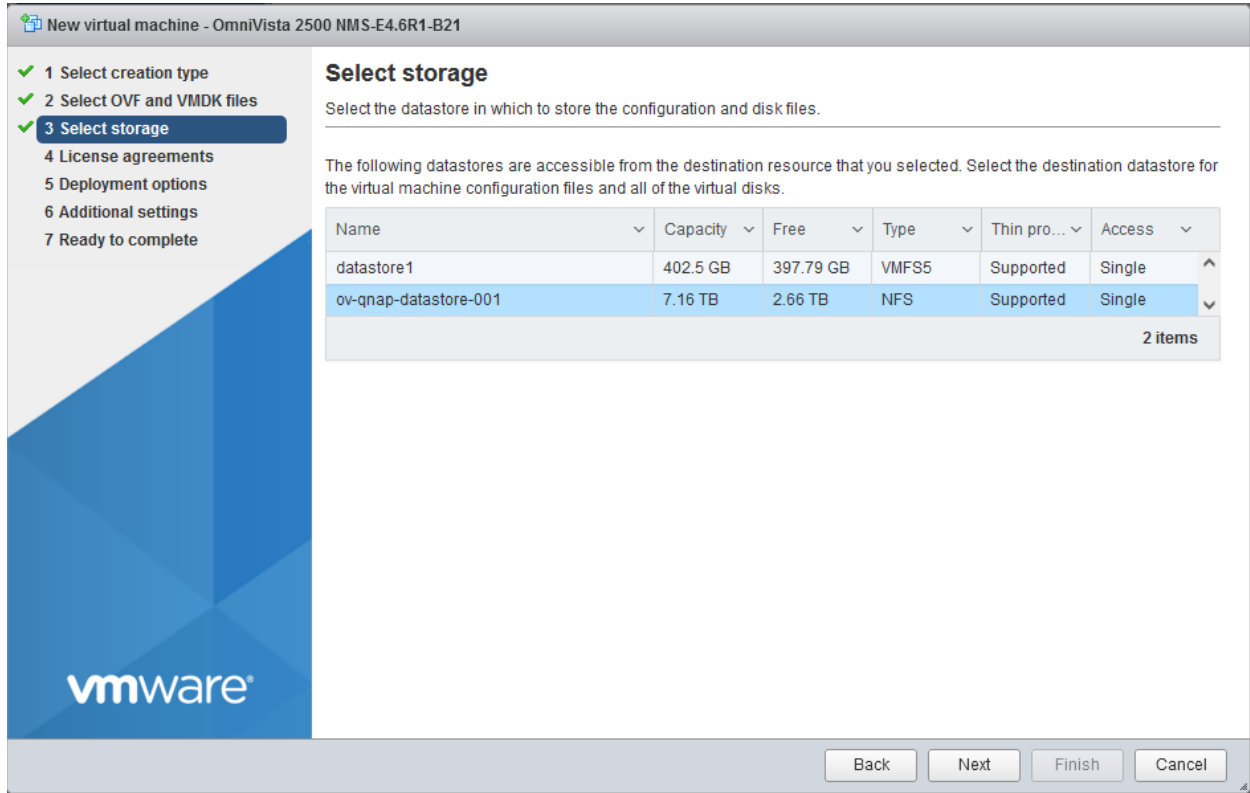


4. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



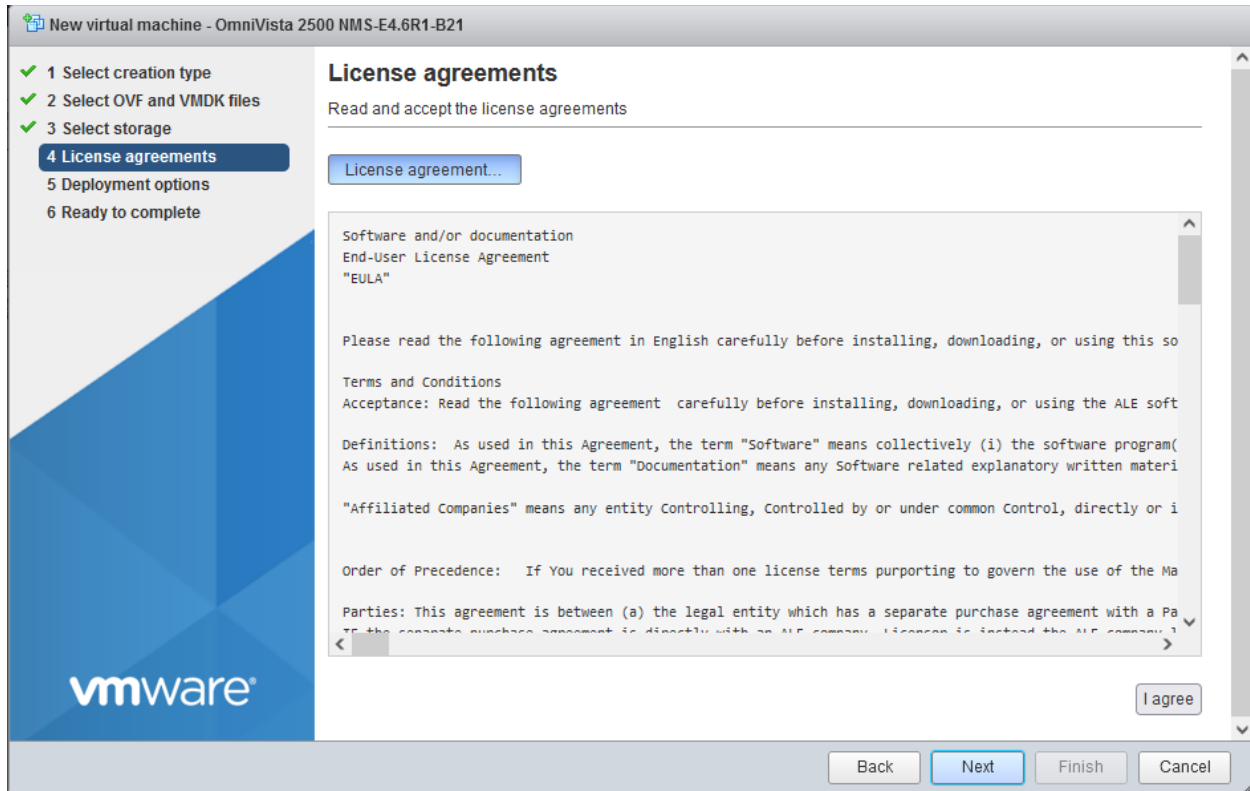
OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

5. Enter a name for the VM (e.g., OmniVista 2500 NMS 4.9R2-GA, click to locate and select the downloaded installation files (or drag the files into the window), then click **Next**. Note that if you plan on configuring a High-Availability installation, you could add Node information to the name (e.g., OmniVista 2500 NMS 4.9R2-GA Node 1) to more easily identify the VM.

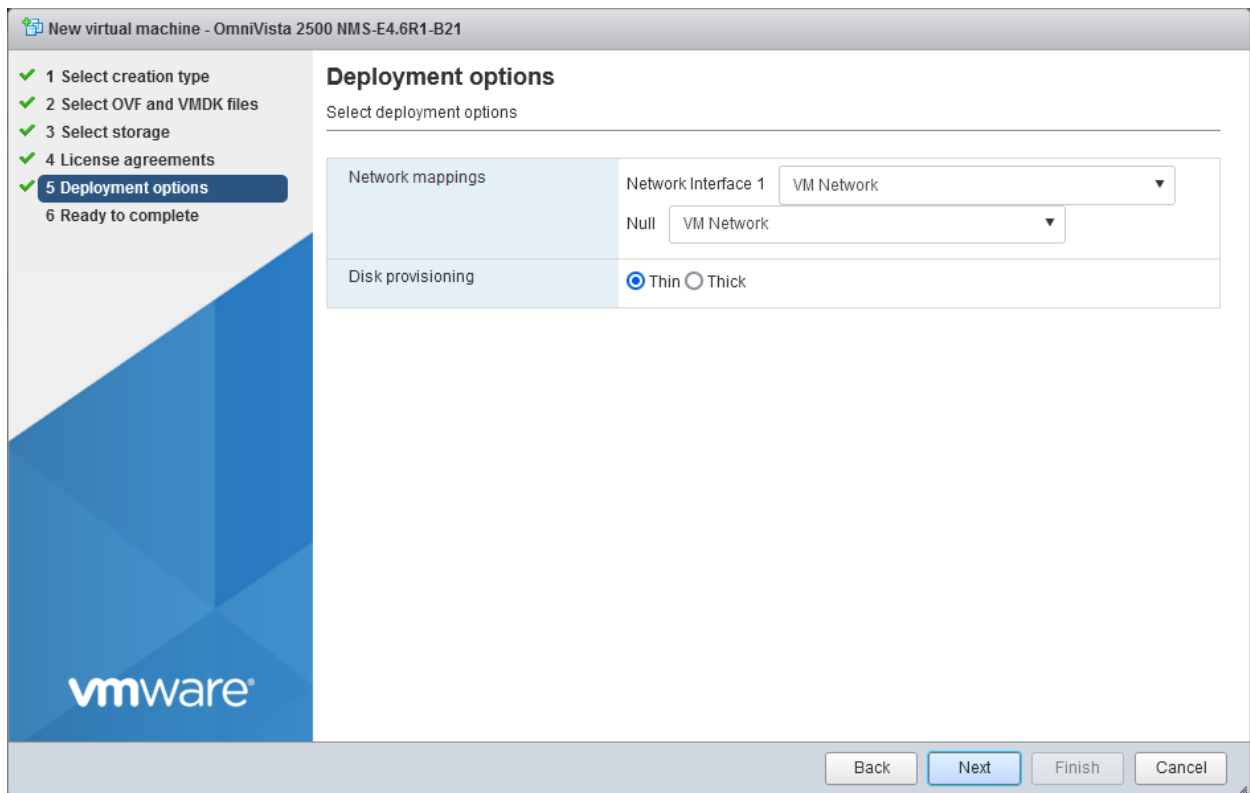


6. Select the destination storage where the template is to be deployed, then click **Next**.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



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




OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

The screenshot shows the 'Ready to complete' step of the 'New virtual machine' wizard. On the left, a progress list shows steps 1 through 6, with '6 Ready to complete' highlighted. The main area contains a table of configuration details and a warning message.

Ready to complete	
Review your settings selection before finishing the wizard	
Product	OmniVista 2500 NMS
VM Name	OmniVista 2500 NMS 4.6R2-B12
Disks	ovnmse-4.6R2-34.0-disk001.vmdk,ovnmse-4.6R2-34.0-disk002.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	Network Interface 1: VM Network, Null: VM Network
Guest OS Name	RedHat_64

 Do not refresh your browser while this VM is being deployed.

At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

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

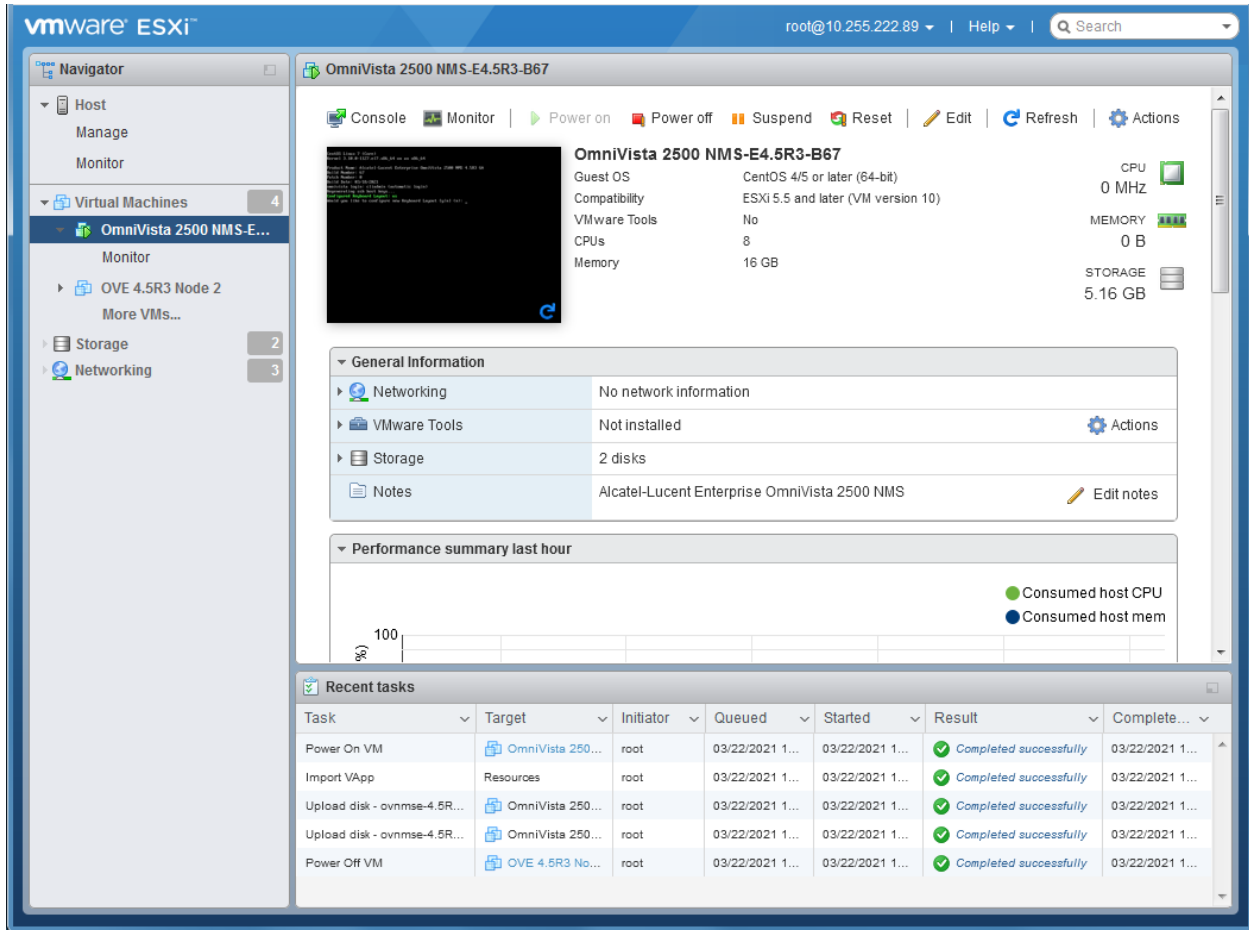
OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

The screenshot displays the VMware ESXi vSphere Client interface. The top navigation bar shows the user is logged in as 'root@10.255.222.89'. The left-hand 'Navigator' pane shows a tree view with 'Host' selected, containing 'Manage' and 'Monitor' options. Under 'Virtual Machines', there are five items, including 'OmniVista 2500 NMS-E...'. The main content area shows the host 'ovmhost-4.arch.test.ind.alcatel.com' with a status of 'Normal (connected to vCenter Server at 10.255.22...)'. Performance metrics are shown: CPU (4% used, 17.9 GHz free), MEMORY (86% used, 2.74 GB free), and STORAGE (1% used, 397.79 GB free). The 'Hardware' section lists: Manufacturer: HP, Model: ProLiant DL380 G5, CPU: 8 CPUs x Intel(R) Xeon(R) CPU E5410 @ 2.33GHz, Memory: 20 GB, Virtual flash: 0 B used, 0 B capacity, and Networking: Hostname: ovmhost-4.arch.test.ind.alcatel.com. The 'Recent tasks' table at the bottom shows the following data:

Task	Target	Initiator	Queued	Started	Result	Complete...
Reconfig VM	OmniVista 25...	VC Internal	06/13/2021 1...	06/13/2021 1...	Failed - The operatio...	06/13/2021 1...
Download VMXConfig	None	VC Internal	06/13/2021 1...	06/13/2021 1...	Completed successfully	06/13/2021 1...
Import VApp	Resources	root	06/13/2021 1...	06/13/2021 1...	Running... 62...	Running... 62...
Upload disk - ovmnse-4.6...	OmniVista 25...	root	06/13/2021 1...	06/13/2021 1...	Running... 83...	Running... 83...
Upload disk - ovmnse-4.6...	OmniVista 25...	root	06/13/2021 1...	06/13/2021 1...	Running... 40...	Running... 40...

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



11. Click on the small Console Screen or click on **Console** at the top of the screen and select **Open Browser Console** to open a Console. Note that it may take several minutes for the deployment to complete. You will see a screen message saying "The Virtual Appliance is being installed. OmniVista will restart automatically after progress is complete". Once the deployment is complete the screen below will appear. Go to [Completing the OmniVista Installation](#) to complete the installation.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 EA
Build Number: 21
Patch Number: 8
Build Date: 06/10/2021
omnivista login: cliadmin (automatic login)
Regenerating ssh host keys...
Configured Keyboard Layout: us
Would you like to configure new Keyboard Layout [yin] (n):
```

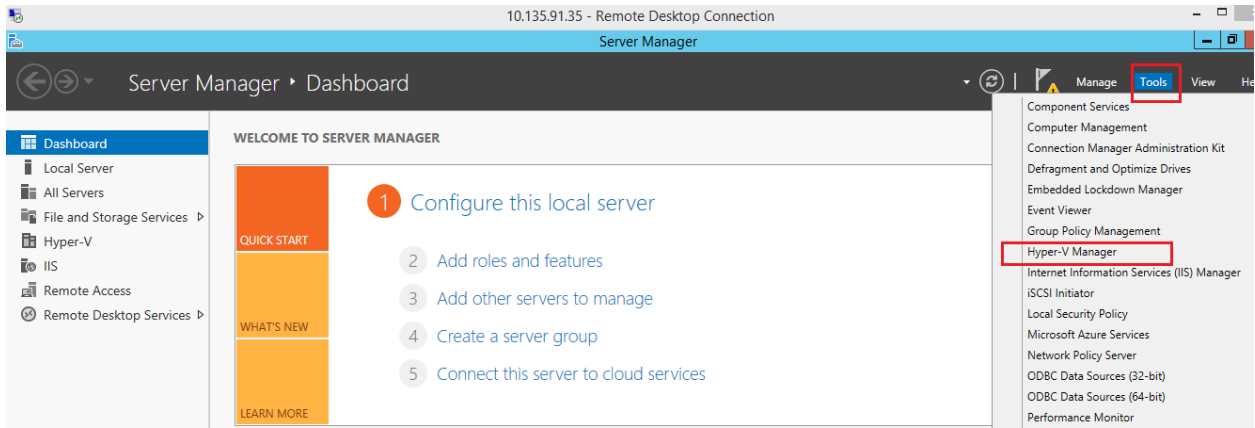
Note: After deploying the OmniVista VM, configure any additional NICs you may need on the VM before [Completing the OmniVista Installation](#).

Deploying the Virtual Appliance on Hyper-V

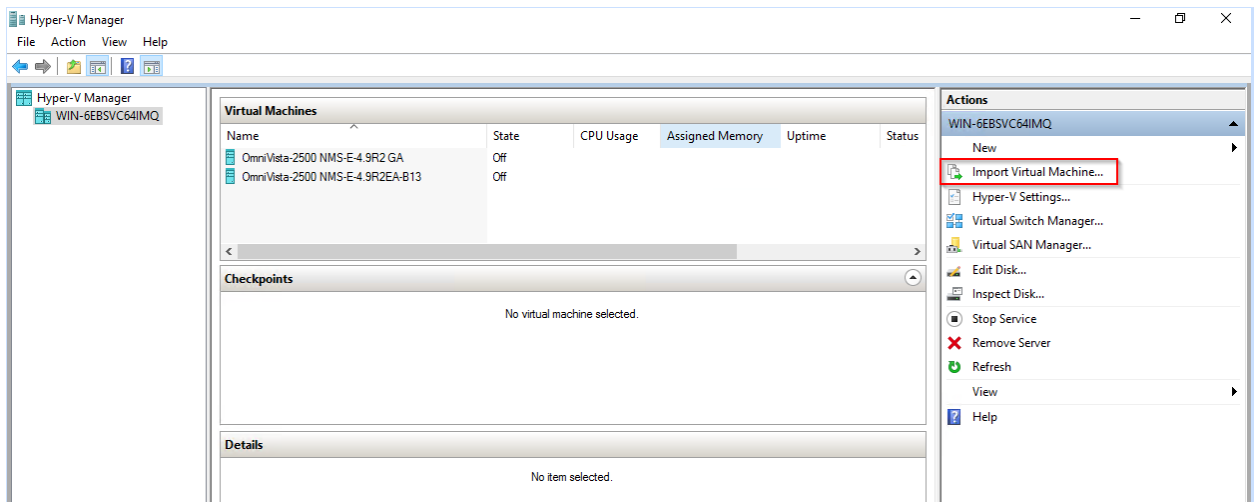
Note that in the instructions below, Hyper-V in Windows 2012 R2 is used for demonstration purposes; and some of the screens shown may depict an older OmniVista Release.

Note: OmniVista does not support Hyper-V Live Migration. Also note that the OmniVista VM Manager application is supported only on Hyper-V 2012, 2012 R2, and 2016; it is not supported on Hyper-V 2019 or higher.

1. Download and unzip the Hyper-V package and select the "hyperv" folder when importing files in Step 5. You will be using the OVF File and **both** VMDK Files (disk 1 and disk 2) for the installation. You will **not** be using the *.mf File.
2. Log into Windows 2012 and open the Hyper-V tool.

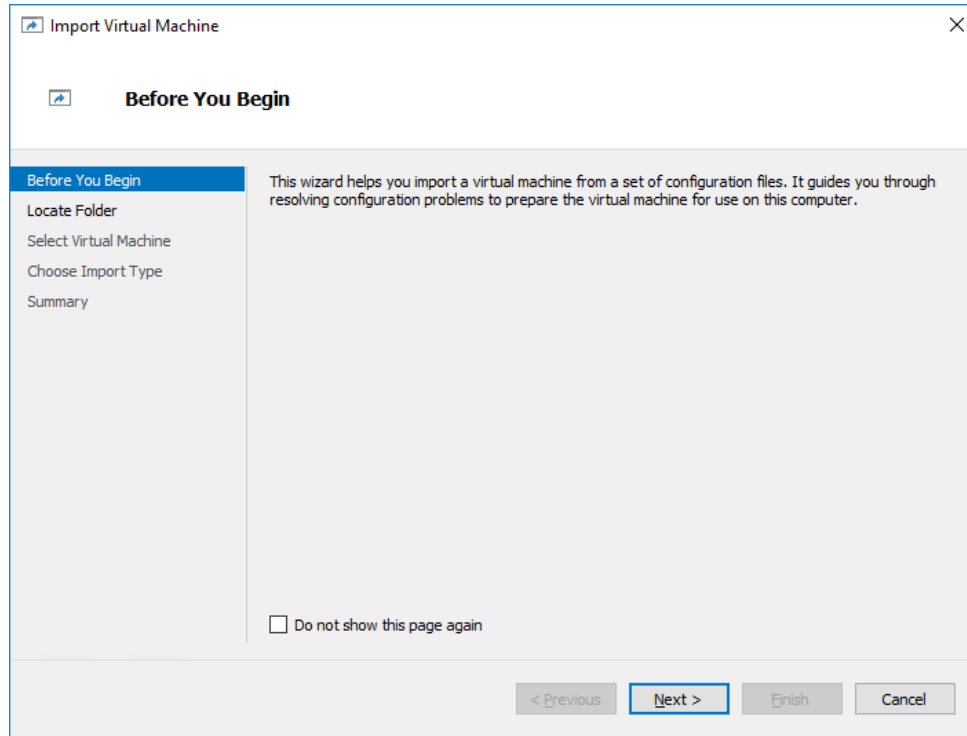


3. Select the Host on which you want to install OmniVista 2500 NMS, click on **Actions > Import Virtual Machine**.

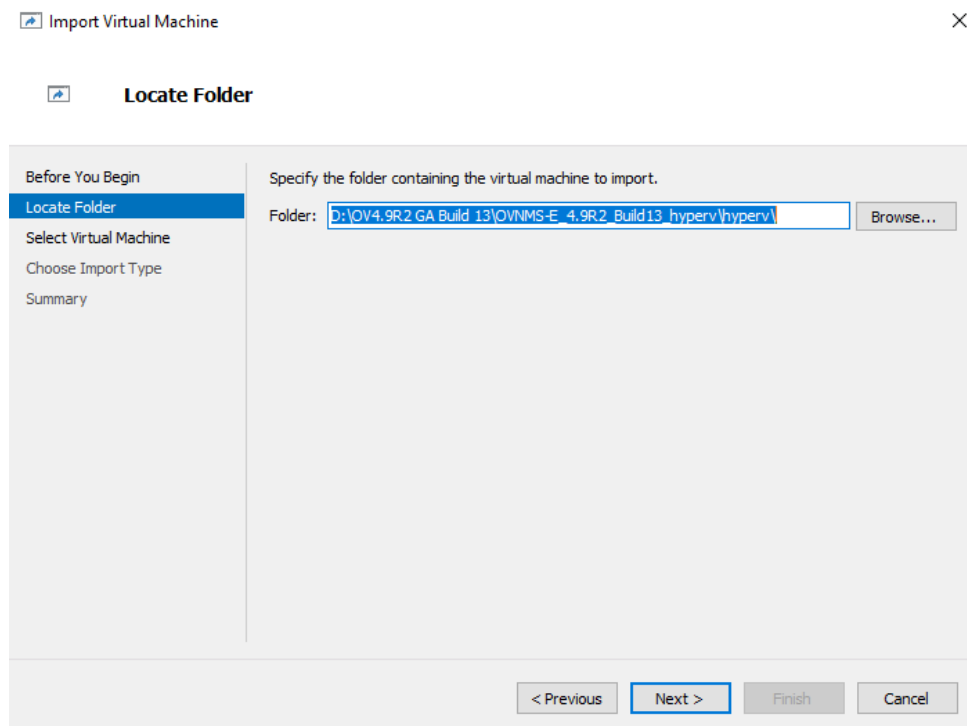


OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

4. The Import Virtual Machine Wizard appears.

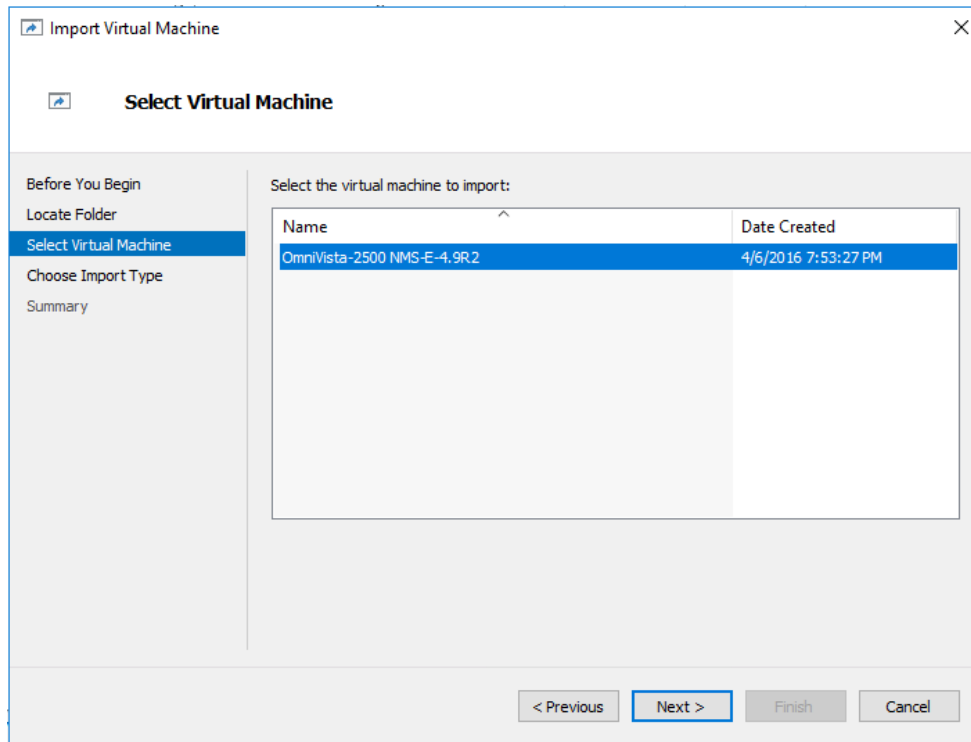


5. Click **Next** to go to the Locate Folder Screen, select the **Folder** that you extracted in Step 1, then click **Next**.

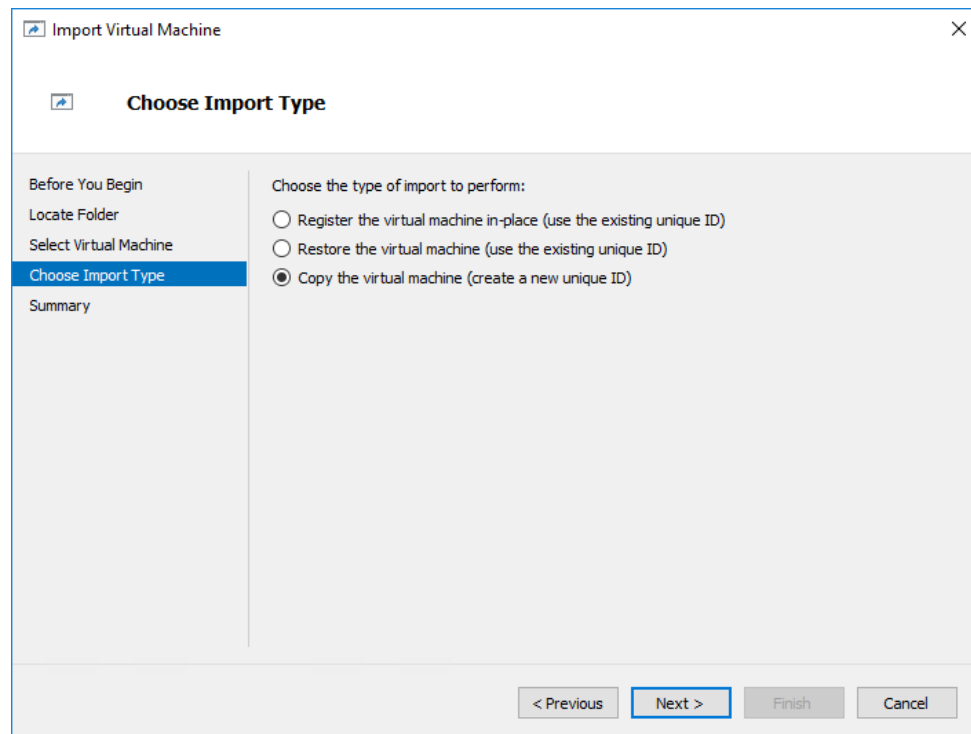


OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

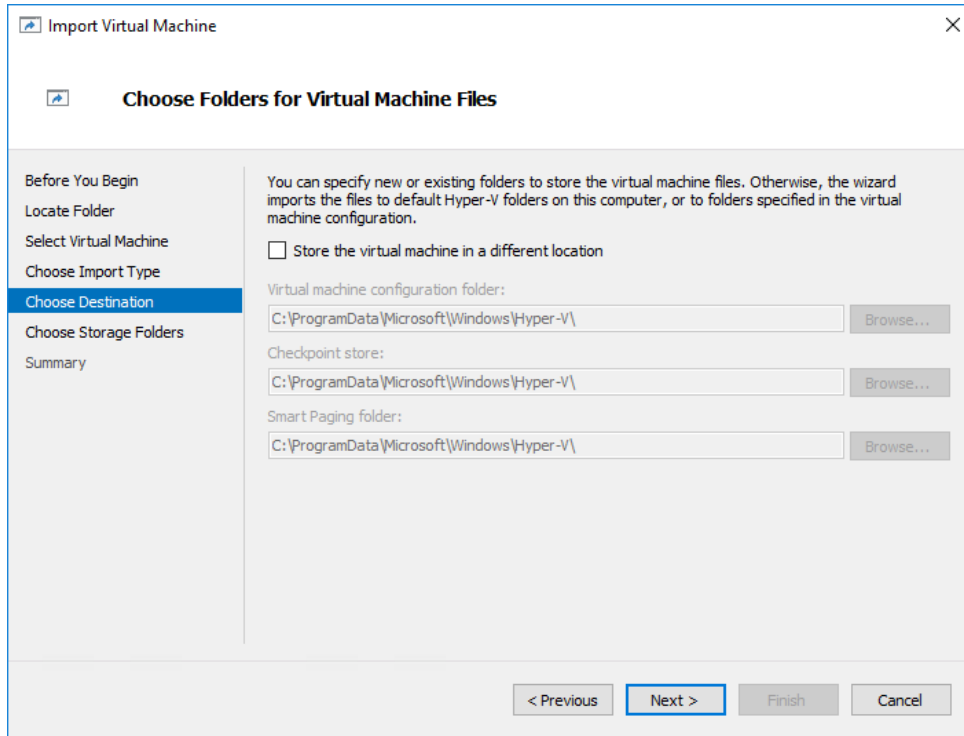


7. Select the Import Type: **Copy the virtual machine (create a new unique ID)**, then click **Next**.

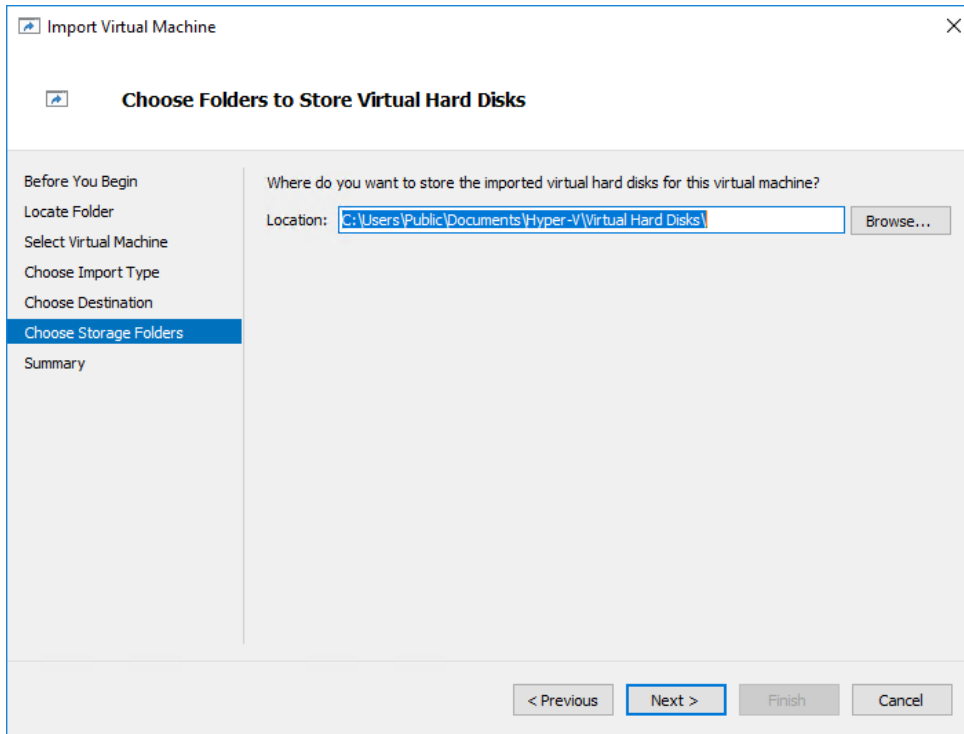


OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

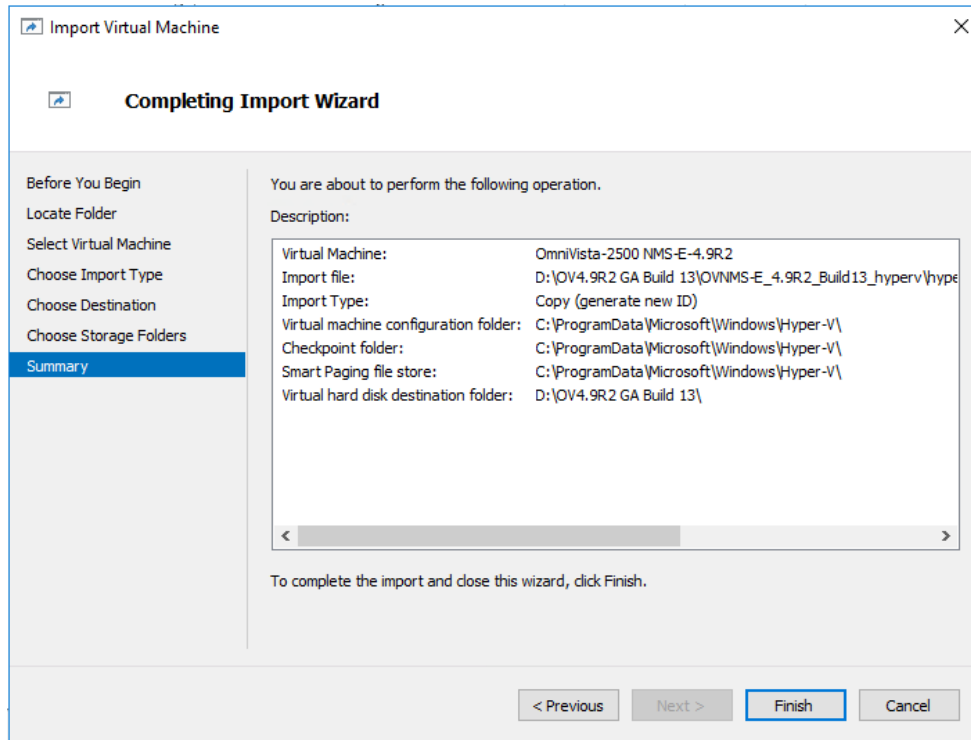


9. Choose folders to store the Virtual Hard Disks or accept the default location and click **Next**.

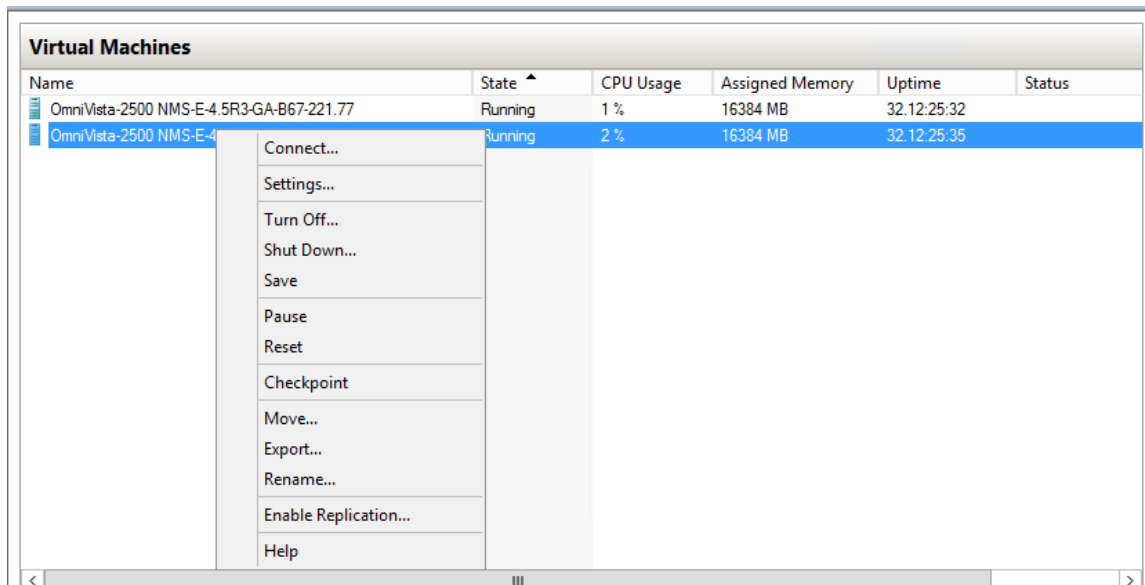


OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

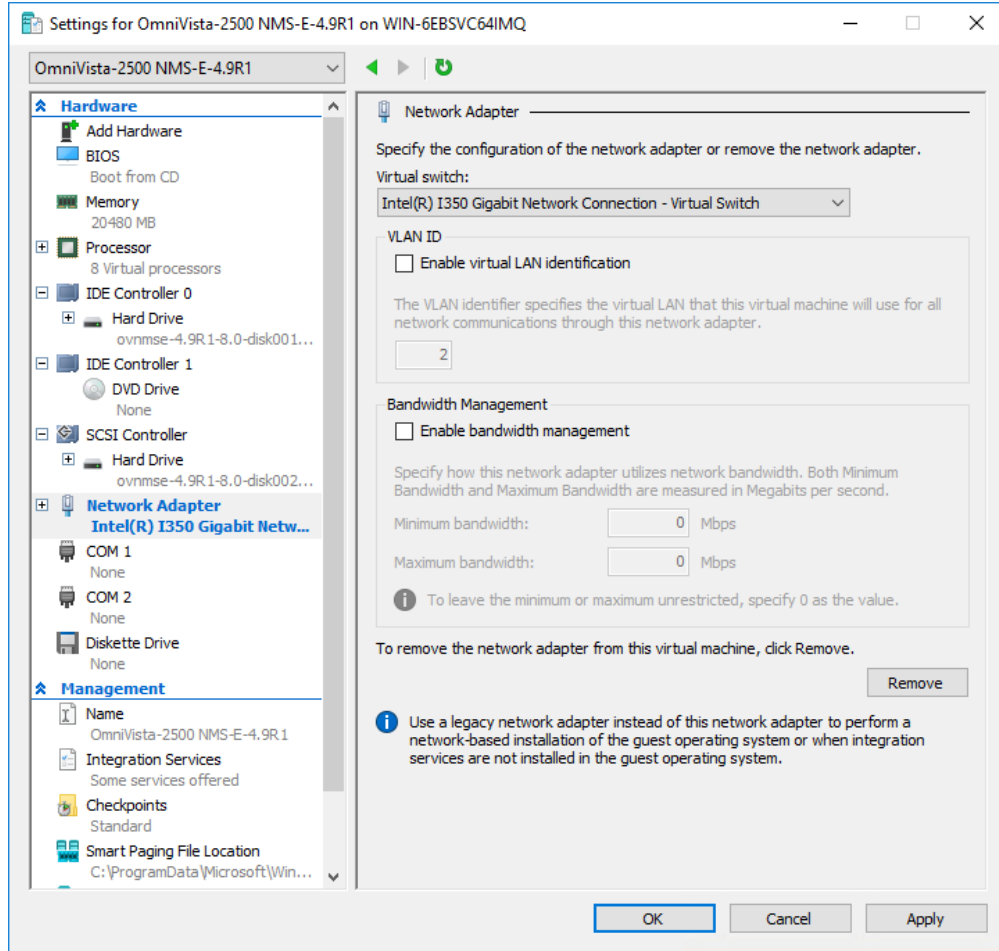


11. Configure the Network Adapter. Right-click on the VA and select **Settings**.



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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



Once the Virtual Appliance is powered on, go to [Completing the OmniVista Installation](#) to complete the installation.

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

Deploying the Virtual Appliance on Linux KVM/Ubuntu 22.04

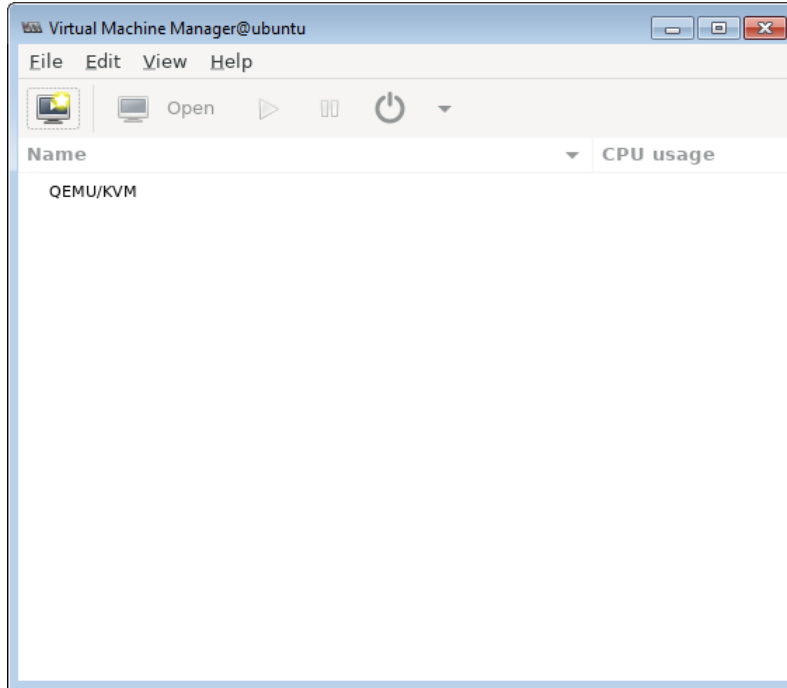
Note that in the instructions below, the screens are for demonstration purposes. Some of the screens shown may depict an older OmniVista Release.

1. Download and unzip the KVM package. You will be using both **qcow2** Files (disk 0001 and disk 0002) for the installation. You will **not** be using the *.mf File.
2. Log into the Linux machine on which you are deploying the VA and launch the Virtual Machine Manager, as shown below.

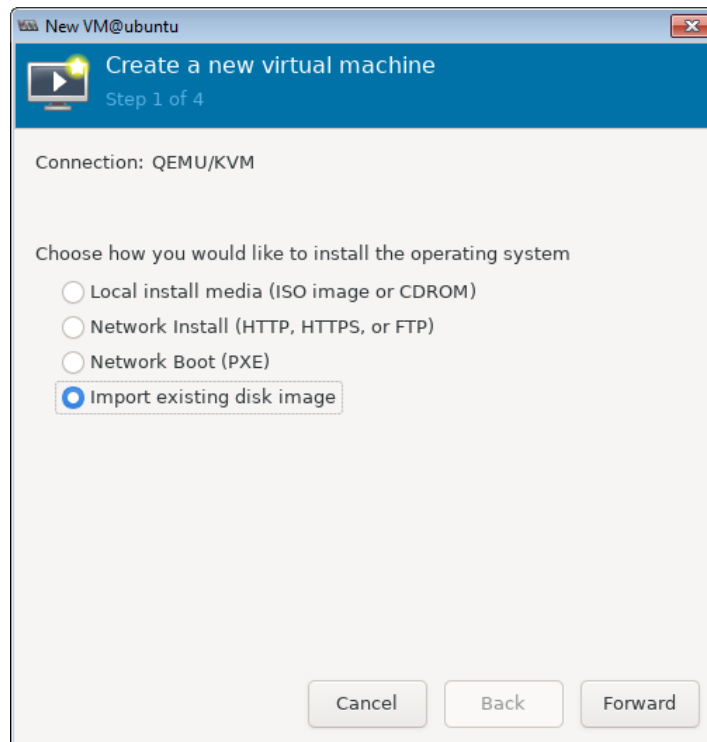
```
admin@ubuntu:~$ virt-manager
admin@ubuntu:~$ █
```

The following screen appears.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

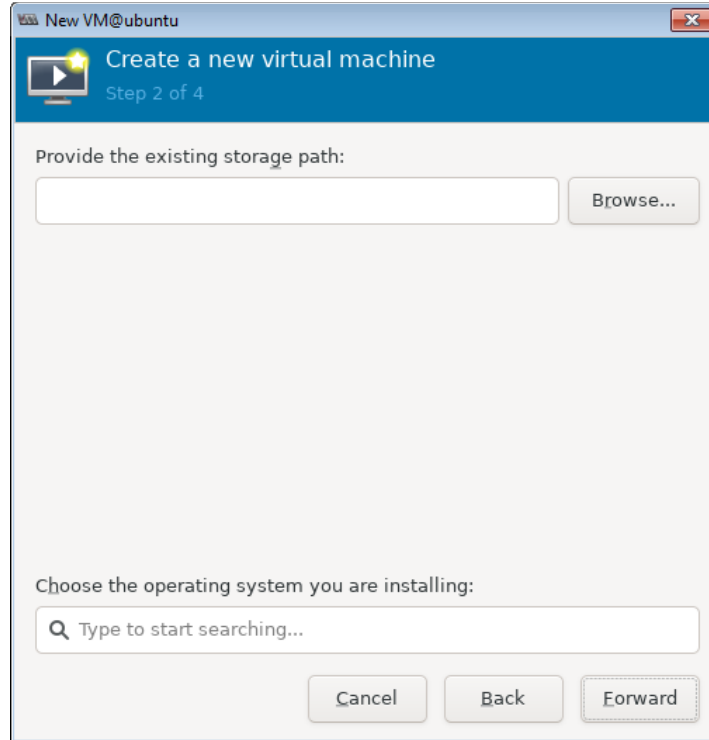


3. Select **File - New Virtual Machine**. The Create a New Virtual Machine Screen (Step 1 of 4) appears.

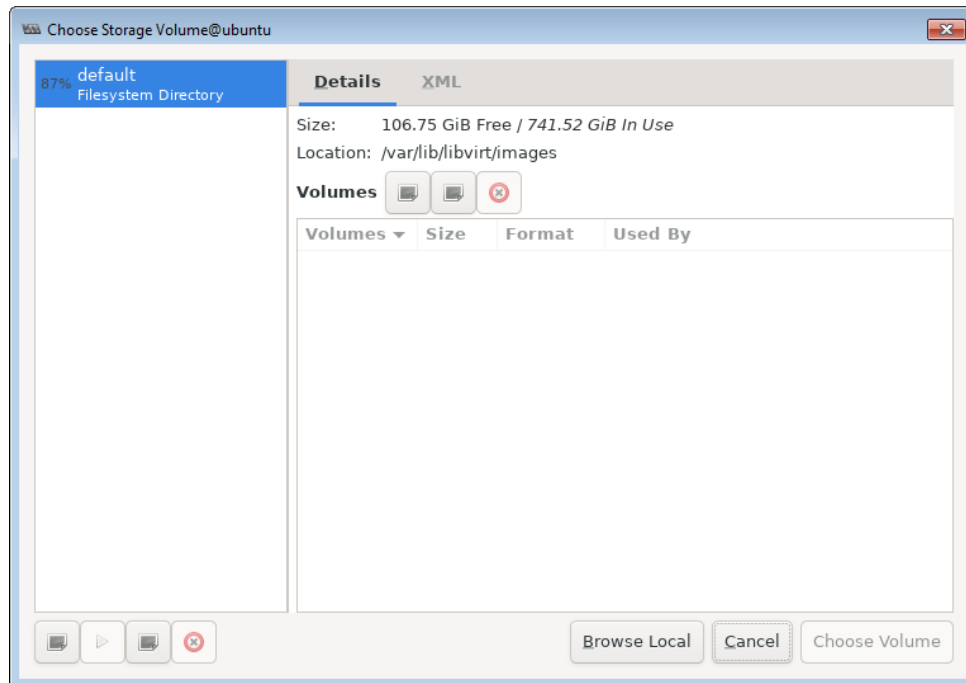


4. Select **Import existing disk image**, and click **Forward**. The Create a New Virtual Machine Screen (Step 2 of 4) appears.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

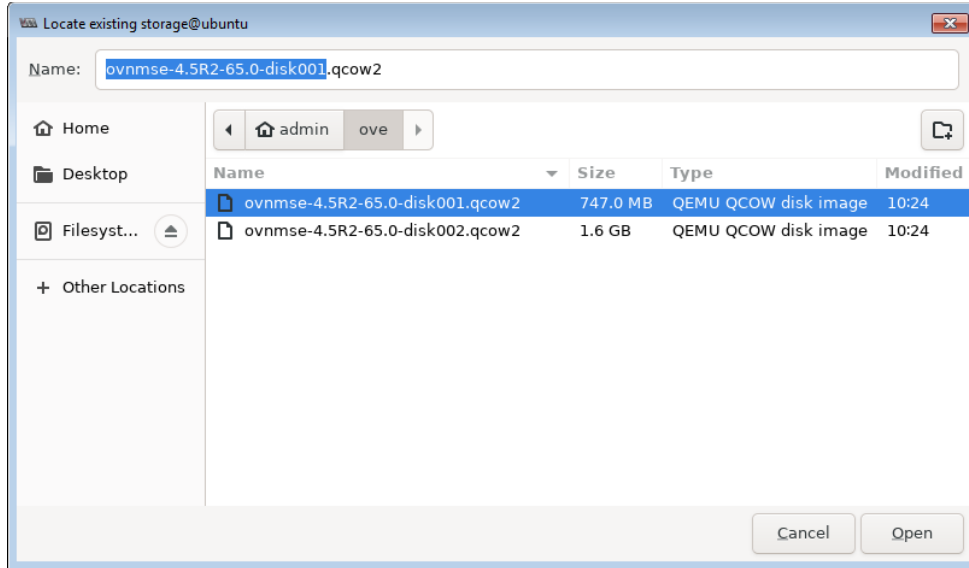


5. Click **Browse** to locate the storage disk.

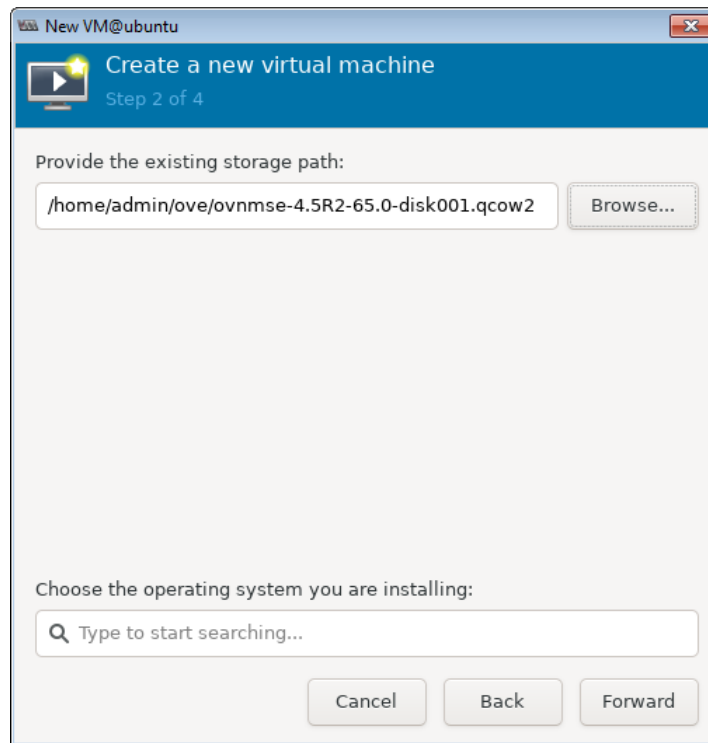


6. Click **Browse Local** to locate the disk files from the KVM package that you downloaded.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

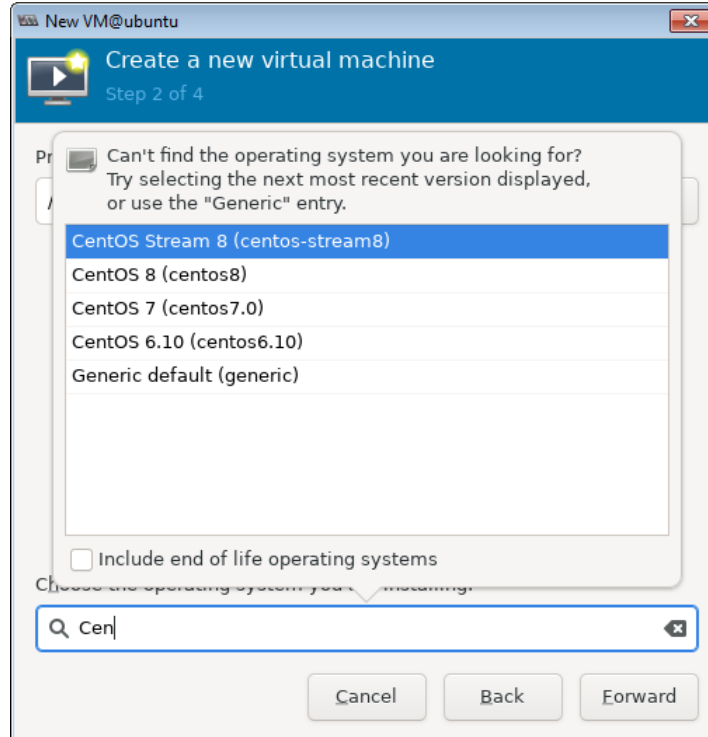


7. Select **disk001** and click **Open**. The Create a New Virtual Machine Screen (Step 2 of 4) appears.

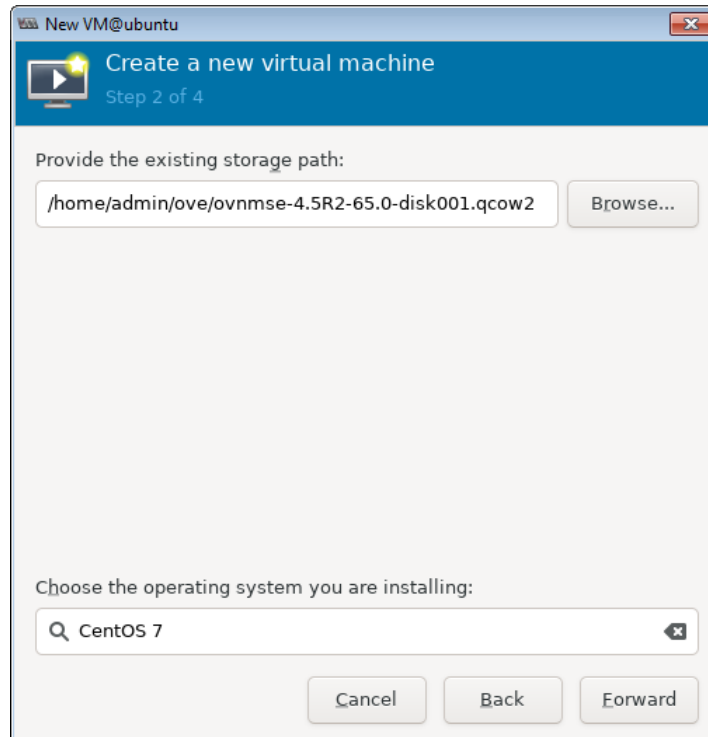


8. In the search field at the bottom of the screen, enter **Cen** to bring up CentOS versions, and select **CentOS 7 (centos7.0)**.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

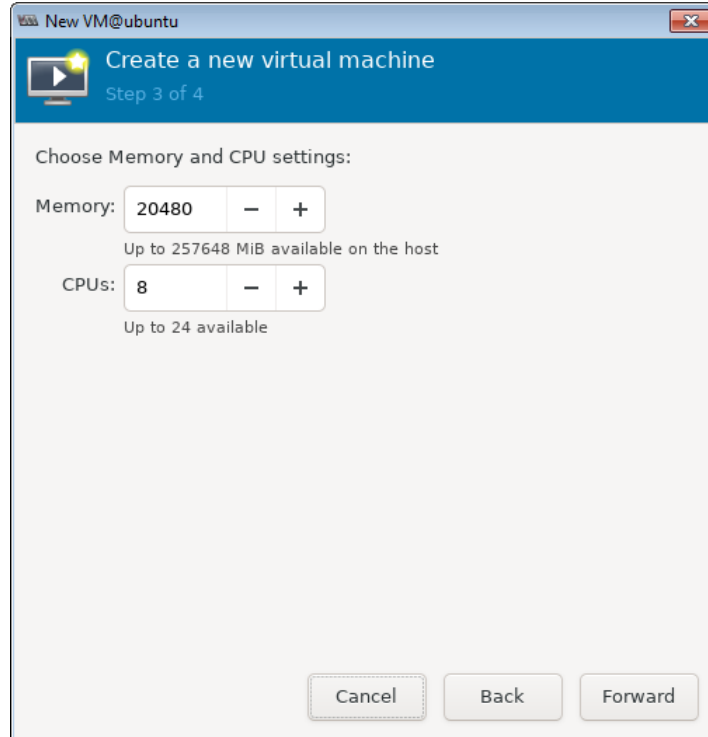


The completed Create a New Virtual Machine Screen (Step 2 of 4) appears, as shown below.



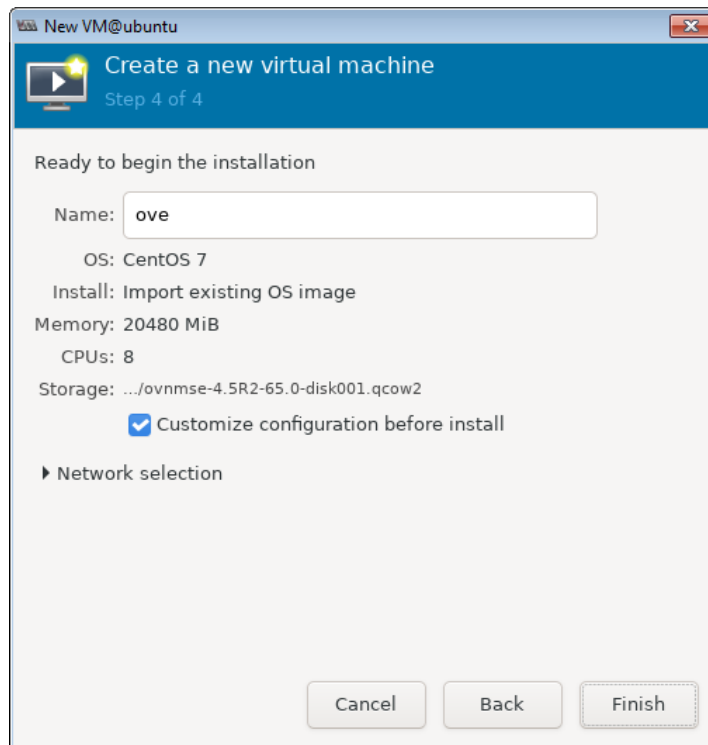
9. Click **Forward**. The Create a New Virtual Machine Screen (Step 3 of 4) appears.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



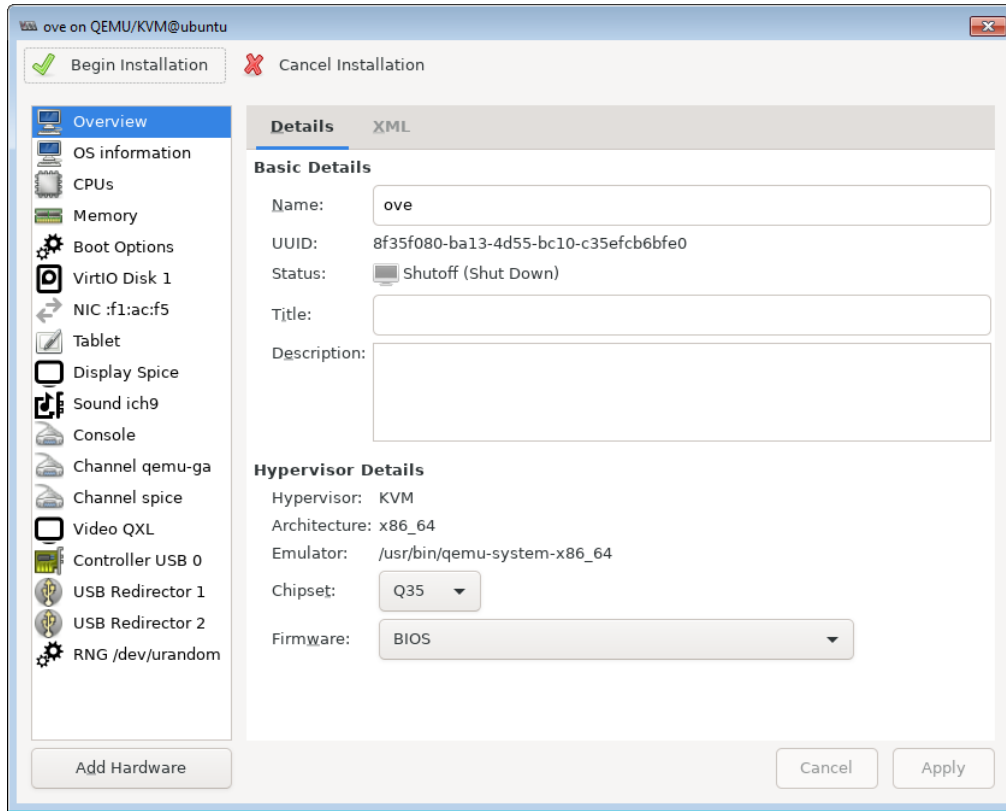
10. The default Memory and CPU values depend on the OS family you select. The list of OS families is in KVM by default, so you cannot change it when deploying OV on KVM. Click **Forward** to continue.

The Create a New Virtual Machine Screen (Step 4 of 4) appears.



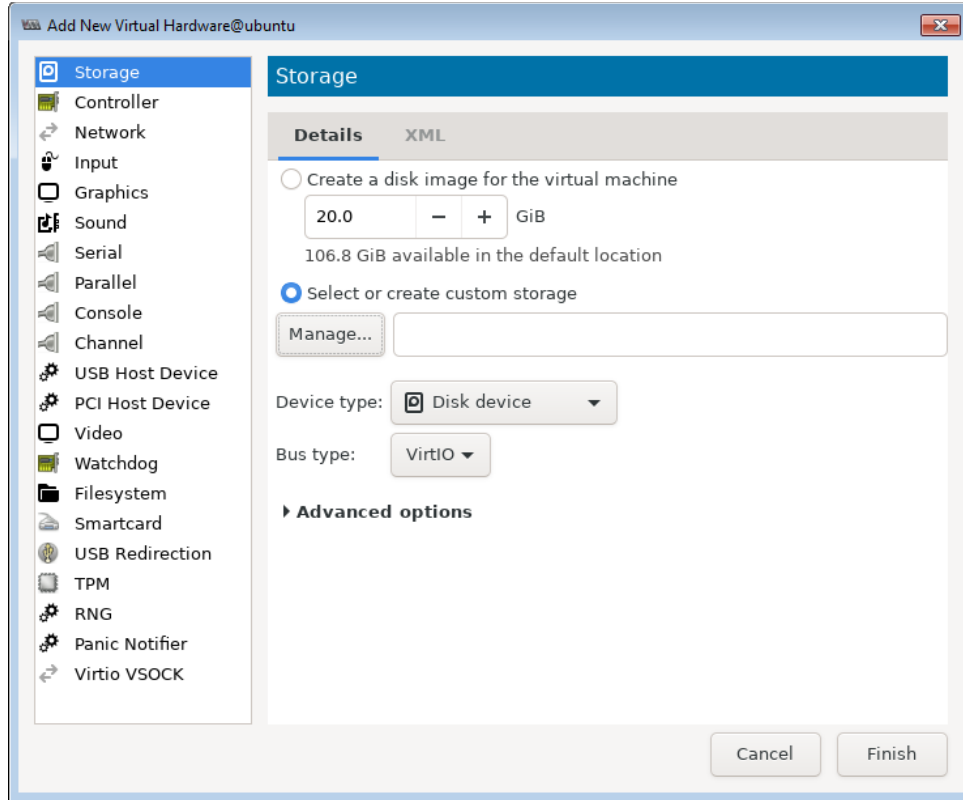
OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

11. Enter a **Name** for the VA (e.g., ove), check the **Customize configuration before install** checkbox, then click **Finish**. The following screen will appear.

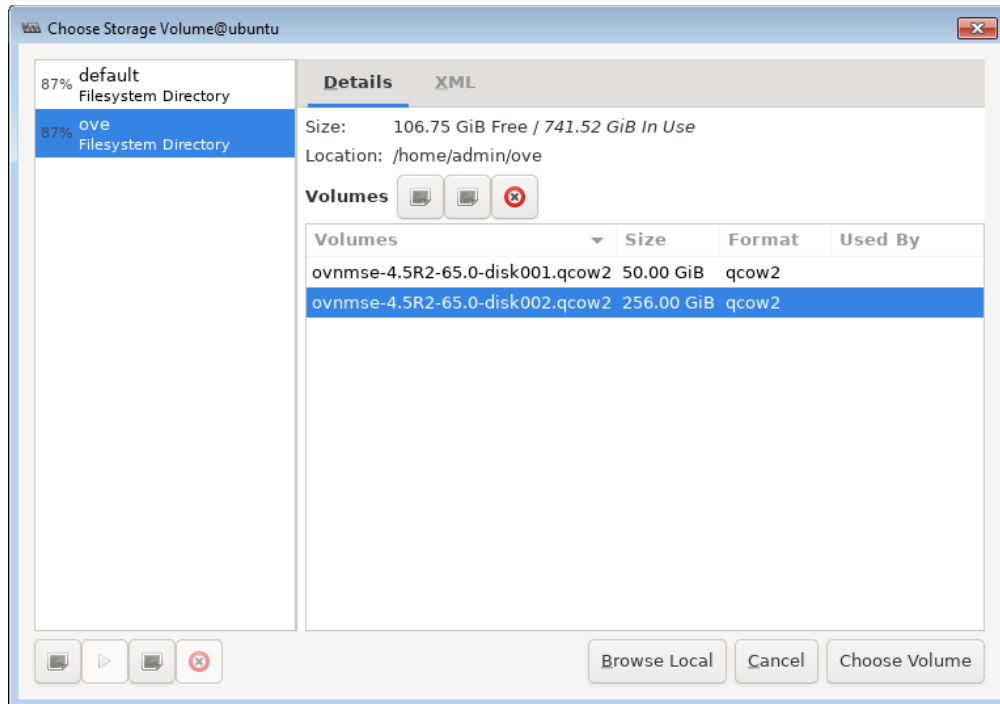


12. Click on **Add Hardware** on the bottom left side of the screen. The following screen appears.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

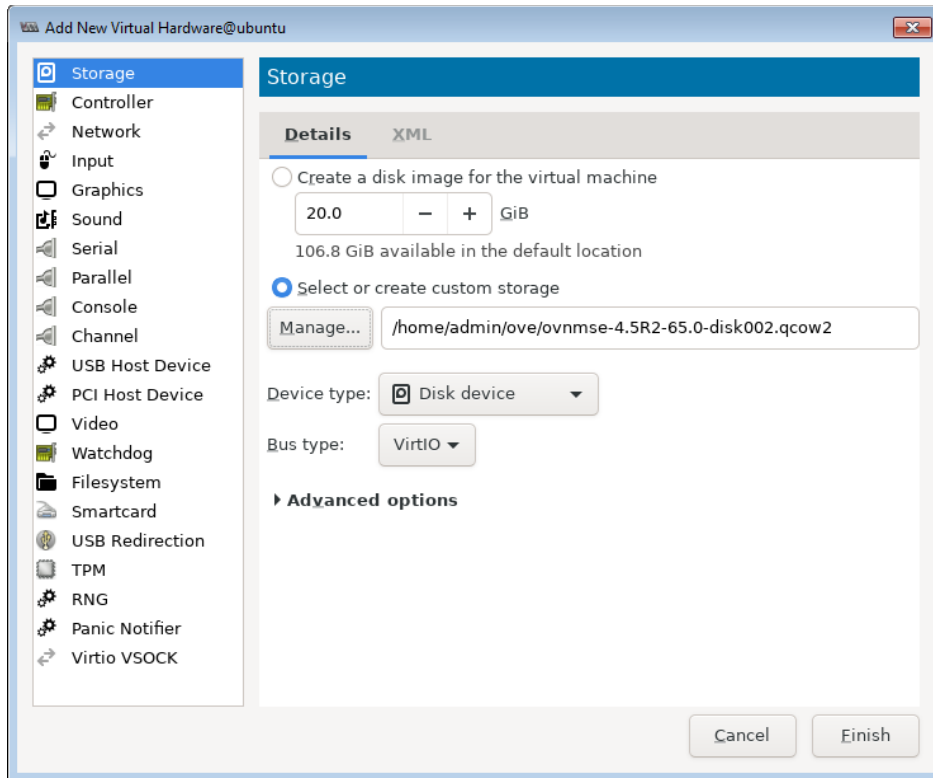


13. Make sure the **Storage** tab is selected, then and click on the **Select or create custom storage** radio button and click on **Manage**. The following screen appears.

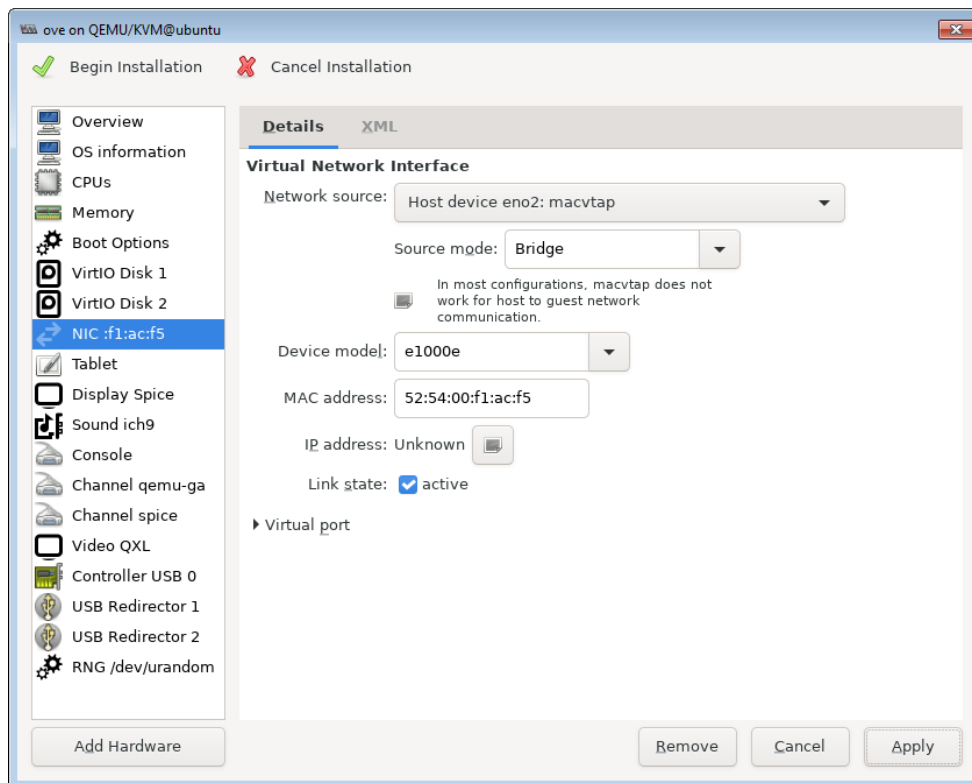


14. Locate the **disk002** file, select it, then click on **Choose Volume**. The following screen appears.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



15. Click **Finish** to return to the VM Configuration Window.

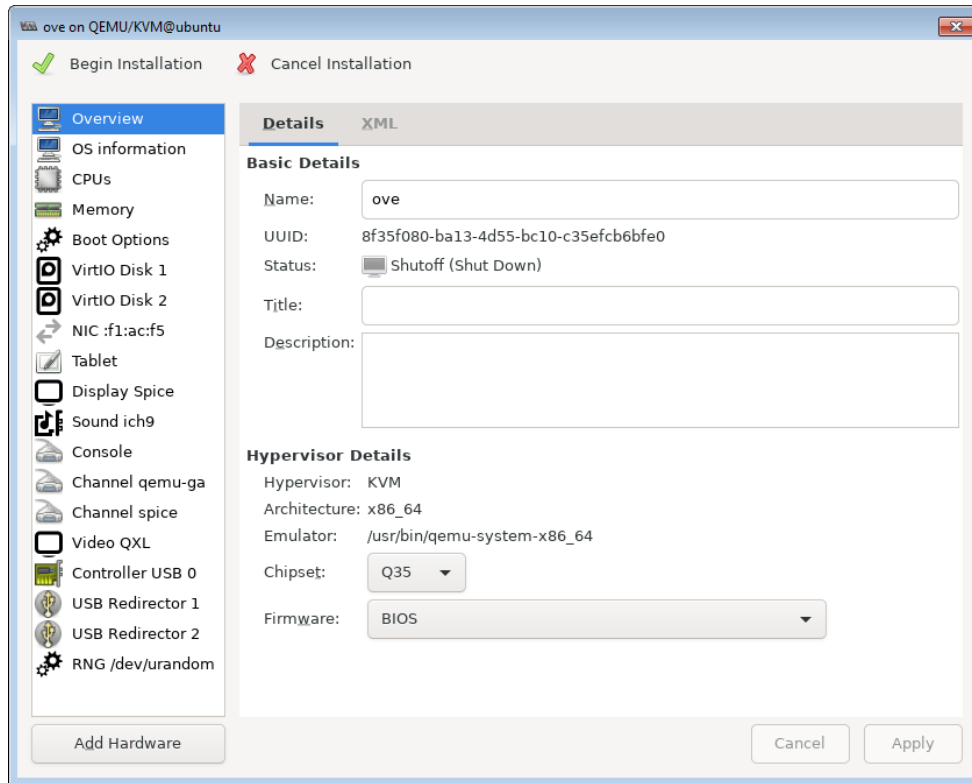


16. Select the VA NIC and configure the NIC as shown below, then click **Apply**:

- **Network Source:** Select the appropriate Host device

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- **Source Mode:** Bridge
- **Device Model:** e1000



17. Before beginning the installation (Step 18), reduce qcow2 disk size. Select **VirtIO Disk 1** on the left side of the screen. Select **Advanced options**, then select **Performance options** and set the **Discard Mode** to **unmap**. Repeat for the **VirtIO Disk 2**.

▼ Advanced options

Disk bus:

Serial number:

Storage format:

▼ Performance options

Cache mode:

IO mode:

Discard mode:

Detect zeroes:

18. Click on **Begin Installation** at the top-left corner of the window to begin the deployment.

19. Once the Virtual Appliance is powered on, the VA Console Screen will appear. Go to [Completing the OmniVista Installation](#) to complete the installation.

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

Completing the OmniVista Installation

Follow the steps in the following sections to complete the OV 2500 NMS 4.9R2 installation.

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

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 13
Patch Number: 0
Build Date: 04/01/2025
Activate the web console with: systemctl enable --now cockpit.socket

omnivista login: cliadmin (automatic login)
Regenerating ssh host keys...
Configured Keyboard Layout: us
Would you like to configure new Keyboard Layout [y|n] (n):
```

The Technical Support Code Password Screen appears.

```
*****
* Configure Technical support code
*****
You must remember the new Code and provide it to ALE Support Team for any troubleshooting on this OV Virtual Appliance.
Press [Enter] to continue
```

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

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

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

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

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

```

*****
* Configure IPs and Ports
*****
Reading current configurations, please wait...
(*) Please input OV IPv4: 10.255.221.26
Please input subnet mask [255.0.0.0]: 255.255.255.0
We have only one unused NIC [eth0-00:15:5d:dd:57:20], so use it for OV IP too
Please input OV Web HTTP port [80]:
Please input OV Web HTTPS port [443]:
Would you like to configure OV IP with:
    IPv4: 10.255.221.26
    Netmask: 255.255.255.0
    NIC: eth0-00:15:5d:dd:57:20
    OV Web HTTP Port: 80
    OV Web HTTPS Port: 443
[y|n] (y): _

```

4. Press **Enter** to configure the OmniVista IP address and mask.
5. Enter an IPv4 address (e.g., 10.255.221.26).
6. Enter the IPv4 network mask (e.g., 255.255.255.0). If you have more than one NIC configured for the Virtual Machine, you will be prompted to select the NIC to use for the OmniVista IP. Select the NIC and press **Enter**.
7. Enter the OV Web HTTP Port (e.g., 80).
8. Enter the OV Web HTTPS Port (e.g., 443).
9. Enter **y** and press **Enter** to continue. The Configure Captive Portal IP & Ports prompt appears.

```

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

```

10. Enter **1** and press **Enter** to configure the Configure Captive Portal IP & Ports. If you are not managing a wireless network and will not be using Captive Portal, enter **2** and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt. Go to Step 13.
- If you select **1** in this step, the Captive Portal IP & Ports configuration must be completed (Steps 11 – 12). If you select **2**, go to Step 13.

```

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

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

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

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

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

```

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

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

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

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

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

```
*****
* 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: 1
Would you like to set:
    The number of devices: Low (lower than 500)
[y/n] (y):
The configuration has been set
Press [Enter] to continue
```

Select the number of devices OV 2500 NMS 4.9R2 will manage. To select a range, enter its corresponding number at the command prompt (e.g., enter **1** for Low). Ranges include:

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

Press **Enter**; then enter **y** and press **Enter** at the confirmation prompt. It may take a minute for the configuration to be applied. The Default Language Prompt appears.

```
Select default language for OV UI
[1] English
[2] Chinese
(*) Type your option: _
```

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

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

Important Note: Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. Insufficient memory or disk space for the chosen network size may cause OV instability. OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 20GB of memory for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to [Recommended System Configurations](#) for details.

```

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

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

```

*****
* 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):
The configuration has been set
Press [Enter] to continue
    
```

17. Enter an IPv4 default gateway IP address (e.g., 10.255.221.254).

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

```

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

19. Type 0 and press **Enter** to exit the menu and complete the installation. The following message will display:

```
Please wait for a moment to complete the deployment process.

You may login to OV Web UI after ensuring that all services are in Running status. Please use watchdog
commands to check services status. If some services are still starting up, OV UI may throw errors
during login, or show other errors when retrieving data from OV server.
Press [Enter] to continue
_
```

Press **Enter** to continue. OmniVista will display the current configuration and reboot (it takes about a minute to display the current configuration and start the reboot). When the reboot is complete, the OmniVista Login Screen will appear.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 13
Patch Number: 0
Build Date: 04/01/2025
Technical Support Code: Alcatel123
Activate the web console with: systemctl enable --now cockpit.socket

omnivista login:
```

20. Log into the VM.

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

After successful login, the Virtual Appliance Menu appears.

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

If necessary, you can configure additional settings (e.g., Proxy, DNS) that may be required to access OV 2500 NMS 4.9R2. For more information on configuring the VM, see [Appendix A – Using the Virtual Appliance Menu](#).

Note: OV 2500 NMS 4.9R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository. 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 4.9R2 to connect to these external sites (Port 443):

- **ALE Central Repository** - ovrepo.fluentnetworking.com
- **AV Repository** - ep1.fluentnetworking.com
- **Fleet Supervision FQDN** – myfleet.ovcirrus.com
- **Call Home Backend** - us.fluentnetworking.com
- **Device Fingerprinting Service** - api.fingerbank.org
- **Web Content Filtering** - api.bcti.brightcloud.com.

21. After completing all required settings, verify that all services are running using the **Run Watchdog Command** in the Virtual Appliance Menu. Select **3**, then press **Enter**, then select **2** and press **Enter** to display the status of OmniVista Services. See [Run Watchdog Command](#) for more details.

22. Once all services are running, enter `https://<OVServerIPaddress>` in a supported browser to launch OV 2500 NMS 4.9R2.

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

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

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

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

Converting to a High-Availability Installation

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

Note:

- An HA license is required for a 4.9R2 HA Installation. Make sure you import the HA license before converting a 4.9R2 Standalone Installation to a 4.9R2 HA Installation.
- You can convert a fresh 4.9R2 Standalone Installation to a 4.9R2 HA Installation.
- You can convert a 4.9R2 Standalone Installation to a 4.9R2 HA Installation if the 4.9R2 Standalone installation was upgraded from a 4.3R2 or newer Standalone Installation.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- You cannot convert a 4.9R2 Standalone Installation to an HA Installation if the 4.9R2 Standalone Installation was upgraded from a 4.3R1 Standalone Installation.
- Converting an L2 HA installation to an L3 HA installation is **not** supported. Only a fresh L3 HA installation is supported. However:
 - You can add a second node to a fresh 4.9R1 standalone installation to convert the cluster to an L3 HA installation.
 - You can also upgrade a 4.8R2 standalone installation to 4.9R1 and then convert it to an L3 HA installation.

There are two HA Installation configurations:

- [Layer 2 Configuration](#) - In a Layer 2 HA Configuration, both OmniVista Server VMs must be on the same subnet. In this configuration, you configure a virtual Cluster IP address. Both the Active and Standby Nodes are reached through the Cluster IP address. Network devices communicate with the Active Node through the Cluster IP address. In the event of a failover, the Standby Node becomes the Active Node and network devices, again, communicate to it through the Cluster IP address.
Generally, when converting an existing Standalone Installation, you will configure it as a Layer 2 Installation (using the existing OmniVista Server IP address as a virtual Cluster IP address). This will avoid having to re-configuring devices to a new OmniVista Server IP address after the conversion because network devices will still be communicating with OmniVista using the same IP address. During the conversion process, there is an option to assign a new IP address to the existing OmniVista Server. The existing IP address is then available in the next step to configure it as the Cluster IP address.
- [Layer 3 Configuration](#) - In a Layer 3 HA Configuration the OmniVista Server VMs are on different subnets, with a unique IP address for each server. Network devices can communicate with both VMs (Active and Standby Nodes). Network devices communicate with the Active Node. In the event of a failover, devices automatically communicate with the new Active Node. You can convert an existing Standalone Installation to a Layer 3 Installation; however, you will have to re-configure network devices to communicate with both Nodes. Make sure network devices can communicate with **both** nodes (Active and Standby).

Important Notes:

- Features or functions that require devices to contact OmniVista are **not** supported in a Layer 3 Configuration (e.g., sFlow, Policy). Consider the following:
 - **Syslog** – Supports AP if an external syslog server is used or if the OV IP for the two nodes is configured when enabling the syslog in AP Group.
 - **IoT** – Supports AP, but not support AOS because AOS receives the IP OV when enabling IoT (must re-apply after failover).
 - **Policy** – Does not support AOS because AOS receives policy server (IP OV) when notified the policy (must re-apply after failover)
 - **Provisioning (AOS)** – Related to DNS configuration, DNS can resolve AS-lite to IP OV (must re-configure DNS if new devices callhome after failover).
 - **Top N Apps/Ports (sflow)** – Does not support AOS.
- Configuring L3 Redundancy Settings is supported only on AP13XX and higher models running AWOS 5.0 or higher; it is not supported on AP11XX or AP12XX models.
- Configuring a [Preferred Node](#) through the cliadmin menu is required for an L3 HA installation.
- When a failover occurs, the AP tries to establish a session with the other OmniVista server in the L3 HA installation. During this time, OmniVista will show that the AP is down (anywhere from 5 to 10 minutes); however, the AP remains up in the network.

Notes:

- The Hypervisor's on which you are installing OmniVista must have the latest Network Adaptor drivers:
 - Hyper-V:
 - Broadcom: Version b57nd60a.sys version 16.8 and later.
 - HP: Version 16.8 and later.
 - VMware:
 - Broadcom: Version Tg3-3.133d.v55.1-101300361 and later.
- The recommended network bandwidth is 1Gbps. The recommended network latency is 1ms.
- You must have a High-Availability License to enable the High Availability Feature. After you complete the installation, the first time you open OmniVista in a browser, you will be prompted to activate the OmniVista License and the High-Availability License.
- Take a VM Snapshot of the current Standalone VM **before** performing the conversion. Note that VM snapshots can cause performance issues on the running VM. It is recommended that you delete any previous snapshots, take a new snapshot of the current Standalone VM configuration, then perform the conversion. After the Standalone VM conversion is successfully completed, it is recommended that you also delete the snapshot taken prior to the conversion. For long-term VM backups, consult the virtualization software documentation for recommended procedures.

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

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

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

- **Captive Portal Virtual IP Address (Layer 2 Configuration Only)** – This IP address is needed if you want to use Captive Portal in HA Cluster Mode (Layer 2 Configuration). This virtual IP address is used to communicate with the network (and with the Active and Standby Nodes) when you use the Captive Portal. This IP address must be on the same subnet as the Static Captive Portal IP address.
- **Additional OV Web Virtual IP (Layer 2 Configuration Only)** – This optional additional OV Web Virtual IP provides you with another way of accessing the OmniVista UI. The OV Web Virtual IP address must be on the same subnet as the static OV Web IP address.

Layer 2 Configuration

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

- [Converting Node 1 to Cluster Mode](#)
- [Joining Node 2 to the Cluster](#)
- [Verifying the Conversion](#)
- [Logging into the OmniVista UI](#)

Converting Node 1 to Cluster Mode

First, convert Node 1 to Cluster Mode. If you are converting an existing 4.9R1 Standalone Installation, these steps are performed on the existing Standalone VM.

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

```

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

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

```

OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed converting to cluster?[y/n] (n): _
    
```

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

```

After rebooting, the background process will continue, this could take a while to complete in boot s
creen!!!
Press [Enter] to continue
_
    
```

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

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

```

Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 13
Patch Number: 0
Build Date: 04/01/2025
Technical Support Code: Alcatel123
Activate the web console with: systemctl enable --now cockpit.socket

omnivista login:
    
```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```
You have selected converting this node to cluster. Please complete this process...

ATTENTION: If you are converting an existing standalone configuration to a cluster configuration, you
must use the existing standalone OUV IP address for the Cluster IP address to avoid re-configuring
devices after the conversion. Change the existing OUV IP address to another IP address and use the
existing OUV IP address for the Cluster IP in next steps. If the existing Captive Portal IP address is
the same as the existing OUV IP address, we must also change it.

Would you like to enter IPs configuration menu to assign another IP address to this cluster node [y|
n] (y):
```

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

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

```
*****
* Configure IPs and Ports
*****
Reading current configurations, please wait...

Current OUV IP Configuration:
  IP: 10.255.222.97
  Netmask: 255.255.255.0
  NIC: eth0
  MAC: 00:0c:29:bc:92:40
  OUV Web HTTP Port: 80
  OUV Web HTTPS Port: 443

Would you like to configure OUV IP and OUV Web Ports [y|n] (n): y
Please input OUV IPv4 [10.255.222.97]: 10.255.222.203
Please input subnet mask [255.255.255.0]:

Select the NIC for assigning OUV IP:
[1] eth0-00:0c:29:bc:92:40
[2] eth1-00:0c:29:bc:92:4a
(*) Type your option: 1
Please input OUV Web HTTP port [80]:
Please input OUV Web HTTPS port [443]:
Would you like to configure OUV IP with:
  IPv4: 10.255.222.203
  Netmask: 255.255.255.0
  NIC: eth0-00:0c:29:bc:92:40
  OUV Web HTTP Port: 80
  OUV Web HTTPS Port: 443
[y|n] (y):
```

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

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

```

Current Captive Portal IP Configuration:
IPv4: 198.168.0.1
Netmask: 255.255.255.0
NIC: eth1
MAC: 08:0c:29:bc:92:4a
Captive Portal Web HTTP Port: 80
Captive Portal Web HTTPS Port: 443
IPv6:
Prefix:

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

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

Configure Captive Portal IP & Ports
[1] Configure new Captive Portal IP & Captive Portal Ports
[2] Disable Captive Portal
(*) Type your option: 1
Please input Captive Portal IPv4 [198.168.0.1]:
Please input subnet mask [255.255.255.0]:
We have only one unused NIC [eth1-08:0c:29:bc:92:4a], so use it for Captive Portal IP too
Would you like to configure Captive Portal IPv6 [y|n] (n):
Please input Captive Portal HTTP port [80]:
Please input Captive Portal HTTPS port [443]:
Would you like to configure Captive Portal IP with:
IPv4: 198.168.0.1
Netmask: 255.255.255.0
NIC: eth1-08:0c:29:bc:92:4a
Captive Portal HTTP Port: 80
Captive Portal HTTPS Port: 443
IPv6:
Prefix:
[y|n] (y): _
    
```

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

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

```

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

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

```

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

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

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

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

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

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

```
(*) Please input Cluster Name: ovcluster1
Would you like to configure:
    Cluster Name: ovcluster1
[y|n] (y):
```

12. Enter an alphanumeric Cluster Name (e.g., ovcluster1), enter **y**, then press **Enter**. The following prompt will appear.

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

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

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

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

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

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

If you have a Captive Portal IPv6 configuration or an additional OV Web IP configuration, you will be prompted to configure the virtual IP addresses for each. Otherwise, the conversion process will start with the progress displayed at the bottom of the screen (the process can take 15 – 20 minutes).

```

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

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

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

```

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

```

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

```

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

```

Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 13
Patch Number: 0
Build Date: 04/01/2025
Technical Support Code: Alcatel123
Activate the web console with: systemctl enable --now cockpit.socket

ov1 login: cliadmin
Password:
Last login: Thu Apr 10 21:48:30 on tty1

```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```

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

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

Joining Node 2 to the Cluster

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

```

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

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

```

All data on this node will be lost and OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed joining cluster?[y/n] (n): _
    
```

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

```

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

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

```
*****
* Configure Hostname
*****
Please input hostname [omnivista]: ov2
Would you like to configure:
    hostname: ov2
[y|n] (y):
The configuration has been set
Press [Enter] to continue
```

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

```
*****
* Configure Peer Node's Information
*****
(*) Please input IP of Peer Node: 10.255.221.27
Would you like to to configure
    IP of Peer Node: 10.255.221.27
[y|n] (y):
```

6. Enter the physical IP address of Node 1. This is the new physical IP address you assigned to Node 1 in Step 6 of the previous section (e.g., 10.255.221.27), then enter **y** and press **Enter** to confirm.

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

```
Getting information from Peer...
After rebooting, the background process will continue, this could take a while to complete in boot screen!!!
Press [Enter] to continue
```

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

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 14
Patch Number: 0
Build Date: 04/05/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```
You have selected Joining cluster on this node. Please complete the process...
Preparing, please wait...
Connecting to Peer...
Continue connecting to Peer as final joining step...

Joining cluster is now completed. Now the data is being synchronized between nodes.

You could trace the progress in show cluster status menu.

You must logout and re-login to use the HA administration menu. Press Enter to do so
```

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

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 14
Patch Number: 0
Build Date: 04/05/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
```

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

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

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

Verifying the Conversion

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

- Go to the HA Virtual Appliance Menu of Node 1.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Enter **5** (Run Watchdog Command) then press **Enter**. Enter **2** (Display Status of All Services) and press **Enter** to display the status of OmniVista Services. See [Run Watchdog Command](#) for more details.
2. Verify that all services are running on Node 2:
- Go to the HA Virtual Appliance Menu of Node 2.
 - Enter **5** (Run Watchdog Command) then press **Enter**. Enter **2** (Display Status of All Services) and press **Enter** to display the status of OmniVista Services. See [Run Watchdog Command](#) for more details. Note that on Node 2, all services should be running except upam and nginx. It is the expected behavior on the Standby Node that these services will be “Stopped”. The ovradius service may also be stopped when Custom RADIUS Certificates are used.
3. Check the Cluster status on Node 1.
- Go to the HA Virtual Appliance Menu of Node 1.
 - Enter **2** (Show OV Cluster Status) then press **Enter**. See [Show OV Cluster Status](#) for more information.

Logging into the OmniVista UI

1. Once all services are running, enter *https://<ClusterIPAddress>* in a supported browser to launch OV 2500 NMS 4.9R1.

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

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

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

Layer 3 Configuration

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

- [Converting Node 1 to a Cluster Configuration](#)
- [Joining Node 2 to the Cluster](#)
- [Verifying the Conversion](#)
- [Logging into the OmniVista UI](#)

Converting Node 1 to Cluster Mode

First, convert Node 1 to Cluster Mode. If you are converting an existing 4.9R2 Standalone Installation, these steps are performed on the existing Standalone VM.

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

```

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

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

```

OU will restart if you continue.
Backing up this OU installation before continue is strongly recommended.
Are you sure want to proceed converting to cluster?[y/n] (n):
    
```

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

```

After rebooting, the background process will continue, this could take a while to complete in boot s
creen!!!
Press [Enter] to continue
    
```

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

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

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 13
Patch Number: 0
Build Date: 04/01/2025
Technical Support Code: Alcatel123
Activate the web console with: systemctl enable --now cockpit.socket

omnivista login:
```

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

```
You have selected converting this node to cluster. Please complete this process..

ATTENTION: If you are converting an existing standalone configuration to a cluster configuration, you
must use the existing standalone OV IP address for the Cluster IP address to avoid re-configuring
devices after the conversion. Change the existing OV IP address to another IP address and use the ex
isting OV IP address for the Cluster IP in next steps. If the existing Captive Portal IP address is
the same as the existing OV IP address, we must also change it.

Would you like to enter IPs configuration menu to assign another IP address to this cluster node [y|
n] (y): _
```

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

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

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

```
*****
* Configure Hostname
*****
Please input hostname [ovnode1]: ove138node1
Would you like to configure:
    hostname: ove138node1
[y|n] (y):
```

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

```
Preparing, please wait...

(*) Please input Cluster Name: ove13HA
Would you like to configure:
    Cluster Name: ove13HA
[y|n] (y): y
```

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

```
Current OV IP Configuration:
IP: 10.255.221.138
Netmask: 255.255.255.0
Would you like to configure OV Virtual IP address [y|n] (y): n_
```

10. Enter **n**, press **Enter**, then enter **y** and press **Enter** again at the Confirmation Prompt. Note that if you are converting from an existing Standalone Installation and were using a Captive

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Portal, it will be disabled in a Layer 3 Configuration. The process will start with the progress displayed at the bottom of the screen (the process can take 10 – 15 minutes).

```
Current Captive Portal IP Configuration:
  IP: 10.255.221.138
  Netmask: 255.255.255.0
OU Virtual IP isn't configured, so skip configuring Captive Portal Virtual IP!

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

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

Initializing (step 1/3).....
```

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

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 14
Patch Number: 0
Build Date: 04/05/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
```

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

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

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

Joining Node 2 to the Cluster

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

```

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

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

```

All data on this node will be lost and OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed joining cluster?[yin] (n):
    
```

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

```

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

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

```

*****
* Configure Hostname
*****
Please input hostname [ovnode2]: ov139node2
Would you like to configure:
    hostname: ov139node2
[yin] (y): y
The configuration has been set
Press [Enter] to continue
    
```

5. Enter a Hostname (up to 15 characters) for Node 2 and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt, then press **Enter** again to continue. Note that the Hostname **must** be in lower case letters (e.g., “ov2” **not** “OV2”). The Configure Peer Node’s Information Screen appears.

```

*****
* Configure Peer Node's Information
*****
(*) Please input IP of Peer Node: 10.255.221.138
Would you like to to configure
    IP of Peer Node: 10.255.221.138
[yin] (y): y
    
```

6. Enter the IP address of Node 1 (e.g., 10.255.221.138), then enter **y** and press **Enter** to confirm.

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

```
After rebooting, the background process will continue, this could take a while to complete in boot screen!!!  
Press [Enter] to continue
```

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

```
Oracle Linux Server 8.10  
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64  
  
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA  
Build Number: 14  
Patch Number: 0  
Build Date: 04/05/2025  
Technical Support Code: alcatel  
Activate the web console with: systemctl enable --now cockpit.socket  
  
l2hanode152 login: cliadmin  
Password:
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```
You have selected Joining cluster on this node. Please complete the process...  
Preparing, please wait...  
Connecting to Peer...  
WARN: stdin/stdout is not a TTY; using /dev/console.Continue connecting to Peer as final joining step...  
  
Joining cluster is now completed. Now the data is being synchronized between nodes.  
You could trace the progress in show cluster status menu.  
  
You must logout and re-login to use the HA administration menu. Press Enter to do so
```

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

```

Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 14
Patch Number: 0
Build Date: 04/05/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
    
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```

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

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

Verifying the Conversion

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

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

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Standby Node that these services will be “Stopped”. The ovradius service may also be stopped when Custom RADIUS Certificates are used.

3. Check the Cluster status on Node 1.

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

Logging into the OmniVista UI

1. Once all services are running, enter *https://<IPaddress of the Active Node>* in a supported browser to launch OV 2500 NMS 4.9R2.

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

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

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

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

Upgrading from 4.9R1 to 4.9R2

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.9R1 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.9R2 Standalone or High-Availability Installation.

Important Notes:

- Upgrading an OV 2500 NMS from 4.9R1 to 4.9R2 automatically includes a required upgrade to a 4.9R1 Patch 1. As a result, there is a change to the upgrade workflow to ensure that the 4.9R1 upgrade to 4.9R1 Patch 1 occurs first, before the upgrade to 4.9R2. The new upgrade workflow is documented in [Upgrading from 4.9R1 Standalone to 4.9R2 Standalone](#) and in [Upgrading from 4.9R1 HA to 4.9R2 HA](#).
- During the upgrade time for an OmniVista Standalone installation, OmniVista is not available for any management functions. There is no impact to the deployed network during the OmniVista upgrade. Managed devices (Switch/AP) and existing device clients will continue to function as before. However, new clients cannot join the network if the Switch/AP is configured to do authentication from UPAM. The upgrade downtime may last between one and four hours and starts when the Maintenance Mode is enabled.
- When one of the nodes in an HA cluster becomes faulty, it can be decommissioned and replaced with a new node. While the HA is running in single node mode, prepare the new node, extend its data partition size as needed to match that of the old node, then join the new node to the cluster.
- It is recommended that you make note of your IP and NIC configurations before initiating a Standalone or HA upgrade to 4.9R2. Depending on the NIC types and hypervisor version, some special cases may require you to reconfigure these settings during or immediately after the upgrade to 4.9R2. If necessary, the VA will prompt you to perform the reconfiguration.
- You must perform the OmniVista upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client, upgrading the installation can result in incomplete upgrades and missing any pending actions, such as pressing the enter key to continue the upgrade.

Upgrading from 4.9R1 Standalone to 4.9R2 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.9R1 Standalone Installation to an OV 2500 NMS 4.9R2 Standalone Installation.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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 OmniVista makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

1. Open a Console on the OV 2500 NMS 4.9R1 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: 4
```

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to "ALE Central Repo", then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **2 - Configure the Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

- Important Note:** This step is required to successfully upgrade to the 4.9R2 release. **DO NOT SKIP THIS STEP FOR ANY REASON.** Enter **3 – To New Release** and press **Enter** to access the Upgrade to New Release menu, then enter **0 – Exit** and press **Enter** to return to the Upgrade VA Menu. Do not select the option to upgrade to 4.9R2.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R2
* [0] Exit
*****
(*) Type your option:
    
```

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

- Enter **2 – To 4.9R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter**. The Upgrade System Options Menu will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R1 GA
Build Number: 24
Patch Number: 8

Checking available packages for 4.9R1 operation is in progress...
Upgrade information for 4.9R1
Available Packages
Name      : ovmnse
Version   : 4.9R2
Release   : 15.0.e17
Architecture : x86_64
Size      : 3.0 G
Source    : ovmnse-4.9R2-15.0.e17.src.rpm
Repository : CustomRepo1_4.9R1
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
          :
          : WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major
          : release.

Would you like to upgrade the package [y/n] (n):

```

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

OmniVista detects the 4.9R2 build and displays the following message:

WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major release.

Enter **y** when asked “Would you like to upgrade the package” and press **Enter**. A warning message will appear asking you to proceed.

```

Would you like to upgrade the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release notes to this.
Are you ready to proceed ? [y/n] (n):

```

4. Enter **y** and press **Enter** to proceed with the upgrade to 4.9R2. The following message will appear, and the upgrade will begin.

```

Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)....

```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

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

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

5. When the installation is complete, the following prompt will appear: “Complete! Operation Successful”.

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

6. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 13
Patch Number: 0
Build Date: 04/01/2025
Technical Support Code: Alcatel1234
Activate the web console with: systemctl enable --now cockpit.socket

omnivista login:
```

7. Log into the VM. The Virtual Appliance Menu will appear.

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [yin] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the Configure the Virtual Appliance Menu, select **9 – Configure Network Size**, then select **4 – Extend Data Partition**.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

8. Verify the update to 4.9R2.
 - Verify that all services have started.
 - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
 - Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See [Run Watchdog Command](#) for more details.
 - Verify that the Build Number is correct.
 - From The Virtual Appliance Menu, select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See [Display Current Configuration](#) for more details.
 - Verify that you can [launch the OmniVista UI](#) and successfully login.
 - Take a VM Snapshot of the current OmniVista VA and remove previous VA snapshots.

Launching the OmniVista UI

Once all services are running after upgrading, enter <https://<OVServerIPAddress>> in a supported browser to launch OV 2500 NMS 4.9R2.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance**.
 2. **Select 2 - Display Current Configuration** to verify your currently configured network size (e.g., Low, Medium, High).

3. Select **9 - Configure Network Size**.
4. Select **2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.9R1 HA to 4.9R2 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.9R1 High-Availability Installation to an OV 2500 NMS 4.9R2 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA on both the Active and Standby nodes. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

- There is a different workflow for [upgrading an L2 HA installation](#) and for [upgrading an L3 HA installation](#). Make sure to follow the steps in each workflow based on whether you are upgrading an L2 HA or an L3 HA installation.

Note that OmniVista 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 **4 - Configure Current Node** on the Virtual Appliance Menu, then select **9 - Configure Proxy**.

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

L2 High-Availability Upgrade Workflow

The basic steps for performing an L2 High-Availability upgrade are:

1. [Upgrade the Active and Standby Nodes \(ov1 and ov2\) from 4.9R1 to 4.9R2](#)

Note: During the 4.9R1 to 4.9R2 upgrade time for an OmniVista High-Availability installation, OmniVista management functions remain available until the failover stage of the upgrade, at which time OmniVista is not available for approximately 5 to 10 minutes.

2. [Verify the cluster status to make sure data is in sync between the two nodes](#)

3. [Enable Maintenance Mode on the Active Node \(ov1\)](#)

4. [Connect to the Standby Node and upgrade the node to 4.9R2](#)

5. When the Standby Node upgrade is complete, do a reboot and failover. The Standby Node (ov2) is now the Active Node. Connect to the ov2 node and wait for all services to start.

6. [Connect to the previous Active Node \(ov1\) and upgrade the node to 4.9R2. Restart ov1 after the upgrade](#)

7. [Verify the Upgrade](#)

Note: After this upgrade process is complete, the Active Node at the beginning of the process is no longer the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return the node to Active Node status, you can do a manual failover on that node.

Upgrade the Active and Standby Nodes (ov1 and ov2) from 4.9R1 to 4.9R2

In this HA upgrade procedure, ov1 is initially the Active Node until the ov2 Standby Node is upgraded first. After ov2 is upgraded, the ov2 Node will become the Active Node and ov1 will become the Standby Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return ov1 to Active Node status, you can do a manual failover after both nodes are upgraded (see Step 13 in [Connect to the ov1 Node and Upgrade the Node to 4.8R2](#) for more details).

Verify the Cluster Status

Before you begin the process to upgrade the HA cluster from 4.9R1 to 4.9R2, verify that the Cluster Status is “Up to Date”. This can be performed on either node.

1. On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.
2. Begin the HA cluster upgrade from 4.9R1 to 4.9R2.

Enable Maintenance Mode on the Active Node (ov1)

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node (ov1). Open a Console on the OV 2500 NMS 4.9R1 ov1 Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

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

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

```
If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make
sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y|n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance
Mode!!!
Press [Enter] to continue
█
```

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

Connect to the Standby Node (ov2) and Upgrade the Node to 4.9R2

Note: During the Standby Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. However, any user-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are lost.

1. Open a Console on the OV 2500 NMS 4.9R1 Standby Node (ov2), which is already in Maintenance Mode.

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to "ALE Central Repo", then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

- Important Note:** This step is required to successfully upgrade to the 4.9R2 release. **DO NOT SKIP THIS STEP FOR ANY REASON.** Enter **3 – To New Release** and press **Enter** to access the Upgrade to New Release menu, then enter **0 – Exit** and press **Enter** to return to the Upgrade VA Menu. Do not select the option to upgrade to 4.9R2.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R2
* [0] Exit
*****
(*) Type your option:
    
```

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

- Enter **2 – To 4.9R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter**. The Upgrade System Options Menu will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R1 GA
Build Number: 24
Patch Number: 0

Checking available packages for 4.9R1 operation is in progress...
Upgrade information for 4.9R1
Available Packages
Name      : ovmnse
Version   : 4.9R2
Release   : 15.0.e17
Architecture : x86_64
Size      : 3.0 G
Source    : ovmnse-4.9R2-15.0.e17.src.rpm
Repository : CustomRepo1_4.9R1
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
          :
          : WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major
          : release.

Would you like to upgrade the package [y/n] (n): y
```

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

OmniVista detects the 4.9R2 build and displays the following message:

WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major release.

Enter **y** when asked “Would you like to upgrade the package” and press **Enter**. A warning message will appear asking you to proceed.

```
Would you like to upgrade the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release notes to this.
Are you ready to proceed ? [y/n] (n):
```

6. Enter **y** and press **Enter** to proceed with the upgrade to 4.9R2. The following message will appear, and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)...
```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
[2025-04-08-17-29-09] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2025-04-08-17-29-09] [POST-UNINSTALL] Done

Verifying      : ovnmse-4.9R2-15.0.e17.x86_64      1/2
Verifying      : ovnmse-4.9R1-24.0.e17.x86_64      2/2

Upgraded:
  ovnmse-4.9R2-15.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [r] to reboot the system.
```

Note: Ignore the warning message and continue with the upgrade by rebooting the Standby Node (ov2).

8. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: _
```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

9. Login through the VA console. When prompted, press **Enter** to perform the failover. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes).

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
Last login: Tue Apr  1 17:12:55 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
_
```

Note: If you are upgrading the Standby Node to 4.9R2 from 4.7R1 or older, you may see the message “{“Status”:true, “message”:”,”error”:”Job for network.service failed because the control process exited with error code.See `systemctl status network.service` and `journalctl -xe`” for

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

details.”}” on the screen after you perform the failover. You can ignore this message, as the Standby Node will continue to complete the upgrade process.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
Last login: Tue Apr 1 17:12:55 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...

Activating cluster.....100%
Cluster reconfiguration is done. Now you can upgrade another node.
Press enter to logout.
```

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: _
```

10. Press **Enter** to logout, then login again to access the HA Virtual Appliance Menu.

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

11. Enter **2** – [Show OV Cluster Status](#) and press **Enter** to display the HA Cluster Status. Verify that Standby Node (ov2) is now the Active Node and ov1 is now the Standby Node.

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

12. Click on **5 – Run Watchdog Command** on the HA Virtual Appliance Menu and press **Enter**.

```
*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option: █
```

13. Click on **2 – Display Status Of All Services** and press **Enter** to verify all services are running on the Active Node (formerly the Standby Node).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
(*) Type your option: 2
Would you like to run continuous status checking [y|n] (n): n
-----
Key Name                Display Name                Status
-----
ovactivemq              OmniVista ActiveMQ          Running
ovredis                 OmniVista Redis             Running
ovldap                  OmniVista OpenLDAP Server   Running
ovmongodb               OmniVista MongoDB           Running
ovpostgres              OmniVista Postgresql        Running
ovjetty                 OmniVista Jetty             Running
ovlog                   OmniVista Log Server        Running
ovdal                   OmniVista DAL Service       Running
ovtomcat                OmniVista Apache Tomcat     Running
ovnginx                 OmniVista Nginx             Running
ovscheduler             OmniVista Scheduler Service Running
ovftp                   OmniVista File Transfer Service Running
ovbyod                  OmniVista BYOD Service      Running
ovmasterpoller         OmniVista Primary Poller Service Running
ovag                    OmniVista AccessGuardian Service Running
ovav                    ..a Application Visibility Service Running
ovwireless              OmniVista Wireless Service  Running
ovmdns                  OmniVista mDNS Service      Running
ovresourcemanager      OmniVista Resource Manager Service Running
ovworkerpoller         OmniVista Worker Poller Service Running
ovclient                OmniVista Core Service      Running
ovanalytics             OmniVista Analytics Service Running
ovsflowcollector        OmniVista Sflow Collector Service Running
ovvxlan                 OmniVista VXLAN Service     Running
ovvlan                  OmniVista VLAN Service      Running
oviot                   OmniVista IoT Service       Running
ovvmmanager             OmniVista VM Manager Service Running
ovsip                   OmniVista SIP Service       Running
ovwma                   OmniVista WMA Service       Running
ovupam                  OmniVista UPAM Service      Running
ovradius                OmniVista Radius            Running
ovinfluxdb              OmniVista InfluxDB          Running
ovgrafana               OmniVista Grafana           Running
ovtelegraf              OmniVista Telegraf          Running
ovstatistics            OmniVista Statistics Service Running
ovbrightcloud           OmniVista Bright Cloud Service Running
ovzcs                   ..Vista Zigbee Controlling Service Running
ovucc                   OmniVista UCC Service       Running
*****
```

Note that when all services are up and running on the ov2 Node, you can proceed with upgrading the ov1 Node.

Connect to the ov1 Node and Upgrade the Node to 4.9R2

Note: During the Active Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. User-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are retained.

1. After the upgrade and failover process has completed on ov2 (now the Active Node), open a Console on the OV 2500 NMS 4.9R1 ov1 Node (now the Standby Node), which is already in Maintenance Mode.

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

3. **Important Note:** This step is required to successfully upgrade to the 4.9R2 release. **DO NOT SKIP THIS STEP FOR ANY REASON.** Enter **3 – To New Release** and press **Enter** to access the Upgrade to New Release menu, then enter **0 – Exit** and press **Enter** to return to the Upgrade VA Menu. Do not select the option to upgrade to 4.9R2.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R2
* [0] Exit
*****
(*) Type your option: █
    
```

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:

```

4. Enter **2** – **To 4.9R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter**. The Upgrade System Options Menu will appear.

```

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R1 GA
Build Number: 24
Patch Number: 0

Checking available packages for 4.9R1 operation is in progress...
Upgrade information for 4.9R1
Available Packages
Name       : ovmnse
Version    : 4.9R2
Release    : 13.0.e17
Architecture : x86_64
Size       : 3.0 G
Source     : ovmnse-4.9R2-13.0.e17.src.rpm
Repository : CustomRepo1_4.9R1
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
:
: WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may
o the next major release.

Would you like to upgrade the package [y/n] (n):

```

5. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

OmniVista detects the 4.9R2 build and displays the following message:

WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major release.

Enter **y** when asked “Would you like to upgrade the package” and press **Enter**. A warning message will appear asking you to proceed.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Would you like to upgrade the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release notes to this.
Are you ready to proceed ? [y/n] (n):
```

6. Enter **y** and press **Enter** to proceed with the upgrade to 4.9R2. The following message will appear, and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)...
```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```
[2025-04-08-17-29-09] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2025-04-08-17-29-09] [POST-UNINSTALL] Done

Verifying      : ovnmse-4.9R2-15.0.e17.x86_64      1/2
Verifying      : ovnmse-4.9R1-24.0.e17.x86_64      2/2

Upgraded:
  ovnmse-4.9R2-15.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [r] to reboot the system.
```

Note: Ignore the warning message and continue with the upgrade by rebooting the now current Standby Node (ov1).

8. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ou12hanode151 login: _
```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

9. Log into the VM. The following screen is displayed.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ou12hanode151 login: cliadmin
Password:
Last login: Mon Apr 14 15:45:10 on tty1
Reconfiguring cluster after upgrade...
Configuring cluster (step 1/1).....100%
Reconfiguring is completed. Press Enter ...
```

10. Press **Enter**, then login into the VM again to display the HA Virtual Appliance Menu.

```

Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

Hint: Num Lock on

ovl2hanode151 login: cliadmin
Password:
Last login: Mon Apr 14 16:49:48 on tty1

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

```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```

The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y|n] (n):

```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

12. When the upgrade of both ov1 and ov2 nodes to 4.9R2 is complete, the role of each node is reversed. The ov1 node that was initially the Active Node at the beginning of the upgrade process, is now the Standby Node and ov2 is now the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return ov1 to Active Node status, select **4** – **Configure Current Node** on the HA Virtual Appliance Menu and press **Enter** to bring up the Configure Cluster menu.

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

13. Select **15** – **Manual Failover** and press **Enter** to manually initiate a failover to the current Standby Node (ov1). The Standby Node will become the Active Node. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes). After the failover is complete, the services on ov1 will be running. The previously Active Node (ov2) will now be the Standby Node.

Verify the Upgrade

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

- Verify that all services are running on each node.

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.9R2. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

L3 High-Availability Upgrade Workflow

The basic steps for performing an L3 High-Availability upgrade are:

1. [Configure the Preemption and Keepalive Global Settings in OmniVista UI](#)

The Global Settings screen is used to configure Layer 3 Redundancy settings to support managed APs accessing a Layer 3 OmniVista High Availability installation.

2. [Upgrade the Active and Standby Nodes \(ov1 and ov2\) from 4.9R1 to 4.9R2](#)

Note: During the 4.9R1 to 4.9R2 upgrade time for an OmniVista High-Availability installation, OmniVista management functions remain available until the failover stage of the upgrade, at which time OmniVista is not available for approximately 5 to 10 minutes.

3. [Verify the cluster status to make sure data is in sync between the two nodes](#)
4. [Connect to the Active Node and enable Maintenance Mode](#)
5. [Connect to the Standby Node and upgrade the node to 4.9R2](#)
6. When the Standby Node upgrade is complete, do a reboot and failover. The Standby Node (ov2) is now the Active Node. Connect to the ov2 node and wait for all services to start.
7. [Connect to the previous Active Node \(ov1\) and upgrade the node to 4.9R2. Restart ov1 after the upgrade](#)
8. [Verify the Upgrade](#)

Note: After this upgrade process is complete, the Active Node at the beginning of the process is no longer the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return the node to Active Node status, you can do a manual failover on that node.

Configure Global Settings in the OmniVista UI

To ensure that APs connected to an L3 HA installation do not reboot when the ov2 Standby Node becomes the Active Node, configure the global Keepalive Interval and Preemption settings.

1. Go to the Global Settings screen in the OmniVista UI (Network > AP Registration > Global Setting) and configure the settings as shown here:

Global Setting

(*) indicates a required field

OV L3 Redundancy Setting

*Use AP Default OV L3 Redundancy Settings OFF *← If "On", click to turn off using AP Default OV L3 Redundancy Settings*

*IP Address Type: Static

*Secondary OVE Server IP Address: 10.255.221.20

*Keepalive Interval: 5 *← Set Keepalive Interval to "2"* Second(s)

*Retries: 3

*Preemption OFF *← If "On", click to turn off Preemption*

Apply

2. When you are finished setting the Keepalive Interval to "2" and disabling Preemption, click **Apply**.
3. Start the L3 HA upgrade process.

Upgrade the Active and Standby Nodes (ov1 and ov2) from 4.9R1 to 4.9R2

In this HA upgrade procedure, ov1 is initially the Active Node until the ov2 Standby Node is upgraded first. After ov2 is upgraded, the ov2 Node will become the Active Node and ov1 will become the Standby Node. This is a perfectly normal state of operation for OmniVista functions.

However, if you want to return ov1 to Active Node status, you can do a manual failover after both nodes are upgraded (see Step 13 in [Connect to the ov1 Node and Upgrade the Node to 4.9R2](#) for more details).

Verify the Cluster Status

Before you begin the process to upgrade the HA cluster from 4.9R1 to 4.9R2, verify that the Cluster Status is “Up to Date”. This can be performed on either node.

3. On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.
4. Begin the HA cluster upgrade from 4.9R1 to 4.9R2.

Enable Maintenance Mode on the Active Node (ov1)

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node (ov1). Open a Console on the OV 2500 NMS 4.9R1 ov1 Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y|n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
█
    
```

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

Connect to the Standby Node (ov2) and Upgrade the Node to 4.9R2

Note: During the Standby Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. However, any user-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are lost.

1. Open a Console on the OV 2500 NMS 4.9R1 Standby Node (ov2), which is already in Maintenance Mode.

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

3. **Important Note:** This step is required to successfully upgrade to the 4.9R2 release. **DO NOT SKIP THIS STEP FOR ANY REASON.** Enter **3 – To New Release** and press **Enter** to access the Upgrade to New Release menu, then enter **0 – Exit** and press **Enter** to return to the Upgrade VA Menu. Do not select the option to upgrade to 4.9R2.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R2
* [0] Exit
*****
(*) Type your option: █
    
```

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

4. Enter **2** – **To 4.9R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter**. The Upgrade System Options Menu will appear.

```

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R1 GA
Build Number: 24
Patch Number: 0

Checking available packages for 4.9R1 operation is in progress...
Upgrade information for 4.9R1
Available Packages
Name       : ovmnse
Version    : 4.9R2
Release    : 15.0.e17
Architecture : x86_64
Size       : 3.0 G
Source     : ovmnse-4.9R2-15.0.e17.src.rpm
Repository : CustomRepo1_4.9R1
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
           :
           : WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major
           : release.

Would you like to upgrade the package [y/n] (n): y
    
```

5. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

OmniVista detects the 4.9R2 build and displays the following message:

WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major release.

Enter **y** when asked “Would you like to upgrade the package” and press **Enter**. A warning message will appear asking you to proceed.

```

Would you like to upgrade the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release notes to this.
Are you ready to proceed ? [y/n] (n):
    
```

6. Enter **y** and press **Enter** to proceed with the upgrade to 4.9R2. The following message will appear, and the upgrade will begin.

```

Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)...
    
```

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```
[2025-04-08-17-29-09] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2025-04-08-17-29-09] [POST-UNINSTALL] Done

Verifying      : ovnmse-4.9R2-15.0.e17.x86_64      1/2
Verifying      : ovnmse-4.9R1-24.0.e17.x86_64      2/2

Upgraded:
  ovnmse-4.9R2-15.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [r] to reboot the system.
```

Note: Ignore the warning message and continue with the upgrade by rebooting the Standby Node (ov2).

8. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/18/2025
Technical Support Code: alcatel
activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: _
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

9. Login through the VA console. When prompted, press **Enter** to perform the failover. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
Last login: Tue Apr 1 17:12:55 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
_
```

Note: If you are upgrading the Standby Node to 4.9R2 from 4.7R1 or older, you may see the message “{“Status”:true, “message”:””, “error”:”Job for network.service failed because the control process exited with error code.See ‘systemctl status network.service’ and ‘journalctl -xe’ for details.”}” on the screen after you perform the failover. You can ignore this message, as the Standby Node will continue to complete the upgrade process.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: cliadmin
Password:
Last login: Tue Apr 1 17:12:55 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...

Activating cluster.....100%
Cluster reconfiguration is done. Now you can upgrade another node.
Press enter to logout.
```

10. Press **Enter** to logout, then login again to access the HA Virtual Appliance Menu.

Note: After the failover, ov2 becomes the new Active Node and ov1 (the new Standby Node) is restarted.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

l2hanode152 login: _
```

```

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

11. Enter **2** – [Show OV Cluster Status](#) and press **Enter** to display the HA Cluster Status. Verify that Standby Node (ov2) is now the Active Node and ov1 is now the Standby Node.

```

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

12. Click on **5** – **Run Watchdog** Command on the HA Virtual Appliance Menu and press **Enter**.

```

*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option: █
    
```

13. Click on **2 – Display Status Of All Services** and press **Enter** to verify all services are running on the Active Node (formerly the Standby Node).

```

*****
(*) Type your option: 2
Would you like to run continuous status checking [y|n] (n): n
Key Name                Display Name                Status
-----
ovactivemq              OmniVista ActiveMQ          Running
ovredis                 OmniVista Redis             Running
ovldap                  OmniVista OpenLDAP Server   Running
ovmongodb               OmniVista MongoDB           Running
ovpostgres              OmniVista PostgreSQL        Running
ovjetty                  OmniVista Jetty              Running
ovlog                    OmniVista Log Server         Running
ovdal                    OmniVista DAL Service        Running
ovtomcat                 OmniVista Apache Tomcat     Running
ovnginx                  OmniVista Nginx              Running
ovscheduler              OmniVista Scheduler Service  Running
ovftplib                 OmniVista File Transfer Service Running
ovbyod                   OmniVista BYOD Service       Running
ovmasterpoller          OmniVista Primary Poller Service Running
ovag                      OmniVista AccessGuardian Service Running
ovav                      ...a Application Visibility Service Running
ovwireless               OmniVista Wireless Service   Running
ovmdns                   OmniVista mDNS Service       Running
ovresourcemanager        OmniVista Resource Manager Service Running
ovworkerpoller           OmniVista Worker Poller Service Running
ovclient                 OmniVista Core Service       Running
ovanalytics              OmniVista Analytics Service  Running
ovsflowcollector         OmniVista Sflow Collector Service Running
ovvxlan                  OmniVista VXLAN Service       Running
ovvlan                    OmniVista VLAN Service       Running
oviot                     OmniVista IoT Service         Running
ovvmmanager              OmniVista VM Manager Service  Running
ovsip                     OmniVista SIP Service         Running
ovwma                     OmniVista WMA Service         Running
ovupam                    OmniVista UPAM Service        Running
ovradius                  OmniVista Radius              Running
ovinfluxdb                OmniVista InfluxDB            Running
ovgrafana                 OmniVista Grafana             Running
ovtelegraf                OmniVista Telegraf            Running
ovstatistics              OmniVista Statistics Service  Running
ovbrightcloud             OmniVista Bright Cloud Service Running
ovzcs                      ...Vista Zigbee Controlling Service Running
ovucc                     OmniVista UCC Service         Running
*****

```

Note that when all services are up and running on the ov2 Node, you can proceed with upgrading the ov1 Node.

Connect to the ov1 Node and Upgrade the Node to 4.9R2

Note: During the Active Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. User-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are retained.

1. After the upgrade and failover process has completed on ov2 (now the Active Node), open a Console on the OV 2500 NMS 4.9R1 ov1 Node (now the Standby Node), which is already in Maintenance Mode.

```

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

Note: Upgrading the ov1 Node requires stopping the OmniVista ActiveMQ (ovactivemq) service before beginning the upgrade process. You must stop this service immediately after the ov2 Node upgrade is completed and all services are running on ov2 Node. This helps to avoid the possibility of APs rebooting and attempting to connect to the ov1 Node if they see the “ovactivemq” service running on ov1 Node.

2. To verify that the “ovactivemq” service is running, click on **5 – Run Watchdog Command** on the HA Virtual Appliance Menu and press **Enter**.

```

*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option: █
    
```

3. Click on **2 – Display Status Of All Services** and press **Enter**. Check the list of all services to verify that the “ovactivemq” service is running.

```

*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option: 7
(*) Please input service name: ovactivemq
Would you like to stop with stop-tree option [y/n] (n): n
Are you sure you want to stop ovactivemq [y/n] (n): y

```

4. To stop the “ovactivemq” service, click on **7 – Stop a Service** on the Run Watchdog Command menu and press **Enter**.

When prompted, enter the service name “ovactivemq”, and press **Enter**.

Enter **n** when asked “Would you like to stop with stop-tree option” and press **Enter**.

Enter **y** to confirm stopping the “ovactivemq” service and press **Enter**.

5. Verify that the status of the “ovactivemq” service is “Stopped”. To check the services status, click on **2 – Display Status Of All Services** on the Run Watchdog Command menu and press **Enter**.
6. Wait about 10-15 minutes to see all APs and connected clients in "UP" status in new active node OmniVista UI, then start the upgrade process.
7. On the HA Virtual Appliance Menu, select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:

```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

8. **Important Note:** This step is required to successfully upgrade to the 4.9R2 release. **DO NOT SKIP THIS STEP FOR ANY REASON.** Enter **3 – To New Release** and press **Enter** to access the Upgrade to New Release menu, then enter **0 – Exit** and press **Enter** to return to the Upgrade VA Menu. Do not select the option to upgrade to 4.9R2.

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R2
* [0] Exit
*****
(*) Type your option: _
```

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.9R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
```

9. Enter **2 – To 4.9R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter**. The Upgrade System Options Menu will appear.

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R1 GA
Build Number: 24
Patch Number: 0

Checking available packages for 4.9R1 operation is in progress...
Upgrade information for 4.9R1
Available Packages
Name       : ovmse
Version    : 4.9R2
Release    : 13.0.e17
Architecture : x86_64
Size       : 3.0 G
Source     : ovmse-4.9R2-13.0.e17.src.rpm
Repository : CustomRepo1_4.9R1
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
           :
           : WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may
           : o the next major release.

Would you like to upgrade the package [y/n] (n): _
```

10. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You **must** select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is **not** supported.

Note: If you see the following error message after selecting the option to download and upgrade, then you need to wait a longer time for services to come up on ov1.

```
*****
* [1] Help
* [2] Download and Upgrade
* [3] Download Only
* [4] Upgrade from downloaded package
* [0] Exit
*****
(*) Type your option: 2
*****
Please make sure data is fully synchronized between 2 nodes before continue. You can check it in "Show cluster status" menu.
Press [Enter] to continue
*****
```

OmniVista detects the 4.9R2 build and displays the following message:

WARNING: The packages belong to 4.9R2. In certain instances, proceeding with the patch upgrade may lead to an automatic upgrade to the next major release.

Enter **y** when asked “Would you like to upgrade the package” and press **Enter**. A warning message will appear asking you to proceed.

```
Would you like to upgrade the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release notes to this.
Are you ready to proceed ? [y/n] (n):
```

11. Enter **y** and press **Enter** to proceed with the upgrade to 4.9R2. The following message will appear, and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)...
```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
[2025-04-08-17-29-09] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2025-04-08-17-29-09] [POST-UNINSTALL] Done

Verifying      : ovnmse-4.9R2-15.0.e17.x86_64          1/2
Verifying      : ovnmse-4.9R1-24.0.e17.x86_64          2/2

Upgraded:
  ovnmse-4.9R2-15.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [r] to reboot the system.
```

Note: Ignore the warning message and continue with the upgrade by rebooting the now current Standby Node (ov1).

13. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov12hanode151 login: _
```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

14. Log into the VM. The following screen is displayed.

```
Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov12hanode151 login: cliadmin
Password:
Last login: Mon Apr 14 15:45:10 on tty1
Reconfiguring cluster after upgrade...
Configuring cluster (step 1/1).....100%
Reconfiguring is completed. Press Enter ...
```

15. Press **Enter**, then log into the VM again to display the HA Virtual Appliance Menu.

```

Oracle Linux Server 8.10
Kernel 4.18.0-553.45.1.el8_10.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.9R2 GA
Build Number: 15
Patch Number: 0
Build Date: 04/10/2025
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

Hint: Num Lock on

ovl2hanode151 login: cliadmin
Password:
Last login: Mon Apr 14 16:49:48 on tty1

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

```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```

The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y|n] (n):

```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

17. When the upgrade of both ov1 and ov2 nodes to 4.9R2 is complete, the role of each node is reversed. The ov1 node that was initially the Active Node at the beginning of the upgrade process, is now the Standby Node and ov2 is now the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return ov1 to Active Node status, select **4** – **Configure Current Node** on the HA Virtual Appliance Menu and press **Enter** to bring up the Configure Cluster menu.

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

18. Select **15** – **Manual Failover** and press **Enter** to manually initiate a failover to the current Standby Node (ov1). The Standby Node will become the Active Node. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes). After the failover is complete, the services on ov1 will be running. The previously Active Node (ov2) will now be the Standby Node.

Verify the Upgrade

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

- Verify that all services are running on each node.

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.9R2. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Upgrading from 4.8R2 to 4.9R1

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.8R2 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.9R1 Standalone or High-Availability Installation.

Important Notes:

- During the upgrade time for an OmniVista Standalone installation, OmniVista is not available for any management functions. There is no impact to the deployed network during the OmniVista upgrade. Managed devices (Switch/AP) and existing device clients will continue to function as before. However, new clients cannot join the network if the Switch/AP is configured to do authentication from UPAM. The upgrade downtime may last between one and four hours and starts when the Maintenance Mode is enabled.
- When one of the nodes in an HA cluster becomes faulty, it can be decommissioned and replaced with a new node. While the HA is running in single node mode, prepare the new node, extend its data partition size as needed to match that of the old node, then join the new node to the cluster.
- It is recommended that you make note of your IP and NIC configurations before initiating a Standalone or HA upgrade to 4.9R1. Depending on the NIC types and hypervisor version, some special cases may require you to reconfigure these settings during or immediately after the upgrade to 4.9R1. If necessary, the VA will prompt you to perform the reconfiguration.
- You must perform the OmniVista upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client, upgrading the installation can result in incomplete upgrades and missing any pending actions, such as pressing the enter key to continue the upgrade.

Upgrading from 4.8R2 Standalone to 4.9R1 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.8R2 Standalone Installation to an OV 2500 NMS 4.9R1 Standalone Installation.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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 OmniVista makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

1. Open a Console on the OV 2500 NMS 4.8R2 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: 4
```

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to "ALE Central Repo", then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the Virtual Appliance Menu, then select **9 - Configure Proxy**.

3. Enter **3 – To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R1
* [0] Exit
*****
(*) Type your option:
    
```

4. Enter **1 – Upgrade to 4.9R1** and press **Enter**. The Upgrade System Options Screen will appear.

```

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 40
Patch Number: 0

Checking available packages for 4.8R2 operation is in progress...
Upgrade to 4.8R2 release is available after upgrading latest to version/patch of
4.8R1 release
Do you want to continue to check upgrade for 4.8R1 release now [y|n] (n): █
    
```

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You **must** select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is **not** supported.

Enter **y** when asked “Do you want to continue to check upgrade for 4.9R1 release now” and press **Enter**.

```
Getting upgrade information for 4.8R2...
Upgrade information for 4.8R2
Available Packages
Name       : ovmnse
Version    : 4.8R2
Release    : 17.0.el7
Architecture : x86_64
Size       : 2.1 G
Source     : ovmnse-4.8R2-17.0.el7.src.rpm
Repository : CustomRepo1_4.8R2
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 chosen to upgrade to latest build of 4.8R2 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): █
```

6. Enter **y** and press **Enter**. A warning message will then appear asking you to proceed.

```
You have chosen to upgrade to latest build of 4.8R2 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot before upgrading.
Are you ready to proceed ? [y|n] (n): y
```

7. Enter **y** and press **Enter** to proceed with the upgrade. The following message will appear, and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)...
```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

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

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

8. When the installation is complete, the following prompt will appear: “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

9. Log into the VM. The Virtual Appliance Menu will appear.

```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```

The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [y|n] (n):
    
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

5. Enter **y** and press **Enter** to power off the VM.
6. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
7. Power on the VM.
8. Extend the data partition on the second hard disk.
 - On the Configure the Virtual Appliance Menu, select **9 – Configure Network Size**, then select **4 – Extend Data Partition**.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

10. Verify the update to 4.9R1.

- Verify that all services have started.
 - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.

- Select option **3 – Run Watchdog** Command, then select option **2 – Display Status of All Services**. See [Run Watchdog Command](#) for more details.
- Verify that the Build Number is correct.
 - From The Virtual Appliance Menu, select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See [Display Current Configuration](#) for more details.
- Verify that you can [launch the OmniVista UI](#) and successfully login.
- Take a VM Snapshot of the current OmniVista VA and remove previous VA snapshots.

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.9R1.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 6. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance.**
 7. **Select 2 - Display Current Configuration** to verify your currently configured network size (e.g., Low, Medium, High).
 8. **Select 9 - Configure Network Size.**
 9. **Select 2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
 10. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.8R2 HA to 4.9R1 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.8R2 High-Availability Installation to an OV 2500 NMS 4.9R1 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OmniVista 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 **4 - Configure Current Node** on the Virtual Appliance Menu, then select **9 - Configure Proxy**.

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

High-Availability Upgrade Workflow

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

1. [Upgrade the Active and Standby Nodes \(ov1 and ov2\) from 4.8R2 to 4.9R1](#)

Note: During the 4.8R2 to 4.9R1 upgrade time for an OmniVista High-Availability installation, OmniVista management functions remain available until the failover stage of the upgrade, at which time OmniVista is not available for approximately 5 to 10 minutes.

2. [Verify the cluster status to make sure data is in sync between the two nodes.](#)

3. [Connect to the Active Node and enable Maintenance Mode](#)

4. [Connect to the Standby Node and upgrade the node to 4.9R1](#)

5. When the Standby Node upgrade is complete, do a reboot and failover. The Standby Node (ov2) is now the Active Node. Connect to the ov2 node and wait for all services to start.
6. [Connect to the previous Active Node \(ov1\) and upgrade the node to 4.9R1. Restart ov1 after the upgrade](#)
7. [Verify the Upgrade](#)

Note: After this upgrade process is complete, the Active Node at the beginning of the process is no longer the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return the node to Active Node status, you can do a manual failover on that node.

Upgrade the Active and Standby Nodes (ov1 and ov2) from 4.8R2 to 4.9R1

In this HA upgrade procedure, ov1 is initially the Active Node until the ov2 Standby Node is upgraded first. After ov2 is upgraded, the ov2 Node will become the Active Node and ov1 will become the Standby Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return ov2 to Active Node status, you can do a manual failover after both nodes are upgraded (see Step 12 in [Connect to the ov1 Node and Upgrade the Node to 4.8R2](#) for more details).

Verify the Cluster Status

Before you begin the process to upgrade the HA cluster from 4.8R2 to 4.9R1, verify that the Cluster Status is “Up to Date”. This can be performed on either node.

5. On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.
6. Begin the HA cluster upgrade from 4.8R2 to 4.9R1.

Enable Maintenance Mode on the Active Node (ov1)

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node (ov1). Open a Console on the OV 2500 NMS 4.8R2 ov1 Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make
sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y|n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance
Mode!!!
Press [Enter] to continue
█
    
```

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

Connect to the Standby Node (ov2) and Upgrade the Node to 4.9R1

Note: During the Standby Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. However, any user-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are lost.

1. Open a Console on the OV 2500 NMS 4.8R2 Standby Node (ov2), which is already in Maintenance Mode.

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R1
* [0] Exit
*****
(*) Type your option: █
    
```

4. Enter **1 - Upgrade to 4.9R1** and press **Enter**.

```

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

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```

=====IMPORTANT:=====
You must start upgrade on the standby node first node.
Press [Enter] to continue

After standby node upgraded. You could upgrade active node.
Press [Enter] to continue

=====
Are you sure want to continue?[y|n] (n): y
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 40
Patch Number: 0

Checking available packages for 4.8R2 operation is in progress...
Upgrade to 4.8R2 release is available after upgrading latest to version/patch of 4.8R1 release
Do you want to continue to check upgrade for 4.8R1 release now [y|n] (n):
    
```

6. Click **y** when asked to check upgrade for 4.9R1 release now.

```

Getting upgrade information for 4.8R1...
Current version of Virtual Appliance is the latest build of 4.8R1

Getting upgrade information for 4.8R2...
Upgrade information for 4.8R2
Available Packages
Name      : ovmnse
Version   : 4.8R2
Release   : 21.0.e17
Architecture : x86_64
Size      : 2.0 G
Source    : ovmnse-4.8R2-21.0.e17.src.rpm
Repository : CustomRepo1_4.8R2
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 chosen to upgrade to latest build of 4.8R2 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore em.
Press any key to continue the upgrade (13s)...
    
```

7. Click **y** and press **Enter** after “Do you want to continue with the upgrade now?” and “Are you ready to proceed?”

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```
[2024-01-09-23-05-22] [PRE-UNINSTALL] Begin...
[2024-01-09-23-05-22] [PRE-UNINSTALL] Done

Cleanup          : ovmse-4.8R1-40.0.e17.x86_64          2/2
Running scriptlet: ovmse-4.8R1-40.0.e17.x86_64          2/2

[2024-01-09-23-05-24] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2024-01-09-23-05-24] [POST-UNINSTALL] Done

Verifying        : ovmse-4.8R2-21.0.e17.x86_64          1/2
Verifying        : ovmse-4.8R1-40.0.e17.x86_64          2/2

Upgraded:
  ovmse-4.8R2-21.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
Press [r] to reboot the system.
```

9. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```

Oracle Linux Server 8.7
Kernel 4.18.0-425.3.1.el8.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 EA
Build Number: 34
Patch Number: 0
Build Date: 07/12/2023
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov140node2 login: cliadmin
Password:
Last login: Mon Jul 10 11:59:57 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...

```

Note: You can ignore the message “Activate the web console with: systemctl enable –now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

10. Login through the VA console. When prompted, press **Enter** to perform the failover. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes).

```

Activate the web console with: systemctl enable --now cockpit.socket
Last login: Fri Jul 14 13:19:50 2023
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
Activating cluster IPs.....100%
Cluster reconfiguration is done. Now you can upgrade another node.
Press enter to logout.

```

Note: If you are upgrading the Standby Node to 4.9R1 from 4.7R1 or older, you may see the message “{“Status”:true, “message”:””, “error”:”Job for network.service failed because the control process exited with error code.See `systemctl status network.service` and `journalctl -xe` for details.”}” on the screen after you perform the failover. You can ignore this message, as the Standby Node will continue to complete the upgrade process.

11. Press **Enter** to logout, then login again to access the HA Virtual Appliance Menu.

```

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

12. Enter **2** – **Show OV Cluster Status** and press **Enter** to display the HA Cluster Status.

```

Cluster Status:
Node      Hostname  Ip Address  Role    Status
Current   ov1       10.255.221.27 Active
Peer      ov2       10.255.221.28 Online
Data sync: Up to Date
    
```

13. Verify that Standby Node (ov1) is now the Active Node and ov2 is now the Standby Node.

```

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

14. Click on **5** – **Run Watchdog** Command on the HA Virtual Appliance Menu and press **Enter**.

```

*****
* 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 *
* [10] Choose Service Profile *
* [0] Exit *
*****
(*) Type your option: █
    
```

15. Click on **2 – Display Status Of All Services** and press **Enter** to verify all services are running on the Active Node (formerly the Standby Node).

```

*****
(*) Type your option: 2
Would you like to run continuous status checking [y|n] (n): n
Key Name                Display Name                Status
-----
ovactivemq              OmniVista ActiveMQ          Running
ovredis                 OmniVista Redis             Running
ovldap                  OmniVista OpenLDAP Server   Running
ovmongodb                OmniVista MongoDB           Running
ovpostgres              OmniVista Postgresql        Running
ovjetty                  OmniVista Jetty             Running
ovlog                    OmniVista Log Server        Running
ovdal                    OmniVista DAL Service       Running
ovtomcat                 OmniVista Apache Tomcat     Running
ovnginx                  OmniVista Nginx             Running
ovscheduler              OmniVista Scheduler Service Running
ovftp                    OmniVista File Transfer Service Running
ovbyod                   OmniVista BYOD Service      Running
ovmasterpoller          OmniVista Primary Poller Service Running
ovag                      OmniVista AccessGuardian Service Running
ovav                      ...a Application Visibility Service Running
ovwireless               OmniVista Wireless Service  Running
ovmdns                   OmniVista mDNS Service      Running
ovresourcemanager        OmniVista Resource Manager Service Running
ovworkerpoller          OmniVista Worker Poller Service Running
ovclient                 OmniVista Core Service      Running
ovanalytics              OmniVista Analytics Service  Running
ovsflowcollector         OmniVista Sflow Collector Service Running
ovvxlan                  OmniVista VXLAN Service     Running
ovvlan                   OmniVista VLAN Service      Running
oviot                     OmniVista IoT Service       Running
ovvmmanager              OmniVista VM Manager Service Running
ovsip                     OmniVista SIP Service       Running
ovwma                     OmniVista WMA Service       Running
ovupam                   OmniVista UPAM Service      Running
ovradius                 OmniVista Radius            Running
ovinfluxdb               OmniVista InfluxDB          Running
ovgrafana                OmniVista Grafana           Running
ovtelegraf               OmniVista Telegraf          Running
ovstatistics             OmniVista Statistics Service Running
ovbrightcloud            OmniVista Bright Cloud Service Running
ovzcs                     ...Vista Zigbee Controlling Service Running
ovucc                     OmniVista UCC Service       Running
*****
    
```

Note that when all services are up and running on the ov2 Node, you can proceed with upgrading the ov1 Node.

Connect to the Active Node (ov1) and Upgrade the Node to 4.9R1

Note: During the Active Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. User-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are retained.

11. After the upgrade and failover process has completed on ov2 (now the Active Node), open a Console on the OV 2500 NMS 4.8R2 ov1 Node (now the Standby Node), which is already in Maintenance Mode.

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

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.9R1
* [0] Exit
*****
(*) Type your option:
    
```

14. Enter **1 - Upgrade to 4.9R1** and press **Enter**.

```

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

15. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.9R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```

=====IMPORTANT:=====
You must start upgrade on the standby node first node.
Press [Enter] to continue

After standby node upgraded. You could upgrade active node.
Press [Enter] to continue

=====
Are you sure want to continue?[y|n] (n): y
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 40
Patch Number: 0

Checking available packages for 4.8R2 operation is in progress...
Upgrade to 4.8R2 release is available after upgrading latest to version/patch of 4.8R1 release
Do you want to continue to check upgrade for 4.8R1 release now [y|n] (n):
    
```

16. Click **y** when asked to check upgrade for 4.9R1 release now.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Setting upgrade information for 4.8R1...
Current version of Virtual Appliance is the latest build of 4.8R1

Getting upgrade information for 4.8R2...
Upgrade information for 4.8R2
Available Packages
Name       : ovmnse
Version   : 4.8R2
Release   : 21.0.e17
Architecture : x86_64
Size      : 2.0 G
Source    : ovmnse-4.8R2-21.0.e17.src.rpm
Repository : CustomRepo1_4.8R2
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 chosen to upgrade to latest build of 4.8R2 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

17. Click **y** and press **Enter** after “Do you want to continue with the upgrade now?” and “Are you ready to proceed?”.

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```
[2024-01-09-23-05-22] [PRE-UNINSTALL] Begin...
[2024-01-09-23-05-22] [PRE-UNINSTALL] Done

Cleanup           : ovmnse-4.8R1-40.0.e17.x86_64           2/2
Running scriptlet: ovmnse-4.8R1-40.0.e17.x86_64           2/2

[2024-01-09-23-05-24] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2024-01-09-23-05-24] [POST-UNINSTALL] Done

Verifying         : ovmnse-4.8R2-21.0.e17.x86_64           1/2
Verifying         : ovmnse-4.8R1-40.0.e17.x86_64           2/2

Upgraded:
  ovmnse-4.8R2-21.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
Press [r] to reboot the system.
```

19. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
Oracle Linux Server 8.7
Kernel 4.18.0-425.3.1.el8.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 EA
Build Number: 34
Patch Number: 0
Build Date: 07/12/2023
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov140node2 login: cliadmin
Password:
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y|n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.

3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The HA Virtual Appliance Menu is displayed.

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

21. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See [Display Current Node Configuration](#) for more details.
22. When the upgrade of both OV-1 and OV-2 nodes to 4.9R1 is complete, the role of each node is reversed. The OV-1 node that was the Active Node at the beginning of the upgrade process, is now the Standby Node and OV-2 is now the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return OV-2 to Active Node status, select **4 – Configure Current Node** on the HA Virtual Appliance Menu and press **Enter** to bring up the Configure Cluster menu.

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

- 23.** Select **15 – Manual Failover** and press **Enter** to manually initiate a failover to the current Standby Node (OV-1). The Standby Node will become the Active Node. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes). After the failover is complete, the services on OV-1 will be running. The previously Active Node (OV-2) will now be the Standby Node.

Verify the Upgrade

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

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.8R2. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Upgrading from 4.8R1 to 4.8R2

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.8R1 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.8R2 Standalone or High-Availability Installation.

Important Notes:

- During the upgrade time for an OmniVista Standalone installation, OmniVista is not available for any management functions. There is no impact to the deployed network during the OmniVista upgrade. Managed devices (Switch/AP) and existing device clients will continue to function as before. However, new clients cannot join the network if the Switch/AP is configured to do authentication from UPAM. The upgrade downtime may last between one and four hours and starts when the Maintenance Mode is enabled.
- When one of the nodes in an HA cluster becomes faulty, it can be decommissioned and replaced with a new node. While the HA is running in single node mode, prepare the new node, extend its data partition size as needed to match that of the old node, then join the new node to the cluster.
- It is recommended that you make note of your IP and NIC configurations before initiating a Standalone or HA upgrade to 4.8R2. Depending on the NIC types and hypervisor version, some special cases may require you to reconfigure these settings during or immediately after the upgrade to 4.8R2. If necessary, the VA will prompt you to perform the reconfiguration.
- You must perform the OmniVista upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client, upgrading the installation can result in incomplete upgrades and missing any pending actions, such as pressing the enter key to continue the upgrade.

Upgrading from 4.8R1 Standalone to 4.8R2 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.8R1 Standalone Installation to an OV 2500 NMS 4.8R2 Standalone Installation.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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 OmniVista makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages.** The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

1. Open a Console on the OV 2500 NMS 4.8R1 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: 4
```

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. OmniVista makes an HTTPS connection to the external repository for software upgrades. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
    
```

3. Enter **3 – To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.8R2
* [0] Exit
*****
(*) Type your option: █
    
```

4. Enter **1 – Upgrade to 4.8R2** and press **Enter**. The Upgrade System Options Screen will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 40
Patch Number: 0

Checking available packages for 4.8R2 operation is in progress...
Upgrade to 4.8R2 release is available after upgrading latest to version/patch of
4.8R1 release
Do you want to continue to check upgrade for 4.8R1 release now [y/n] (n): █
```

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.8R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

Enter **y** when asked “Do you want to continue to check upgrade for 4.8R1 release now” and press **Enter**.

```
Getting upgrade information for 4.8R2...
Upgrade information for 4.8R2
Available Packages
Name       : ovmnse
Version    : 4.8R2
Release    : 17.0.el7
Architecture : x86_64
Size       : 2.1 G
Source     : ovmnse-4.8R2-17.0.el7.src.rpm
Repository : CustomRepo1_4.8R2
Summary    : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL        : http://enterprise.alcatel-lucent.com/?product=OmniVista2500Networ
kManagementSystem&page=overview
License    : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.8R2 release. Please refer to Rel
ease Notes and Installation Guide of the new release before continuing with this
upgrade
Do you want to continue with upgrade now ?[y/n] (n): █
```

6. Enter **y** and press **Enter**. A warning message will then appear asking you to proceed.

```
You have chosen to upgrade to latest build of 4.8R2 release. Please refer to Rele
Do you want to continue with upgrade now ?[y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snaps
Are you ready to proceed ? [y/n] (n): y
```

7. Enter **y** and press **Enter** to proceed with the upgrade. The following message will appear, and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RP
Press any key to continue the upgrade (3s)...
```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

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

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

- When the installation is complete, the following prompt will appear: “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.
- Log into the VM. The Virtual Appliance Menu will appear.

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OU VM using
hypervisor and then power on the OU 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [y|n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the Configure the Virtual Appliance Menu, select **9 – Configure Network Size**, then select **4 – Extend Data Partition**.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

10. Verify the update to 4.8R2.
 - Verify that all services have started.
 - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
 - Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See [Run Watchdog Command](#) for more details.
 - Verify that the Build Number is correct.
 - From The Virtual Appliance Menu, select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See [Display Current Configuration](#) for more details.
 - Verify that you can [launch the OmniVista UI](#) and successfully login.
 - Take a VM Snapshot of the current OmniVista VA and remove previous VA snapshots.

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPaddress>` in a supported browser to launch OV 2500 NMS 4.8R2. **Once OmniVista is launched, do a hard refresh (Shift+F5) of your browser window to ensure the display of the latest UI.**

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance.**
 2. **Select 2 - Display Current Configuration** to verify your currently configured network size (e.g., Low, Medium, High).
 3. **Select 9 - Configure Network Size.**

4. Select **2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.8R1 HA to 4.8R2 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.8R1 High-Availability Installation to an OV 2500 NMS 4.8R2 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA on both the Active and Standby nodes. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OmniVista 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 **4 - Configure Current Node** on the Virtual Appliance Menu, then select **9 - Configure Proxy**.

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages.** The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

High-Availability Upgrade Workflow

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

1. [Upgrade the Active and Standby Nodes \(ov1 and ov2\) from 4.8R1 to 4.8R2](#)

Note: During the 4.8R1 to 4.8R2 upgrade time for an OmniVista High-Availability installation, OmniVista management functions remain available until the failover stage of the upgrade, at which time OmniVista is not available for approximately 5 to 10 minutes.

2. [Verify the cluster status to make sure data is in sync between the two nodes.](#)

3. [Connect to the Active Node and enable Maintenance Mode](#)

4. [Connect to the Standby Node and upgrade the node to 4.8R2](#)

5. When the Standby Node upgrade is complete, do a reboot and failover. The Standby Node (ov2) is now the Active Node. Connect to the ov2 node and wait for all services to start.

6. [Connect to the previous Active Node \(ov1\) and upgrade the node to 4.8R2. Restart ov1 after the upgrade](#)

7. [Verify the Upgrade](#)

Note: After this upgrade process is complete, the Active Node at the beginning of the process is no longer the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return the node to Active Node status, you can do a manual failover on that node.

Upgrade the Active and Standby Nodes (ov1 and ov2) from 4.8R1 to 4.8R2

In this HA upgrade procedure, ov1 is initially the Active Node until the ov2 Standby Node is upgraded first. After ov2 is upgraded, the ov2 Node will become the Active Node and ov1 will become the Standby Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return ov2 to Active Node status, you can do a manual failover after both nodes are upgraded (see Step 12 in [Connect to the ov1 Node and Upgrade the Node to 4.8R2](#) for more details).

Verify the Cluster Status

Before you begin the process to upgrade the HA cluster from 4.8R1 to 4.8R2, verify that the Cluster Status is “Up to Date”. This can be performed on either node.

1. On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.
2. Begin the HA cluster upgrade from 4.8R1 to 4.8R2.

Enable Maintenance Mode on the Active Node (ov1)

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node (ov1). Open a Console on the OV 2500 NMS 4.8R1 ov1 Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

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

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

```
If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make
sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y|n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance
Mode!!!
Press [Enter] to continue
█
```

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

Connect to the Standby Node (ov2) and Upgrade the Node to 4.8R2

Note: During the Standby Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. However, any user-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are lost.

5. Open a Console on the OV 2500 NMS 4.8R1 Standby Node (ov2), which is already in Maintenance Mode.

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.8R2
* [0] Exit
*****
(*) Type your option: █
    
```

8. Enter **1 - Upgrade to 4.8R2** and press **Enter**.

```

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

9. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.8R2 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```

=====IMPORTANT:=====
You must start upgrade on the standby node first node.
Press [Enter] to continue

After standby node upgraded. You could upgrade active node.
Press [Enter] to continue

=====
Are you sure want to continue?[y|n] (n): y
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 40
Patch Number: 0

Checking available packages for 4.8R2 operation is in progress...
Upgrade to 4.8R2 release is available after upgrading latest to version/patch of 4.8R1 release
Do you want to continue to check upgrade for 4.8R1 release now [y|n] (n):

```

10. Click **y** when asked to check upgrade for 4.8R1 release now.

```

Getting upgrade information for 4.8R1...
Current version of Virtual Appliance is the latest build of 4.8R1

Getting upgrade information for 4.8R2...
Upgrade information for 4.8R2
Available Packages
Name       : ovmnse
Version    : 4.8R2
Release    : 21.0.e17
Architecture : x86_64
Size       : 2.0 G
Source     : ovmnse-4.8R2-21.0.e17.src.rpm
Repository : CustomRepo1_4.8R2
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 chosen to upgrade to latest build of 4.8R2 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...

```

11. Click **y** and press **Enter** after “Do you want to continue with the upgrade now?” and “Are you ready to proceed?”

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
[2024-01-09-23-05-22] [PRE-UNINSTALL] Begin...
[2024-01-09-23-05-22] [PRE-UNINSTALL] Done

Cleanup          : ovmse-4.8R1-40.0.e17.x86_64          2/2
Running scriptlet: ovmse-4.8R1-40.0.e17.x86_64          2/2

[2024-01-09-23-05-24] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2024-01-09-23-05-24] [POST-UNINSTALL] Done

Verifying       : ovmse-4.8R2-21.0.e17.x86_64          1/2
Verifying       : ovmse-4.8R1-40.0.e17.x86_64          2/2

Upgraded:
  ovmse-4.8R2-21.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
Press [r] to reboot the system.
```

13. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
Oracle Linux Server 8.7
Kernel 4.18.0-425.3.1.el8.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 EA
Build Number: 34
Patch Number: 0
Build Date: 07/12/2023
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov140mode2 login: cliadmin
Password:
Last login: Mon Jul 10 11:59:57 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
-
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

14. Login through the VA console. When prompted, press **Enter** to perform the failover. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Activate the web console with: systemctl enable --now cockpit.socket
Last login: Fri Jul 14 13:19:50 2023
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
Activating cluster IPs.....100%
Cluster reconfiguration is done. Now you can upgrade another node.
Press enter to logout.
```

Note: If you are upgrading the Standby Node to 4.8R2 from 4.7R1 or older, you may see the message “{“Status”:true, “message”:””, “error”:”Job for network.service failed because the control process exited with error code. See ‘systemctl status network.service’ and ‘journalctl -xe’ for details.”}” on the screen after you perform the failover. You can ignore this message, as the Standby Node will continue to complete the upgrade process.

15. Press **Enter** to logout, then login again to access the HA Virtual Appliance Menu.

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

16. Enter **2** – **Show OV Cluster Status** and press **Enter** to display the HA Cluster Status.

```
Cluster Status:
Node   Hostname  Ip Address   Role   Status
Current ov1       10.255.221.27 Active
Peer   ov2       10.255.221.28 Online
Data sync: Up to Date
```

17. Verify that Standby Node (ov2) is now the Active Node and ov1 is now the Standby Node.

```

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

18. Click on **5 – Run Watchdog** Command on the HA Virtual Appliance Menu and press **Enter**.

```

*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option: █
    
```

19. Click on **2 – Display Status Of All Services** and press **Enter** to verify all services are running on the Active Node (formerly the Standby Node).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
(*) Type your option: 2
Would you like to run continuous status checking [y|n] (n): n
-----
Key Name                Display Name                Status
-----
ovactivemq              OmniVista ActiveMQ          Running
ovredis                 OmniVista Redis             Running
ovldap                  OmniVista OpenLDAP Server   Running
ovmongodb               OmniVista MongoDB           Running
ovpostgres              OmniVista Postgresql        Running
ovjetty                 OmniVista Jetty             Running
ovlog                   OmniVista Log Server        Running
ovdal                   OmniVista DAL Service       Running
ovtomcat                OmniVista Apache Tomcat     Running
ovnginx                 OmniVista Nginx             Running
ovscheduler             OmniVista Scheduler Service Running
ovftp                   OmniVista File Transfer Service Running
ovbyod                  OmniVista BYOD Service      Running
ovmasterpoller         OmniVista Primary Poller Service Running
ovag                    OmniVista AccessGuardian Service Running
ovav                    ..a Application Visibility Service Running
ovwireless              OmniVista Wireless Service  Running
ovmdns                  OmniVista mDNS Service      Running
ovresourcemanager      OmniVista Resource Manager Service Running
ovworkerpoller         OmniVista Worker Poller Service Running
ovclient                OmniVista Core Service      Running
ovanalytics             OmniVista Analytics Service Running
ovsflowcollector       OmniVista Sflow Collector Service Running
ovvxlan                 OmniVista VXLAN Service     Running
ovvlan                  OmniVista VLAN Service      Running
oviot                   OmniVista IoT Service       Running
ovvmmanager             OmniVista VM Manager Service Running
ovsip                   OmniVista SIP Service       Running
ovwma                   OmniVista WMA Service       Running
ovupam                  OmniVista UPAM Service      Running
ovradius                OmniVista Radius            Running
ovinfluxdb              OmniVista InfluxDB          Running
ovgrafana               OmniVista Grafana           Running
ovtelegraf              OmniVista Telegraf          Running
ovstatistics            OmniVista Statistics Service Running
ovbrightcloud           OmniVista Bright Cloud Service Running
ovzcs                   ..Vista Zigbee Controlling Service Running
ovucc                   OmniVista UCC Service       Running
*****
```

Note that when all services are up and running on the ov2 Node, you can proceed with upgrading the ov1 Node.

Connect to the Active Node (ov1) and Upgrade the Node to 4.8R2

Note: During the Active Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. User-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are retained.

1. After the upgrade and failover process has completed on ov2 (now the Active Node), open a Console on the OV 2500 NMS 4.8R1 ov1 Node (now the Standby Node), which is already in Maintenance Mode.

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.8R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: █
    
```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.8R2
* [0] Exit
*****
(*) Type your option: █
    
```

4. Enter **1 - Upgrade to 4.8R2** and press **Enter**.

```

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

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.8R2 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```

=====IMPORTANT:=====
You must start upgrade on the standby node first node.
Press [Enter] to continue

After standby node upgraded. You could upgrade active node.
Press [Enter] to continue

=====
Are you sure want to continue?[yln] (n): y
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 40
Patch Number: 0

Checking available packages for 4.8R2 operation is in progress...
Upgrade to 4.8R2 release is available after upgrading latest to version/patch of 4.8R1 release
Do you want to continue to check upgrade for 4.8R1 release now [yln] (n):
    
```

6. Click **y** when asked to check upgrade for 4.8R1 release now.

```

Getting upgrade information for 4.8R1...
Current version of Virtual Appliance is the latest build of 4.8R1

Getting upgrade information for 4.8R2...
Upgrade information for 4.8R2
Available Packages
Name       : ovmnse
Version    : 4.8R2
Release    : 21.0.e17
Architecture : x86_64
Size       : 2.0 G
Source     : ovmnse-4.8R2-21.0.e17.src.rpm
Repository : CustomRepo1_4.8R2
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 chosen to upgrade to latest build of 4.8R2 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?[yln] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed? [yln] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
    
```

7. Click **y** and press **Enter** after “Do you want to continue with the upgrade now?” and “Are you ready to proceed?”.

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You can ignore the following messages that may appear during the upgrade process:

- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```
[2024-01-09-23-05-22] [PRE-UNINSTALL] Begin...
[2024-01-09-23-05-22] [PRE-UNINSTALL] Done

Cleanup          : ovmnse-4.8R1-40.0.e17.x86_64          2/2
Running scriptlet: ovmnse-4.8R1-40.0.e17.x86_64          2/2

[2024-01-09-23-05-24] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2024-01-09-23-05-24] [POST-UNINSTALL] Done

Verifying        : ovmnse-4.8R2-21.0.e17.x86_64          1/2
Verifying        : ovmnse-4.8R1-40.0.e17.x86_64          2/2

Upgraded:
  ovmnse-4.8R2-21.0.e17.x86_64

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

The Virtual Appliance has to be restarted for applying new changes
Press [r] to reboot the system.
```

9. Press **r** to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
Oracle Linux Server 8.7
Kernel 4.18.0-425.3.1.el8.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 EA
Build Number: 34
Patch Number: 0
Build Date: 07/12/2023
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov140node2 login: cliadmin
Password:
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```

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

```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```

The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y/n] (n):

```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
 - a. Power on the VM.
 - b. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The HA Virtual Appliance Menu is displayed.

```

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

11. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See [Display Current Node Configuration](#) for more details.
12. When the upgrade of both OV-1 and OV-2 nodes to 4.8R2 is complete, the role of each node is reversed. The OV-1 node that was the Active Node at the beginning of the upgrade process, is now the Standby Node and OV-2 is now the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return OV-2 to Active Node status, select **4 – Configure Current Node** on the HA Virtual Appliance Menu and press **Enter** to bring up the Configure Cluster menu.

```

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

13. Select **15 – Manual Failover** and press **Enter** to manually initiate a failover to the current Standby Node (OV-1). The Standby Node will become the Active Node. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes). After the failover is complete, the services on OV-1 will be running. The previously Active Node (OV-2) will now be the Standby Node.

Verify the Upgrade

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

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.8R2. This is the Virtual IP address that you configured for the cluster. **Once OmniVista is launched, do a hard refresh (Shift+F5) of your browser window to ensure the display of the latest UI.**

Important Notes for Stellar APs:

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

Upgrading from 4.7R1 to 4.7R1 Patch 2 to 4.8R1

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.7R1 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.8R1 Standalone or High-Availability Installation.

Important Notes:

- You must upgrade from OV 2500 NMS 4.7R1 to the 4.7R1 Patch 2 release before you can upgrade to 4.8R1. Upgrading to the patch first requires you to create a custom repository for the 4.7R1 Patch 2 image. If you are already running the 4.7R1 Patch 2 release, you can directly upgrade to 4.8R1.
- During the 4.7R1 to 4.7R1 Patch 2 upgrade time for an OmniVista High-Availability installation, there is complete downtime until the upgrade is completed on both nodes and the Maintenance Mode is disabled.
- During the 4.7R1 Patch 2 to 4.8R1 upgrade time for an OmniVista High-Availability installation, OmniVista management functions remain available until the failover stage of the upgrade, at which time OmniVista is not available for approximately 5 to 10 minutes.
- During the upgrade time for an OmniVista Standalone installation, OmniVista is not available for any management functions. There is no impact to the deployed network during the OmniVista upgrade. Managed devices (Switch/AP) and existing device clients will continue to function as before. However, new clients cannot join the network if the Switch/AP is configured to do authentication from UPAM. The upgrade downtime may last between one and four hours and starts when the Maintenance Mode is enabled.
- When one of the nodes in an HA cluster becomes faulty, it can be decommissioned and replaced with a new node. While the HA is running in single node mode, prepare the new node, extend its data partition size as needed to match that of the old node, then join the new node to the cluster.
- It is recommended that you make note of your IP and NIC configurations before initiating a Standalone or HA upgrade to the 4.7R1 Patch2 or 4.8R1. Depending on the NIC types and hypervisor version, some special cases may require you to reconfigure these settings during or immediately after the upgrade to 4.8R1. If necessary, the VA will prompt you to perform the reconfiguration.
- You must perform the OmniVista upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client, upgrading the installation can result in incomplete upgrades and missing any pending actions, such as pressing the enter key to continue the upgrade.

Upgrading from 4.7R1 Standalone to 4.7R1 Patch 2 Standalone to 4.8R1 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.7R1 Standalone Installation to the 4.7R1 Patch 2 first, then to an OV 2500 NMS 4.8R1 Standalone Installation.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM

configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.

- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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 OmniVista makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

Standalone Upgrade Workflow

The basic steps for performing a Standalone upgrade are:

1. [Upgrading from 4.7R1 to 4.7R1 Patch 2](#) – Note that before you can upgrade to 4.8R1, you must first upgrade from 4.7R1 to 4.7R1 Patch 2. Upgrading to 4.7R1 Patch 2 requires configuring a custom repository for the patch. Follow the steps in this section to upgrade to 4.7R1 Patch 2.
2. [Upgrading from 4.7R1 Patch 2 to 4.8R1](#) – After you have successfully upgraded to 4.7R1 Patch 2, follow the steps in this section to upgrade to 4.8R1.

Upgrading from 4.7R1 to 4.7R1 Patch 2

1. Open a Console on the OV 2500 NMS 4.7R1 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: 4
```

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 5
```

3. Enter **5** – **Configure Custom Repositories** and press **Enter** to bring up the Configure Custom Repositories Screen.

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

4. Enter **3** – **"Custom Repo 2" Repository** and press **Enter**.

```

Current configuration
Repository Name:
Repository Full URL:

Please input Repository name [Custom Repo 2]: PatchRepo
(*) Please input Repository URL: https://ovrepo.fluentnetworking.com/ov/patch
Would you like to configure Repository with:
    Name: PatchRepo
    URL: https://ovrepo.fluentnetworking.com/ov/patch
[y|n] (y): y
The configuration has been set
Press [Enter] to continue
    
```

- When prompted to input a Repository name and URL, enter **PatchRepo** and **<https://ovrepo.fluentnetworking.com/ov/patch>**. After you enter the name and URL, enter **y** and press **Enter** to create the custom repository. The Configure Custom Repositories screen displays the repository you just created.

Note: OmniVista makes an HTTPS connection to the external repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

```

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

- Enter **0 – Exit** and press **Enter**, to return to the Upgrade VA Screen.

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 5
    
```

- Enter **4 – Enable Repository (Selected – ALE Central Repo)** and press **Enter**, to bring up the Enable Repository Screen.

```

*****
* Enable Repository
*****
* [1] Help
* [2] "ALE Central Repo" Repository
* [3] "SQAREpo" Repository (Selected)
* [4] "test-repo" Repository
* [5] "PatchRepo" Repository
* [6] "Offline Repo" Repository
* [0] Exit
*****
(*) Type your option: █
    
```

8. Enter **5** – “PatchRepo” Repository to select the custom repository you created in Step 5 and press **Enter**. At the prompt, enter **y** to enable the “PatchRepo” Repository and press **Enter** to return to the Upgrade VA Screen, which now shows “PatchRepo” as the selected repository.

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - PatchRepo)
* [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 **2** – To 4.7R1 (Upgrade to Latest patch of Current Release, if any) and press **Enter** to bring up the Upgrade System Options Screen.

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

10. Enter **2** – Download and Upgrade and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.7R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.7R1 GA
Build Number: 30
Patch Number: 0

Checking available packages for 4.7R1 operation is in progress...
Upgrade information for 4.7R1
Available Packages
Name      : ovmnsepatchb30
Arch      : x86_64
Version   : 4.7R1
Release   : 30.2.el7
Size      : 2.6 M
Repo      : CustomRepo2_4.7R1
Summary   : OV Patch 2 for 4.7R1 build 30
URL       : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&page=overview
License   : ALE USA Inc.
Description: Patch 2 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E 4.7R1
           : build 30
           : -----
           : Fixes:
           :
           : -CRNOV-4364: "In UPAM authentication, any user can elevate his
           : rights to the admin user"
           :
           : -OVE-12201: UPAM LDAP/AD configuration: cannot apply or test
           : connectivity to LDAP/AD server
           :
           : -ALEISSUE-1431 - OVE-12286: The value is always 0 for the first
           : hour in WLAN client summary report
           :
           : -OVC-9356: Cannot receive email from Report app with Encryption
           : TLS
           :
           : -OVC-9362: WiFi Clients connected to SSID with Map to Tunnel case
           : lost IP address after upgrading OV to 4.7.1
           :
           : -OVC-9353: Dashboard does not load widgets and shows communication
           : failure
           :
           : -OVE-12295: Cannot change Mongo Database Password on VA menu
           :
           : -OVE-12351: UPAM fails 802.1x authentication with Windows 11
           : clients (with 22H2 patch) wireless client due to missing TLS 1.3
           : support
           :
           : -OVE-12402: Cannot install VMware tool 4.7R1
           :
           : -OVE-12489: Cannot upgrade 4.7R1 using ALE default repo
           :
           : -----
Would you like to install the package [y/n] (n): █
```

11. Enter **y** and press **Enter** to continue.

```
-----
Would you like to install the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed? [y/n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Loaded plugins: langpacks, ulninfoade (16s)...
Resolving Dependencies
```

12. Enter **y** again when prompted, then press **Enter** to begin the download and upgrade to 4.7R1 Patch 2. The following screen appears when the upgrade is complete:

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
The Virtual Appliance has to be restarted for applying new changes
Rebooting...
Rebooting.
█
```

13. Press **Enter** to continue. The Virtual Appliance is restarted.

14. Verify the update to 4.7R1 Patch 2.

- Verify that all services have started.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
- Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See [Run Watchdog Command](#) for more details
- Verify that the Build Number is correct.
 - From The Virtual Appliance Menu, select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See [Display Current Configuration](#) for more details.
- Verify that you can [launch the OmniVista UI](#) and successfully login.
- Take a VM Snapshot of the current OmniVista VA and remove previous VA snapshots.

Note that once the 4.7R1 Patch 2 is installed and you have verified the update to 4.7R1 Patch 2, you can go ahead and upgrade to 4.8R1.

Upgrade from 4.7R1 Patch 2 to 4.8R1

1. Open a Console on the OV 2500 NMS 4.7R1 Patch 2 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: 4
```

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - PatchRepo)
* [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 **4 – Enable Repository (Selected – PatchRepo)** and press **Enter**, to bring up the Enable Repository Screen.

```
*****
* Enable Repository
*****
* [1] Help
* [2] "ALE Central Repo" Repository
* [3] "SQAREpo" Repository (Selected)
* [4] "test-repo" Repository
* [5] "PatchRepo" Repository
* [6] "Offline Repo" Repository
* [0] Exit
*****
(*) Type your option: █
```

4. Enter **2** – “ALE Central Repo” Repository and press **Enter**. At the prompt, enter **y** to enable the “ALE Central Repo” Repository and press **Enter** to return to the Upgrade VA Screen, which now shows “ALE Central Repo” as the selected repository.

Note: OmniVista makes an HTTPS connection to the external repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 5
```

5. Enter **3** – **To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.8R1
* [0] Exit
*****
(*) Type your option: █
```

6. Enter **1** – **Upgrade to 4.8R1** and press **Enter**. The Upgrade System Options Screen will appear.

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

7. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.8R1 upgrade packages.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

Enter **y** when asked “do you want to continue to check upgrade for 4.7r1 release now“ and press **Enter**.

```
(*) Type your option: 2

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.7R1 GA
Build Number: 30
Patch Number: 2

Checking available packages for 4.8R1 operation is in progress...
Upgrade to 4.8R1 release is available after upgrading latest to version/patch of 4.7R1 release
Do you want to continue to check upgrade for 4.7R1 release now [y|n] (n): y

Getting upgrade information for 4.7R1...
Current version of Virtual Appliance is the latest build of 4.7R1

Getting upgrade information for 4.8R1...
Upgrade information for 4.8R1
```

```
Getting upgrade information for 4.7R1...
Current version of Virtual Appliance is the latest build of 4.7R1

Getting upgrade information for 4.8R1...
Upgrade information for 4.8R1
Available Packages
Name      : ovmnse
Arch      : x86_64
Version   : 4.8R1
Release   : 34.0.el7
Size      : 1.9 G
Repo      : CustomRepo1_4.8R1
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 chosen to upgrade to latest build of 4.8R1 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):
```

8. Enter **y** and press **Enter**. A warning message will then appear asking you to proceed.

```
You have chosen to upgrade to latest build of 4.8R1 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
```

9. Enter **y** and press **Enter** to proceed with the upgrade. The following message will appear, and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Press any key to continue the upgrade (11s)...
```

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

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

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

10. When the installation is complete, the following prompt will appear: “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

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

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [yin] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the Configure the Virtual Appliance Menu, select **9** – Configure Network Size, then select **4** – Extend Data Partition.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

12. Verify the update to 4.8R1.

- Verify that all services have started.
 - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
 - Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See [Run Watchdog Command](#) for more details
- Verify that the Build Number is correct.
 - From The Virtual Appliance Menu, select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See [Display Current Configuration](#) for more details.
- Verify that you can [launch the OmniVista UI](#) and successfully login.
- Take a VM Snapshot of the current OmniVista VA and remove previous VA snapshots.

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.8R1. **Once OmniVista is launched, do a hard refresh (Shift+F5) of your browser window to ensure the display of the latest UI.**

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance.**
 2. **Select 2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
 3. **Select 9 - Configure Network Size.**
 4. **Select 2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
 5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.7R1 HA to 4.7R1 Patch 2 to 4.8R1 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.7R1 High-Availability Installation to the 4.7R1 Patch 2 first, then to an OV 2500 NMS 4.8R1 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Take a VM Snapshot of the current OmniVista VA on both the Active and Standby nodes. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OmniVista 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 **4 - Configure Current Node** on the Virtual Appliance Menu, then select **9 - Configure Proxy**.

You must perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 1 to 4 hours depending on network speed, network size, and database size.

High-Availability Upgrade Workflow

To upgrade to version 4.8R1, your system must be on 4.7R1 Patch 2. If your system is currently at the 4.7R1 GA level, you'll need to first upgrade to Patch 2 before proceeding to 4.8R1. The procedures for each of these stages are distinct. Consult the detailed steps outlined below for guidance.

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

1. [Upgrade the Active and Standby Nodes \(OV-1 and OV-2\) from 4.7R1 to 4.7R1 Patch 2.](#)

Note: During the 4.7R1 to 4.7R1 Patch 2 upgrade time for an OmniVista High-Availability installation, there is complete downtime until the upgrade is completed on both nodes and the Maintenance Mode is disabled.

- a. Verify the cluster status to make sure data is in sync between the two nodes.
- b. Connect to the Active Node and enable Maintenance Mode.
- c. Connect to the Standby Node and upgrade the node to 4.7R1 Patch 2. (As part of the upgrade process, do **not** reboot the Standby Node until the Active Node is upgraded.)
- d. Connect to the Active Node and upgrade the node to 4.7R1 Patch 2.
- e. When the upgrade to 4.7R1 Patch 2 is complete on the Active Node, reboot the Active Node.
- f. Reboot the Standby Node.
- g. Disable Maintenance Mode and wait for all services to start on the Active Node.
- h. Before upgrading the High-Availability cluster to 4.8R1, verify the following:
 - i. Maintenance Mode is disabled.
 - ii. All services are up and running on both nodes.
 - iii. The cluster status shows that the data is in sync between the two nodes.
 - iv. The OmniVista UI is reachable and loads; check the OmniVista Dashboard UI.
 - v. Take a VM Snapshot of the current OmniVista VA on both nodes.
 - vi. Remove any previous VM snapshots.

2. [Upgrade the Active and Standby Nodes \(OV-1 and OV-2\) from 4.7R1 Patch 2 to 4.8R1](#)

Note: During the 4.7R1 Patch 2 to 4.8R1 upgrade time for an OmniVista High-Availability installation, OmniVista management functions remain available until the failover stage of the upgrade, at which time OmniVista is not available for approximately 5 to 10 minutes.

- a. Verify the cluster status to make sure data is in sync between the two nodes.
- b. Connect to the Active Node and enable Maintenance Mode
- c. Connect to the Standby Node and upgrade the node to 4.8R1.
- d. When the Standby Node upgrade is complete, do a reboot and failover. The Standby Node (OV-2) is now the Active Node. Connect to the OV-2 node and wait for all services to start.
- e. Connect to the previous Active Node (OV-1) and upgrade the node to 4.8R1. Restart OV-1 after the upgrade.
- f. Verify the Upgrade

Note: After this upgrade process is complete, the Active Node at the beginning of the process is no longer the Active Node. This is a perfectly normal state of operation for

OmniVista functions. However, if you want to return the node to Active Node status, you can do a manual failover on that node.

Upgrade the Active and Standby Nodes (OV-1 and OV-2) from 4.7R1 to 4.7R1 Patch 2

Verify the Cluster Status

Before you begin the process to upgrade the HA cluster from 4.7R1 to 4.7R1 Patch 2, verify that the Cluster Status is “Up to Date”. This can be performed on either node.

1. On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.
2. Begin the HA cluster upgrade from 4.7R1 to 4.7R1 Patch 2.

Enable Maintenance Mode on the Active Node (OV-1)

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node (OV-1). Open a Console on the OV 2500 NMS 4.7R1 OV-1 Node. This will enable Maintenance Mode on both nodes (OV-1 and OV-2) in the Cluster.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [yn] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

Connect to the Standby Node (OV-2) and Upgrade the Node to 4.7R1 Patch 2

Note: Do not reboot after completing the following steps to upgrade the Standby Node to 4.7R1 Patch 2. Instead, go to the section for [upgrading the Active Node \(OV-1\) to 4.7R1 Patch 2](#) and complete the steps in that section before rebooting both nodes.

1. Open a Console on the OV 2500 NMS 4.7R1 Standby Node, which is already in Maintenance Mode.

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 5
    
```

3. Enter **5** – **Configure Custom Repositories** and press **Enter** to bring up the Configure Custom Repositories Screen.

```

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

4. Enter **2** – **"Custom Repo 1" Repository** and press **Enter**.

```

Current configuration
Repository Name:
Repository Full URL:

Please input Repository name [Custom Repo 2]: PatchRepo
(*) Please input Repository URL: https://ovrepo.fluentnetworking.com/ov/patch
Would you like to configure Repository with:
    Name: PatchRepo
    URL: https://ovrepo.fluentnetworking.com/ov/patch
[y|n] (y): y
The configuration has been set
Press [Enter] to continue
    
```

5. When prompted to input a Repository name and URL, enter **PatchRepo** and **https://ovrepo.fluentnetworking.com/ov/patch**. After you enter the name and URL, enter

y and press **Enter** to create the custom repository. The Configure Custom Repositories screen displays the repository you just created.

Note: OmniVista makes an HTTPS connection to the 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 **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

6. Enter **0 – Exit** and press **Enter**, to return to the Upgrade VA Screen

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 5
```

7. Enter **4 – Enable Repository (Selected – ALE Central Repo)** and press **Enter**, to bring up the Enable Repository Screen.

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

8. Enter **3 – “PatchRepo” Repository** to select the custom repository you created in Step 5 and press **Enter**. At the prompt, enter **y** to enable the “PatchRepo” Repository and press **Enter** to return to the Enable Repository Screen, which now shows “PatcRepo” as the selected repository.

```

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

9. Enter **0** – **Exit** and press **Enter** to return to the Upgrade VA Screen.

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - PatchRepo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 2
    
```

10. Enter **2** – **To 4.7R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Screen.

```

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

11. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.7R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

When the upgrade process is complete for the Standby Node, do not reboot the VM when prompted to do so. Wait until after upgrading the Active Node to reboot both VMs.

Connect to the Active Node (OV-1) and upgrade the node to 4.7R1 Patch 2

1. Open a Console on the OV 2500 NMS 4.7R1 Active Node.

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

2. To upgrade the Active Node (OV-1) to 4.7R1 Patch 2, follow the steps used to [upgrade the Standby Node \(OV-2\) to 4.7R1 Patch 2](#).
3. When the upgrade to 4.7R1 Patch 2 is completed on both the Active Node (OV-1) and the Standby Node (OV-2), restart both nodes.

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

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

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

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

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

Verify the Upgrade

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

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

on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.

You can now [launch the OmniVista UI](#).

Note that once the 4.7R1 Patch 2 is installed on both Active and Standby Nodes, you can go ahead and upgrade to 4.8R1.

Upgrade the Active and Standby Nodes (OV-1 and OV-2) from 4.7R1 Patch 2 to 4.8R1

In this HA upgrade procedure, OV-1 is initially the Active Node until the OV-2 Standby Node is upgraded first. After OV-2 is upgraded, the OV-2 Node will become the Active Node and OV-1 will become the Standby Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return OV-2 to Active Node status, you can do a manual failover after both nodes are upgraded (see Step 12 in [Connect to the OV-1 Node and Upgrade the Node to 4.8R1](#) for more details).

Verify the Cluster Status

Before you begin the process to upgrade the HA cluster from 4.7R1 Patch 2 to 4.8R1, verify that the Cluster Status is “Up to Date”. This can be performed on either node.

1. On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.
2. Begin the HA cluster upgrade from 4.7R1 Patch 2 to 4.8R1.

Enable Maintenance Mode on the Active Node (OV-1)

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node (OV-1). Open a Console on the OV 2500 NMS 4.7R1 Patch 2 OV-1 Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y/n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

Connect to the Standby Node (OV-2) and Upgrade the Node to 4.8R1

Note: During the Standby Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. However, any user-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are lost.

1. Open a Console on the OV 2500 NMS 4.7R1 Patch 2 Standby Node (OV-2), which is already in Maintenance Mode.

```

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

```

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 3

```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.8R1
* [0] Exit
*****
(*) Type your option: 1

```

4. Enter **1 - Upgrade to 4.8R1** and press **Enter**.

```

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

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.8R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```

=====IMPORTANT:=====
You must upgrade the standby node first for the new upgrade flow.
Please read the installation guide for details...
=====
Press [Enter] to continue
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.7R1 GA
Build Number: 30
Patch Number: 2

Checking available packages for 4.8R1 operation is in progress...
Upgrade to 4.8R1 release is available after upgrading latest to version/patch of 4.7R1 release
Do you want to continue to check upgrade for 4.7R1 release now [y|n] (n): y
    
```

6. Click **y** when asked to check upgrade for 4.7R1 release now.

```

Getting upgrade information for 4.7R1...
Current version of Virtual Appliance is the latest build of 4.7R1

Getting upgrade information for 4.8R1...
Upgrade information for 4.8R1
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.8R1
Release   : 34.0.e17
Size      : 1.9 G
Repo      : CustomRepo1 4.8R1
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 chosen to upgrade to latest build of 4.8R1 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Press any key to continue the upgrade (17s)...
    
```

7. Click **y** and press **Enter** after “Do you want to continue with the upgrade now?” and “Are you ready to proceed?”

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Upgrading Oracle Linux from 7.9 to 8.7” progress messages. 4.8R1 includes an update to Oracle Linux 8.7, which occurs during the upgrade process.
- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```

=====IMPORTANT=====
The upgrade flow may print a Warning message in Yellow color about do not reboot until the other node in the cluster is upgraded.
Please ignore the warning and proceed with the Reboot now.
Refer to Install Guide for this known issue or incorrect warning getting printed on console.
=====

[2023-08-01-16-40-39] [PRE-UNINSTALL] Begin...
[2023-08-01-16-40-41] [PRE-UNINSTALL] Done

Cleanup      : ovmse-4.7R1-30.0.e17.x86_64                2/2

[2023-08-01-16-40-49] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2023-08-01-16-40-49] [POST-UNINSTALL] Done

Verifying   : ovmse-4.8R1-40.0.e17.x86_64                1/2
Verifying   : ovmse-4.7R1-30.0.e17.x86_64                2/2

Updated:
  ovmse.x86_64 0:4.8R1-40.0.e17

Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.
Press [r] to reboot the system.
    
```

9. Please ignore the “WARNING” message about not rebooting this node unless the other node is also upgraded. It is necessary to reboot this node (OV-2) now to proceed with the upgrade. Press r to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```

Oracle Linux Server 8.7
Kernel 4.18.0-425.3.1.el8.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 EA
Build Number: 34
Patch Number: 0
Build Date: 07/12/2023
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov140node2 login: cliadmin
Password:
Last login: Mon Jul 10 11:59:57 on tty1
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
    
```

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

10. Login through the VA console. When prompted, press **Enter** to perform the failover. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes).

```
Activate the web console with: systemctl enable --now cockpit.socket
Last login: Fri Jul 14 13:19:50 2023
Configuring cluster after upgrade...
Initializing (step 1/3).....100%
Finalizing configuration (step 2/3).....100%
Starting services (step 3/3).....100%
Press Enter to failover...
Activating cluster IPs.....100%
Cluster reconfiguration is done. Now you can upgrade another node.
Press enter to logout.
```

11. Press **Enter** to logout, then login again to access the HA Virtual Appliance Menu.

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

12. Enter **2** – Show OV Cluster Status and press **Enter** to display the HA Cluster Status.

```
*****
(*) Type your option: 2
Cluster Status:
Node      Hostname      Ip Address      Role      Status
Current  ovl40node2    172.20.0.142    Active
Peer     ovl40node1    172.20.0.141    Offline (Last seen: Jul-14-2023 06:13:28 GMT -07:00)
Data sync: Paused
*****
* The HA Virtual Appliance Menu
*****
```

13. Verify that Standby Node (OV-2) is now the Active Node and OV-1 is now the Standby Node.

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

14. Click on **5 – Run Watchdog Command** on the HA Virtual Appliance Menu and press **Enter**.

```
*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option: 2
Would you like to run continuous status checking [y|n] (n):
```

15. Click on **2 – Display Status Of All Services** and press **Enter** to verify all services are running on the Active Node (formerly the Standby Node).

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
(*) Type your option: 2
Would you like to run continuous status checking [y|n] (n): n
-----
Key Name                Display Name                Status
-----
ovactivemq              OmniVista ActiveMQ          Running
ovredis                 OmniVista Redis             Running
ovldap                  OmniVista OpenLDAP Server   Running
ovmongodb               OmniVista MongoDB           Running
ovpostgres              OmniVista Postgresql        Running
ovjetty                 OmniVista Jetty             Running
ovlog                   OmniVista Log Server        Running
ovdal                   OmniVista DAL Service       Running
ovtomcat                OmniVista Apache Tomcat     Running
ovnginx                 OmniVista Nginx             Running
ovscheduler             OmniVista Scheduler Service Running
ovftp                   OmniVista File Transfer Service Running
ovbyod                  OmniVista BYOD Service      Running
ovmasterpoller         OmniVista Primary Poller Service Running
ovag                    OmniVista AccessGuardian Service Running
ovav                    ..a Application Visibility Service Running
ovwireless              OmniVista Wireless Service  Running
ovmdns                  OmniVista mDNS Service      Running
ovresourcemanager      OmniVista Resource Manager Service Running
ovworkerpoller         OmniVista Worker Poller Service Running
ovclient                OmniVista Core Service      Running
ovanalytics             OmniVista Analytics Service Running
ovsflowcollector        OmniVista Sflow Collector Service Running
ovvxlan                 OmniVista VXLAN Service     Running
ovvlan                  OmniVista VLAN Service      Running
oviot                   OmniVista IoT Service       Running
ovvmmanager             OmniVista VM Manager Service Running
ovsip                   OmniVista SIP Service       Running
ovwma                   OmniVista WMA Service       Running
ovupam                  OmniVista UPAM Service      Running
ovradius                OmniVista Radius            Running
ovinfluxdb              OmniVista InfluxDB          Running
ovgrafana               OmniVista Grafana           Running
ovtelegraf              OmniVista Telegraf          Running
ovstatistics            OmniVista Statistics Service Running
ovbrightcloud           OmniVista Bright Cloud Service Running
ovzcs                   ..Vista Zigbee Controlling Service Running
ovucc                   OmniVista UCC Service       Running
*****
```

Note that when all services are up and running on the OV-2 Node, you can proceed with upgrading the OV-1 Node.

Connect to the Active Node (OV-1) and Upgrade the Node to 4.8R1

Note: During the Active Node upgrade process, OmniVista UI monitoring and UPAM authentications are available. User-configured changes and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are retained.

1. After the upgrade and failover process has completed on OV-2, open a Console on the OV 2500 NMS 4.7R1 Patch 2 OV-1 Node (now the Standby Node), which is already in Maintenance Mode.

```

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

```

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.7R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 3

```

Note: You must use the default ALE Central Repo in Option 4 above. If you were using a repository with a different name, you must first change it to “ALE Central Repo”, then continue with the next step. If your OmniVista 2500 NMS Server is not directly connected to the Internet, a Proxy to reach the external repository is required. To configure a Proxy, select **4 - Configure Current Node** on the HA Virtual Appliance Menu, then select **9 - Configure Proxy**.

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.8R1
* [0] Exit
*****
(*) Type your option: 1

```

4. Enter **1 - Upgrade to 4.8R1** and press **Enter**.

```

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

5. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.8R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```

=====IMPORTANT:=====
You must upgrade the standby node first for the new upgrade flow.
Please read the installation guide for details...
=====
Press [Enter] to continue
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.7R1 GA
Build Number: 30
Patch Number: 2

Checking available packages for 4.8R1 operation is in progress...
Upgrade to 4.8R1 release is available after upgrading latest to version/patch of 4.7R1 release
Do you want to continue to check upgrade for 4.7R1 release now [y|n] (n): y
    
```

6. Click **y** when asked to check upgrade for 4.7R1 release now.

```

Getting upgrade information for 4.7R1...
Current version of Virtual Appliance is the latest build of 4.7R1

Getting upgrade information for 4.8R1...
Upgrade information for 4.8R1
Available Packages
Name      : omnise
Arch      : x86_64
Version   : 4.8R1
Release   : 34.0.el7
Size      : 1.9 G
Repo      : CustomRepo1.4.8R1
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 chosen to upgrade to latest build of 4.8R1 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to remove unexisting files. You can ignore them.
Press any key to continue the upgrade (17s)...
    
```

7. Click **y** and press **Enter** after “Do you want to continue with the upgrade now?” and “Are you ready to proceed?”.

Note: The upgrade usually takes 1 - 2 hours to complete. But it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: You can ignore the following messages that may appear during the upgrade process:

- “Upgrading Oracle Linux from 7.9 to 8.7” progress messages. 4.8R1 includes an update to Oracle Linux 8.7, which occurs during the upgrade process.
- “Warning: Unmaintained hardware is detected” error messages.
- “no such file or directory” error messages.

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

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

```

=====IMPORTANT=====
The upgrade flow may print a Warning message in Yellow color about do not reboot until the other node in the cluster is upgraded.
Please ignore the warning and proceed with the Reboot now.
Refer to Install Guide for this known issue or incorrect warning getting printed on console.
=====

[2023-08-01-16-40-39] [PRE-UNINSTALL] Begin...
[2023-08-01-16-40-41] [PRE-UNINSTALL] Done

Cleanup      : ovmse-4.7R1-30.0.e17.x86_64                2/2

[2023-08-01-16-40-49] [POST-UNINSTALL] Begin...
Perform a removal for upgrading
[2023-08-01-16-40-49] [POST-UNINSTALL] Done

Verifying   : ovmse-4.8R1-40.0.e17.x86_64                1/2
Verifying   : ovmse-4.7R1-30.0.e17.x86_64                2/2

Updated:
  ovmse.x86_64 0:4.8R1-40.0.e17

Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.
Press [r] to reboot the system.
  
```

9. Please ignore the yellow “WARNING” message about not rebooting this node unless the other node is also upgraded. It is necessary to reboot this node (OV-1) now to proceed with the upgrade. Press r to reboot the system. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```

Oracle Linux Server 8.7
Kernel 4.18.0-425.3.1.el8.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 EA
Build Number: 34
Patch Number: 0
Build Date: 07/12/2023
Technical Support Code: alcatel
Activate the web console with: systemctl enable --now cockpit.socket

ov148node2 login: cliadmin
Password:
  
```

Note: You can ignore the message “Activate the web console with: systemctl enable --now cockpit.socket” that appears on the login screen and continue with the login. This message is normal.

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

```

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

```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```

The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y/n] (n):

```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The HA Virtual Appliance Menu is displayed.

```

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

11. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See [Display Current Node Configuration](#) for more details.
12. When the upgrade of both OV-1 and OV-2 nodes to 4.8R1 is complete, the role of each node is reversed. The OV-1 node that was the Active Node at the beginning of the upgrade process, is now the Standby Node and OV-2 is now the Active Node. This is a perfectly normal state of operation for OmniVista functions. However, if you want to return OV-2 to Active Node status, select **4 – Configure Current Node** on the HA Virtual Appliance Menu and press **Enter** to bring up the Configure Cluster menu.

```

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

13. Select **15 – Manual Failover** and press **Enter** to manually initiate a failover to the current Standby Node (OV-1). The Standby Node will become the Active Node. Note that OmniVista functions, including UI monitoring and UPAM authentications, will not be available during the failover time (approximately 5-10 minutes). After the failover is complete, the services on OV-1 will be running. The previously Active Node (OV-2) will now be the Standby Node.

Verify the Upgrade

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

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.8R1. This is the Virtual IP address that you configured for the cluster. **Once OmniVista is launched, do a hard refresh (Shift+F5) of your browser window to ensure the display of the latest UI.**

Important Notes for Stellar APs:

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

Upgrading from 4.6R2 to 4.7R1

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.6R2 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.7R1 Standalone or High-Availability Installation.

Note: During the upgrade time, OmniVista (standalone or HA) is not available for any management functions. So, none of the OmniVista functionality is available during upgrade. There is no impact to the deployed network during the OmniVista upgrade. Managed devices (Switch/AP) and existing device clients will continue to function as before. However, new clients cannot join the network if the Switch/AP is configured to do authentication from UPAM. The upgrade downtime may last between one and four hours and starts when the Maintenance Mode is enabled.

Note: When one of the nodes in an HA cluster becomes faulty, it can be decommissioned and replaced with a new node. While the HA is running in single node mode, prepare the new node, extend its data partition size as needed to match that of the old node, and then join it to the cluster.

Upgrading from 4.6R2 Standalone to 4.7R1 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.6R2 Standalone Installation to an OV 2500 NMS 4.7R1 Standalone Installation.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- The reserved RAM requirement for standalone installations in a Medium network was increased to 36GB for OmniVista 4.6R2. To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- 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 OV 2500 NMS 4.7R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

1. Open a Console on the OV 2500 NMS 4.6R1 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: _
```

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.6R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - SQARepo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 0
```

3. Enter **3** – **To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.6R2
* [0] Exit
*****
(*) Type your option: _
```

4. Enter **1** – **Upgrade to 4.7R1** and press **Enter**. The Upgrade System Options Screen will appear.

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

5. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.7R1 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0

Checking available packages for 4.6R2 operation is in progress...
Upgrade to 4.6R2 release is available after upgrading latest to version/patch of 4.6R1 release
Do you want to continue to check upgrade for 4.6R1 release now [y|n] (n): y

Getting upgrade information for 4.6R1...
```

6. Enter **y** and press **Enter** to continue. OmniVista retrieves and displays upgrade information for 4.7R1.

```
Getting upgrade information for 4.6R1...
Current version of Virtual Appliance is the latest build of 4.6R1

Getting upgrade information for 4.6R2...
Upgrade information for 4.6R2
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.6R2
Release   : 34.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.6R2
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 chosen to upgrade to latest build of 4.6R2 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): _
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following message will appear and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (11s)...
```

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

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

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

8. When the installation is complete, the following prompt will appear “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several

minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R2 GA
Build Number: 33
Patch Number: 0
Build Date: 01/27/2022
Technical Support Code: alcate1123
omnivista login: _
```

9. Log into the VM. The Virtual Appliance Menu will appear.

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [yn] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.

- On the Configure the Virtual Appliance Menu, select **9** – Configure Network Size, then select **4** – Extend Data Partition.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

10. Verify the upgrade.

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

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPaddress>` in a supported browser to launch OV 2500 NMS 4.7R1.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance**.
 2. Select **2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
 3. Select **9 - Configure Network Size**.
 4. Select **2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
 5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.6R2 HA to 4.7R1 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.6R2 High-Availability Installation to an OV 2500 NMS 4.7R1 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- The reserved RAM requirement for HA installations in a Medium network was increased to 40GB for OmniVista 4.6R2. To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OV 2500 NMS 4.7R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can

take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

High-Availability Upgrade Workflow

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

1. [Enable Maintenance Mode on the Active Node](#)
2. [Upgrade the Active Node to 4.7R1](#) (as part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
3. [Upgrade the Standby Node to 4.7R1](#)
4. [Disable Maintenance Mode on the Active Node](#)
5. [Verify the Upgrade.](#)

Enable Maintenance Mode on the Active Node

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node. Open a Console on the OV 2500 NMS 4.6R1 Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [yin] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

Upgrade the Active Node to 4.7R1

```

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade UA                                                                 *
*****
* [1] Help                                                                 *
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)      *
* [3] To New Release                                                       *
* [4] Enable Repository (Selected - ALE Central Repo)                    *
* [5] Configure Custom Repositories                                       *
* [6] Configure "Update Check Interval" (Selected - Disabled)           *
* [7] Backup/Restore OmniVista 2500 NMS Data                             *
* [0] Exit                                                                 *
*****
(*) Type your option:
```

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

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

```
*****
* Upgrade to New Release                                                  *
*****
* [1] Upgrade to 4.6R2                                                    *
* [0] Exit                                                                *
*****
(*) Type your option: _
```

3. Enter **1 - Upgrade to 4.7R1** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0

Checking available packages for 4.6R2 operation is in progress...
Upgrade to 4.6R2 release is available after upgrading latest to version/patch of 4.6R1 release
Do you want to continue to check upgrade for 4.6R1 release now [y/n] (n): y
Getting upgrade information for 4.6R1
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.7R1.

```
Getting upgrade information for 4.6R1...
Current version of Virtual Appliance is the latest build of 4.6R1

Getting upgrade information for 4.6R2...
Upgrade information for 4.6R2
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.6R2
Release   : 34.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.6R2
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 chosen to upgrade to latest build of 4.6R2 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): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [y|n] (n):
```

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

9. [Upgrade the Standby Node to 4.7R1](#). After upgrading the Standby Node, return to this screen and continue with Step 10 below to reboot the Active Node and complete the upgrade process.

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

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R2 GA
Build Number: 33
Patch Number: 0
Build Date: 01/27/2022
Technical Support Code: alcatel123
omnivista login: _
```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y|n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The following prompt will appear, and the HA Virtual Appliance Menu is displayed.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

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

```

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

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

Upgrade the Standby Node to 4.7R1

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade to New Release *
*****
* [1] Upgrade to 4.6R2 *
* [0] Exit *
*****
(*) Type your option: _
```

3. Enter **1 - Upgrade to 4.7R1** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0

Checking available packages for 4.6R2 operation is in progress...
Upgrade to 4.6R2 release is available after upgrading latest to version/patch of 4.6R1 release
Do you want to continue to check upgrade for 4.6R1 release now [y|n] (n): y
Getting upgrade information for 4.6R1
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.7R1.

```
Getting upgrade information for 4.6R1...
Current version of Virtual Appliance is the latest build of 4.6R1

Getting upgrade information for 4.6R2...
Upgrade information for 4.6R2
Available Packages
Name      : ovmnse
Arch      : x86_64
Version   : 4.6R2
Release   : 34.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.6R2
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 chosen to upgrade to latest build of 4.6R2 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): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [y|n] (n):
```

9. Type **y** then press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 10, page 61).

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R2 GA
Build Number: 33
Patch Number: 0
Build Date: 01/27/2022
Technical Support Code: alcatel123
omnivista login: _
```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OUV VM using
hypervisor and then power on the OUV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [y|n] (n):
```

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

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

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

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

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

```

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

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

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

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

Verify the Upgrade

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

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.6R1. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Upgrading from 4.6R1 to 4.6R2

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.6R1 Standalone or High-Availability Installation to an OV 2500 NMS 4.6R2 Standalone or High-Availability Installation.

Note: During the upgrade time, OmniVista (standalone or HA) is not available for any management functions. So, none of the OmniVista functionality is available during upgrade. There is no impact to the deployed network during the OmniVista upgrade. Managed devices (Switch/AP) and existing device clients will continue to function as before. However, new clients cannot join the network if the Switch/AP is configured to do authentication from UPAM. The upgrade downtime may last between one and four hours and starts when the Maintenance Mode is enabled.

Upgrading from 4.6R1 Standalone to 4.6R2 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.6R1 Standalone Installation to an OV 2500 NMS 4.6R2 Standalone Installation.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- The reserved RAM requirement for standalone installations in a Medium network was increased to 36GB for OmniVista 4.6R2. To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note that OV 2500 NMS 4.6R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

1. Open a Console on the OV 2500 NMS 4.6R1 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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option: _
```

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.6R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - SQARepo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: 0
```

3. Enter **3** – **To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.6R2
* [0] Exit
*****
(*) Type your option: _
```

4. Enter **1** – **Upgrade to 4.6R2** and press **Enter**. The Upgrade System Options Screen will appear.

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

5. Enter **2 – Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.6R2 upgrade packages.

Note: You must select **2 – Download and Upgrade**. Option **4 – Upgrade from downloaded package** is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0

Checking available packages for 4.6R2 operation is in progress...
Upgrade to 4.6R2 release is available after upgrading latest to version/patch of 4.6R1 release
Do you want to continue to check upgrade for 4.6R1 release now [y|n] (n): y

Getting upgrade information for 4.6R1...
```

6. Enter **y** and press **Enter** to continue. OmniVista retrieves and displays upgrade information for 4.6R2.

```
Getting upgrade information for 4.6R1...
Current version of Virtual Appliance is the latest build of 4.6R1

Getting upgrade information for 4.6R2...
Upgrade information for 4.6R2
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.6R2
Release   : 34.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.6R2
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 chosen to upgrade to latest build of 4.6R2 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): _
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following message will appear and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (11s)...
```

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

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

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

8. When the installation is complete, the following prompt will appear “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several

minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R2 GA
Build Number: 33
Patch Number: 0
Build Date: 01/27/2022
Technical Support Code: alcatel123
omnivista login: _
```

9. Log into the VM. The Virtual Appliance Menu will appear.

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [y/n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.

- On the Configure the Virtual Appliance Menu, select **9** – Configure Network Size, then select **4** – Extend Data Partition.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

10. Verify the upgrade.

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

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.6R2.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance**.
 2. Select **2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
 3. Select **9 - Configure Network Size**.
 4. Select **2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
 5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.6R1 HA to 4.6R2 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.6R1 High-Availability Installation to an OV 2500 NMS 4.6R2 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space and reserved RAM for OmniVista.
- The reserved RAM requirement for HA installations in a Medium network was increased to 40GB for OmniVista 4.6R2. To increase the RAM size:
 - Log into OmniVista VA with “cliadmin” and use the “Power Off” menu option to shut OmniVista down.
 - Increase memory for the VM from the hypervisor.
 - Power the VM back on, log into OmniVista VA and wait for services to start, then start the upgrade.
- 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.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OV 2500 NMS 4.6R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

High-Availability Upgrade Workflow

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

1. [Enable Maintenance Mode on the Active Node](#)
2. [Upgrade the Active Node to 4.6R2](#) (as part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
3. [Upgrade the Standby Node to 4.6R2](#)
4. [Disable Maintenance Mode on the Active Node](#)
5. [Verify the Upgrade.](#)

Enable Maintenance Mode on the Active Node

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node. Open a Console on the OV 2500 NMS 4.6R1 Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

```

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y/n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

Upgrade the Active Node to 4.6R2

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade to New Release *
*****
* [1] Upgrade to 4.6R2 *
* [0] Exit *
*****
(*) Type your option: _
```

3. Enter **1 - Upgrade to 4.6R2** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0

Checking available packages for 4.6R2 operation is in progress...
Upgrade to 4.6R2 release is available after upgrading latest to version/patch of 4.6R1 release
Do you want to continue to check upgrade for 4.6R1 release now [y|n] (n): y
Getting upgrade information for 4.6R1
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.6R2.

```
Getting upgrade information for 4.6R1...
Current version of Virtual Appliance is the latest build of 4.6R1

Getting upgrade information for 4.6R2...
Upgrade information for 4.6R2
Available Packages
Name       : ovmnse
Arch       : x86_64
Version    : 4.6R2
Release    : 34.0.e17
Size       : 1.6 G
Repo       : CustomRepo1_4.6R2
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 chosen to upgrade to latest build of 4.6R2 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): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [yin] (n):
```

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

9. [Upgrade the Standby Node to 4.6R2](#). After upgrading the Standby Node, return to this screen and continue with Step 10 below to reboot the Active Node and complete the upgrade process.

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

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R2 GA
Build Number: 33
Patch Number: 0
Build Date: 01/27/2022
Technical Support Code: alcatel123
omnivista login: _
```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OU VM using
hypervisor and then power on the OU 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y/n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The following prompt will appear, and the HA Virtual Appliance Menu is displayed.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

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

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

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

Upgrade the Standby Node to 4.6R2

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

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

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.6R2
* [0] Exit
*****
(*) Type your option: _
    
```

3. Enter **1 - Upgrade to 4.6R2** and press **Enter** to bring up the Upgrade System Options Menu.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

4. Enter **2** – **Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0

Checking available packages for 4.6R2 operation is in progress...
Upgrade to 4.6R2 release is available after upgrading latest to version/patch of 4.6R1 release
Do you want to continue to check upgrade for 4.6R1 release now [y/n] (n): y

Getting upgrade information for 4.6R1
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.6R2.

```
Getting upgrade information for 4.6R1...
Current version of Virtual Appliance is the latest build of 4.6R1

Getting upgrade information for 4.6R2...
Upgrade information for 4.6R2
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.6R2
Release   : 34.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.6R2
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 chosen to upgrade to latest build of 4.6R2 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): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [y/n] (n):
```

9. Type **y** then press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 10, page 61).

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R2 GA
Build Number: 33
Patch Number: 0
Build Date: 01/27/2022
Technical Support Code: alcatel123
omnivista login: _
```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y/n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

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

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

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

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

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

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

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

Verify the Upgrade

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

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

on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.6R1. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Upgrading from 4.5R3 to 4.6R1

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R3 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.6R1 Standalone or High-Availability Installation.

Upgrading from 4.5R3 Standalone to 4.6R1 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R3 Standalone Installation to an OV 2500 NMS 4.6R1 Standalone Installation.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista may take up to a day to purge the older data, but it is recommended as a way to save disk space.

Note that OV 2500 NMS 4.6R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

1. Open a Console on the OV 2500 NMS 4.5R3 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
* [12] Convert to Cluster
* [13] Join Cluster
* [0] Log Out
*****
(*) Type your option:
```

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
```

3. Enter **3** – **To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.6R1
* [0] Exit
*****
(*) Type your option:
```

4. Enter **1** – **Upgrade to 4.6R1** and press **Enter**. The Upgrade System Options Screen will appear.

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

5. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.6R1 upgrade packages.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You **must** select 2 – Download and Upgrade. Option 4 – Upgrade from downloaded package is **not** supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 0

Checking available packages for 4.6R1 operation is in progress...
Upgrade to 4.6R1 release is available after upgrading latest to version/patch of 4.5R3 release
Do you want to continue to check upgrade for 4.5R3 release now [y/n] (n):
```

6. Enter **y** and press **Enter** to continue. OmniVista retrieves and displays upgrade information for 4.6R1.

```
Getting upgrade information for 4.5R3...
Current version of Virtual Appliance is the latest build of 4.5R3

Getting upgrade information for 4.6R1...
Upgrade information for 4.6R1
Available Packages
Name       : ovnmse
Arch       : x86_64
Version    : 4.6R1
Release    : 44.0.e17
Size       : 1.5 G
Repo       : CustomRepo1_4.6R1
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 chosen to upgrade to latest build of 4.6R1 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):
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following message will appear and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (11s)...
```

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

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

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

8. When the installation is complete, the following prompt will appear “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0
Build Date: 09/17/2021
Technical Support Code: 12345678
omnivista login:
```

9. Log into the VM. The Virtual Appliance Menu will appear.

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 2-Configure the Virtual Appliance Menu, select
9-Configure Network Size, then select 4-Extend Data Partition
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now?
Choose 'n' to do it later [y|n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the Configure the Virtual Appliance Menu, select **9** – Configure Network Size, then select **4** – Extend Data Partition.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

10. Verify the upgrade.

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

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.6R1.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance**.
 2. **Select 2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
 3. **Select 9 - Configure Network Size**.
 4. **Select 2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
 5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.5R3 HA to 4.6R1 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R3 High-Availability Installation to an OV 2500 NMS 4.6R1 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM

configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.

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

Note that OV 2500 NMS 4.5R3 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

High-Availability Upgrade Workflow

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

1. [Enable Maintenance Mode on the Active Node](#)
2. [Upgrade the Active Node to 4.6R1](#) (as part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
3. [Upgrade the Standby Node to 4.6R1](#)
4. [Disable Maintenance Mode on the Active Node](#)
5. [Verify the Upgrade.](#)

Enable Maintenance Mode on the Active Node

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node. Open a Console on the OV 2500 NMS 4.5R3 Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

```

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y/n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

Upgrade the Active Node to 4.6R1

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

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
```

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

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

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.6R1
* [0] Exit
*****
(*) Type your option:
```

3. Enter **1 - Upgrade to 4.6R1** and press **Enter** to bring up the Upgrade System Options Menu.

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

4. Enter **2** – **Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 0

Checking available packages for 4.6R1 operation is in progress...
Upgrade to 4.6R1 release is available after upgrading latest to version/patch of 4.5R3 release
Do you want to continue to check upgrade for 4.5R3 release now [y/n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.6R1.

```
Getting upgrade information for 4.5R3...
Current version of Virtual Appliance is the latest build of 4.5R3

Getting upgrade information for 4.6R1...
Upgrade information for 4.6R1
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.6R1
Release   : 44.0.e17
Size      : 1.5 G
Repo      : CustomRepo1_4.6R1
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 chosen to upgrade to latest build of 4.6R1 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):
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [y|n] (n):
```

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

9. [Upgrade the Standby Node to 4.6R1](#). After upgrading the Standby Node, return to this screen and continue with Step 10 below to reboot the Active Node and complete the upgrade process.

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

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0
Build Date: 09/17/2021
Technical Support Code: 12345678
o01 login:
```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
To add more disk space, please power off, add a new disk with at least 257GB space to the OV VM using
hypervisor and then power on the OV 2500 and go to 4-Configure current Node, select 17-Extend part
itions, then select 2-Omnivista Data Partition
(Please perform this action on all nodes with exact same size)
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [y|n] (n):
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Data Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The following prompt will appear and the HA Virtual Appliance Menu is displayed.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

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

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

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

Upgrade the Standby Node to 4.6R1

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
```

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

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

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.6R1
* [0] Exit
*****
(*) Type your option:
```

3. Enter **1 - Upgrade to 4.6R1** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 0

Checking available packages for 4.6R1 operation is in progress...
Upgrade to 4.6R1 release is available after upgrading latest to version/patch of 4.5R3 release
Do you want to continue to check upgrade for 4.5R3 release now [yin] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.6R1.

```
Getting upgrade information for 4.5R3...
Current version of Virtual Appliance is the latest build of 4.5R3

Getting upgrade information for 4.6R1...
Upgrade information for 4.6R1
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.6R1
Release   : 44.0.e17
Size      : 1.5 G
Repo      : CustomRepo1_4.6R1
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 chosen to upgrade to latest build of 4.6R1 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):
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [y|n] (n):
```

9. Type **y** then press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 10, page 61).

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.6R1 GA
Build Number: 44
Patch Number: 0
Build Date: 09/17/2021
Technical Support Code: 12345678
ooZ login: _
```

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Would you like to continue to reboot the system? [y|n] (n):
```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Data Partitions. Select “OmniVista Data Partition” for the Logical Volume Type. This must be performed on **both** nodes.
Note: Do **not** power off or reset the VM until the operation completes.

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

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

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

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

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

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

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

Verify the Upgrade

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

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

on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.6R1. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Upgrading from 4.5R2 to 4.5R3

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R2 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.5R3 Standalone or High-Availability Installation.

Upgrading from 4.5R2 Standalone to 4.5R3 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R2 Standalone Installation to an OV 2500 NMS 4.5R3 Standalone Installation.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista may take up to a day to purge the older data, but it is recommended as a way to save disk space.

Note that OV 2500 NMS 4.5R3 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

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

1. Open a Console on the OV 2500 NMS 4.5R2 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
* [12] Convert to Cluster
* [13] Join Cluster
* [0] Log Out
*****
(*) Type your option:
```

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

```

*****
* Upgrade Un
*****
* [1] Help
* [2] To 4.5R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: _
    
```

3. Enter **3** – **To New Release** and press **Enter**. The Upgrade to New Release Screen will appear.

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.5R3
* [0] Exit
*****
(*) Type your option:
    
```

4. Enter **1** – **Upgrade to 4.5R3** and press **Enter**. The Upgrade System Options Screen will appear.

```

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

5. Enter **2** – **Download and Upgrade** and press **Enter**. Information on the current installation is displayed and OmniVista checks the Repository for the latest 4.5R2 upgrade packages.

Note: You **must** select 2 – Download and Upgrade. Option 4 – Upgrade from downloaded package is **not** supported.

```

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R2 GA
Build Number: 71
Patch Number: 0

Checking available packages for 4.5R3 operation is in progress...
Upgrade to 4.5R3 release is available after upgrading latest to version/patch of 4.5R2 release
Do you want to continue to check upgrade for 4.5R2 release now [yin] (n):
    
```

6. Enter **y** and press **Enter** to continue. OmniVista retrieves and displays upgrade information for 4.5R3.

```
Getting upgrade information for 4.5R2...
Current version of Virtual Appliance is the latest build of 4.5R2

Getting upgrade information for 4.5R3...
Upgrade information for 4.5R3
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.5R3
Release   : 67.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.5R3
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 chosen to upgrade to latest build of 4.5R3 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Installation guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y/n] (n): _
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following message will appear and the upgrade will begin.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (11s)...
```

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

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

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

8. When the installation is complete, the following prompt will appear “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 0
Build Date: 03/18/2021
Technical Support Code: alcatel
omnivista login: _
```

9. Log into the VM. The Virtual Appliance Menu will appear.

```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```

The system HDD2 (256GB) is less than the minimum required (512GB).
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later [yn] (n): _
    
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below. If you plan to extend the data partition at a later time, go to Step 10.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.
 - On the Configure the Virtual Appliance Menu, select **9** – Configure Network Size, then select **4** – Extend Data Partition.

Note: Do **not** power off or reset the VM until the operation completes.

For detailed procedures on extending the data partition at a later time, go to the [Configure Network Size Menu](#) and select Option **4 – Extend the Data Partition**.

10. Verify the upgrade.

- Verify that the Build Number is correct.
 - From The Virtual Appliance Menu, select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See [Display Current Configuration](#) for more details.

- Verify that all services have started.
 - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
 - Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See [Run Watchdog Command](#) for more details.

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.5R3.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance**.
 2. Select **2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
 3. Select **9 - Configure Network Size**.
 4. Select **2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
 5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.5R2 HA to 4.5R3HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R2 High-Availability Installation to an OV 2500 NMS 4.5R3 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

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

Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.

- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista may take up to a day to purge the older data, but it is recommended as a way to save disk space.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OV 2500 NMS 4.5R3 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

High-Availability Upgrade Workflow

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

1. [Enable Maintenance Mode on the Active Node](#)
2. [Upgrade the Active Node to 4.5R3](#) (as part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
3. [Upgrade the Standby Node to 4.5R3](#)
4. [Disable Maintenance Mode on the Active Node](#)
5. [Verify the Upgrade.](#)

Enable Maintenance Mode on the Active Node

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node. Open a Console on the OV 2500 NMS 4.5R2 Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

```

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [yin] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

Upgrade the Active Node to 4.5R3

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: _
    
```

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

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.5R3
* [0] Exit
*****
(*) Type your option: _
    
```

3. Enter **1 - Upgrade to 4.5R3** and press **Enter** to bring up the Upgrade System Options Menu.

```

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

4. Enter **2** – **Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R2 GA
Build Number: 71
Patch Number: 0

Checking available packages for 4.5R3 operation is in progress...
Upgrade to 4.5R3 release is available after upgrading latest to version/patch of 4.5R2 release
Do you want to continue to check upgrade for 4.5R2 release now [yin] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.5R3.

```
Getting upgrade information for 4.5R3...
Upgrade information for 4.5R3
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.5R3
Release   : 67.0.e17
Size      : 1.6 G
Repo      : CustomRepo1_4.5R3
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 chosen to upgrade to latest build of 4.5R3 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 ?[yin] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Installation guide, Release Notes of new release prior to this.
Are you ready to proceed ? [yin] (n): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [Enter] to reboot.
_
```

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

9. [Upgrade the Standby Node to 4.5R3](#). After upgrading the Standby Node, return to this screen and continue with Step 10 below to reboot the Active Node and complete the upgrade process.

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

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 0
Build Date: 03/10/2021
Technical Support Code: alcatel
ovl login: _
```

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources now? Choose 'n' to do it later [yn] (n): _
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
3. Power on the VM.
4. Extend the data partition on the second hard disk.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Data Partitions. Select “**lvdatasync**” for the Logical Volume Type. This must be performed on **both** nodes.

Note: Do **not** power off or reset the VM until the operation completes.

The following prompt will appear and The HA Virtual Appliance Menu is displayed.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

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

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

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

Upgrade the Standby Node to 4.5R3

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade UA
*****
* [1] Help
* [2] To 4.5R2 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: _
```

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

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

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.5R3
* [0] Exit
*****
(*) Type your option: _
```

3. Enter **1 - Upgrade to 4.5R3** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. You **must** select Option 2 – Download and Upgrade. Option 4 – Upgrade from a Downloaded Package is not supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R2 GA
Build Number: 71
Patch Number: 0

Checking available packages for 4.5R3 operation is in progress...
Upgrade to 4.5R3 release is available after upgrading latest to version/patch of 4.5R2 release
Do you want to continue to check upgrade for 4.5R2 release now [y/n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.5R3.

```
Getting upgrade information for 4.5R3...
Upgrade information for 4.5R3
Available Packages
Name       : ovmmse
Arch       : x86_64
Version    : 4.5R3
Release    : 67.0.e17
Size       : 1.6 G
Repo       : CustomRepo1_4.5R3
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 chosen to upgrade to latest build of 4.5R3 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Installation guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade. The following screen will appear.

```
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries to
remove unexisting files. You can ignore them.
Press any key to continue the upgrade (13s)...
```

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [Enter] to reboot.
```

9. Press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 10, page 60).

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 8
Build Date: 03/18/2021
Technical Support Code: alcatel
ov2 login: _
```

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

Note: If your Hypervisor HDD2 capacity is less than the minimum recommended configuration for the network size configured, a prompt such as the one below, will appear after you log into the VM.

```
The system HDD2 (256GB) is less than the minimum required (512GB).
Would you like to proceed with powering off the Virtual Appliance and reconfigure the VM resources n
ow? Choose 'n' to do it later (yn): _
```

You can press **Enter** to accept the default of “no” to complete the upgrade and perform the HDD2 upgrade later; or enter **y** and press **Enter** to power off the VM and extend the data partition for HDD2 now. It is highly recommended that you configure HDD2 as detailed in [Required Minimum System Configurations](#). For detailed procedures on extending the data partition at a later time, go to the [Extend Data Partition Menu](#).

Extending the data partition requires the installation of a second hard disk. If you are prepared to install a new hard disk, you can extend the hard disk now by following the steps below.

1. Enter **y** and press **Enter** to power off the VM.
 2. Add hardware for additional disk space. You **must** install a second hard disk. Resizing of the existing hard disk is not supported.
 3. Power on the VM.
 4. Extend the data partition on the second hard disk.
 - On the HA Virtual Appliance Menu, select **4** – Configure Current Node, then select **17** – Extend Data Partitions. Select “**lvdatasync**” for the Logical Volume Type. This must be performed on **both** nodes.
- Note:** Do **not** power off or reset the VM until the operation completes.

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

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

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

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

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

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

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

Verify the Upgrade

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

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

on the amount of data and the network speed between the two Nodes. See [Show OV Cluster Status](#) for more details.

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.5R3. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Upgrading from 4.5R1 to 4.5R2

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R1 [Standalone](#) or [High-Availability](#) Installation to an OV 2500 NMS 4.5R2 Standalone or High-Availability Installation.

Upgrading from 4.5R1 Standalone to 4.5R2 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R1 Standalone Installation to an OV 2500 NMS 4.5R2 Standalone Installation.

Important Notes: Before beginning the upgrade:

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista may take up to a day to purge the older data, but it is recommended as a way to save disk space.

Note that OV 2500 NMS 4.5R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

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

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

1. Open a Console on the OV 2500 NMS 4.5R1 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
* [12] Convert to Cluster
* [13] Join Cluster
* [0] Log Out
*****
(*) Type your option:
```

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade Ua
*****
* [1] Help
* [2] To 4.5R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: _
```

3. Enter **2** – **To 4.5R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2** – **Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the “Install” Prompt. Note that you **must** select **2** – **Download and Upgrade**. Option 4 – Upgrade from downloaded package is **not** supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 0

Checking available packages for 4.5R1 operation is in progress...
Upgrade information for 4.5R1
Available Packages
Name       : ovmnsepatchb51
Arch      : x86_64
Version   : 4.5R1
Release   : 51.2.e17
Size      : 2.1 M
Repo      : CustomRepo1_4.5R1
Summary   : OU Patch 2 for 4.5R1 build 51
URL       : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&
;page=overview
License   : ALE USA Inc.
Description : Patch 2 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E 4.5R1
           : build 51
           : -----
           : Fix CRNOU-2077 OS6350-10 : Cloud-Agent - Call Home Request
           : Returned Failure Due To SSL Certificate Expired
           :
           : Fix OVE-8279: [Customer Issue] Support multipart for
           : HamLocatorServiceQueue
           : -----

Would you like to install the package [yin] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [yin] (n): _
```

5. Enter **y** and press **Enter** at the Confirmation Prompts to apply the patch.
6. The installation will take several minutes. When the installation is complete, the following message will appear. Press **Enter** to continue. The VM will be rebooted.

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

When the reboot is complete, the login screen will appear. Note the Build Number and Patch Number displayed (e.g., Build Number 51, Patch 2).

```
CentOS Linux 7 (Core)  
Kernel 3.10.0-957.el7.x86_64 on an x86_64  
  
Technical Support Code: alcatel  
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA  
Build Number: 51  
Patch Number: 2  
Build Date: 04/06/2020  
omnivista login: _
```

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

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

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

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

```
*****  
* Upgrade VA  
*****  
* [1] Help  
* [2] To 4.5R1 (Upgrade to Latest patch of Current Release, if any)  
* [3] To New Release  
* [4] Enable Repository (Selected - ALE Central Repo)  
* [5] Configure Custom Repositories  
* [6] Configure "Update Check Interval" (Selected - Disabled)  
* [7] Backup/Restore OmniVista 2500 NMS Data  
* [0] Exit  
*****  
(* Type your option:
```

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.5R2
* [0] Exit
*****
(*) Type your option: _
```

10. Enter **1** - **Upgrade to 4.5R2** and press **Enter** to bring up the Upgrade System Options Menu.

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

11. Enter **2** – **Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the “Install” Prompt. Note that you **must** select **2 – Download and Upgrade**. Option 4 – Upgrade from downloaded package is **not** supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 2

Checking available packages for 4.5R2 operation is in progress...
Upgrade to 4.5R2 release is available after upgrading latest to version/patch of 4.5R1 release
Do you want to continue to check upgrade for 4.5R1 release now [yin] (n): _
```

12. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.5R2.

```
Getting upgrade information for 4.5R2...
Upgrade information for 4.5R2
Available Packages
Name       : ovmse
Arch       : x86_64
Version    : 4.5R2
Release    : 65.0.e17
Size       : 1.4 G
Repo       : CustomRepo1_4.5R2
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 chosen to upgrade to latest build of 4.5R2 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 ?[yin] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed ? [yin] (n):
```

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

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

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

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

14. When the installation is complete, the following prompt will appear “Complete! Operation Successful”. Press **Enter** to continue. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt.

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

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R2 GA
Build Number: 65
Patch Number: 0
Build Date: 09/18/2020
Technical Support Code: alcatel
omnivista login:
```

15. Log into the VM and verify the upgrade.

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

Launching the OmniVista UI

Once all services are running after upgrading, enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.5R2.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
 1. From the Virtual Appliance Menu. **Select 2 - Configure the Virtual Appliance**.
 2. **Select 2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).

3. Select **9 - Configure Network Size**.
4. Select **2 - Configure OV2500 Memory**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
5. At the Watchdog Service prompt, press **Enter** to restart Watchdog Services.

Upgrading from 4.5R1 HA to 4.5R2 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS 4.5R1 High-Availability Installation to an OV 2500 NMS 4.5R2 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

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

Note that OV 2500 NMS 4.5R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can

take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

High-Availability Upgrade Workflow

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

1. [Enable Maintenance Mode on the Active Node](#)
2. [Upgrade the Active Node to the Latest 4.5R1 Patch](#) (As part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
3. [Upgrade the Standby Node to the Latest 4.5R1 Patch](#)
4. [Disable Maintenance Mode on the Active Node](#) (Make sure the cluster is synchronized before going to Step 5. See procedure for details.)
5. [Enable Maintenance Mode on the Active Node](#) (to continue upgrade to 4.5R2)
6. [Upgrade the Active Node to 4.5R2](#) (as part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
7. [Upgrade the Standby Node to 4.5R2](#)
8. [Disable Maintenance Mode on the Active Node](#) (You **must** disable Maintenance Mode on the Active Node to complete the upgrade.)
9. [Verify the Upgrade](#).

Enable Maintenance Mode on the Active Node

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node. Open a Console on the OV 2500 NMS 4.5R1 Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y;n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

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

```

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

Upgrade the Active Node to the Latest 4.5R1 Patch

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

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

2. Enter **2 – To 4.5R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

```

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

3. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the “Install” Prompt. Note that you **must** select **2 – Download and Upgrade**. Option 4 – Upgrade from downloaded package is **not** supported.

```

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 0

Checking available packages for 4.5R1 operation is in progress...
Upgrade information for 4.5R1
Available Packages
Name       : ovmnsepatchb51
Arch      : x86_64
Version   : 4.5R1
Release   : 51.2.e17
Size      : 2.1 M
Repo      : CustomRepo1_4.5R1
Summary   : OV Patch 2 for 4.5R1 build 51
URL       : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&
;page=overview
License   : ALE USA Inc.
Description : Patch 2 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E 4.5R1
           : build 51
           : -----
           : Fix CRNDU-2077 OS6350-10 : Cloud-Agent - Call Home Request
           : Returned Failure Due To SSL Certificate Expired
           :
           : Fix OVE-8279: [Customer Issue] Support multipart for
           : HamLocatorServiceQueue
           : -----

Would you like to install the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y/n] (n):

```

4. Enter **y** and press **Enter** at the Confirmation Prompt to apply the patch. The following prompt will appear. You can press any key to continue or just wait until the countdown completes.

```

Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (0s)...

```

5. When the installation is complete, the following message will appear. Press **Enter** to continue.

```

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

```

A second prompt will appear.

```

The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [Enter] to reboot.

```

Do not press Enter at the second prompt to reboot the VM. Reboot the VM and complete the upgrade to the latest 4.5R1 Patch **after** upgrading the Standby Node to the latest 4.5R1 Patch.

6. [Upgrade the Standby Node to the latest 4.5R1 patch](#). After upgrading the Standby Node, return to this screen and continue with Step 7 below to reboot the Active Node and complete the upgrade process.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

8. The reboot process will take several minutes. When the reboot is complete, the login screen will appear. Note the Build Number and Patch Number displayed (e.g., Build Number 51, Patch 2).

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

Technical Support Code: alcatel
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 2
Build Date: 04/06/2020
ov1 login:
```

9. Log into the VM. The following prompt will appear, followed by The HA Virtual Appliance Menu.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

This prompt is just a reminder. Do **not** disable Maintenance Mode at this time. You will disable Maintenance Mode after the upgrade of **both** Nodes to the latest 4.5R1 Patch is complete.

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

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

11. Verify that the Patch Number is correct (e.g., Patch Number 2). On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See [Display Current Node Configuration](#) for more details.

Upgrade the Standby Node to the Latest 4.5R1 Patch

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

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

2. Enter **2 – To 4.5R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

```

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

3. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the “Install” Prompt. Note that you **must** select **2 – Download and Upgrade**. Option 4 – Upgrade from downloaded package is **not** supported.

```

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 0

Checking available packages for 4.5R1 operation is in progress...
Upgrade information for 4.5R1
Available Packages
Name       : ovmsepatchb51
Arch      : x86_64
Version   : 4.5R1
Release   : 51.2.e17
Size      : 2.1 M
Repo      : CustomRepo1_4.5R1
Summary   : OV Patch 2 for 4.5R1 build 51
URL       : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&
;page=overview
License   : ALE USA Inc.
Description : Patch 2 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E 4.5R1
           : build 51
           : -----
           : Fix CRNOV-2077 OS6350-10 : Cloud-Agent - Call Home Request
           : Returned Failure Due To SSL Certificate Expired
           :
           : Fix OVE-8279: [Customer Issue] Support multipart for
           : HamLocatorServiceQueue
           : -----

Would you like to install the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y/n] (n):

```

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

```

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

```

A second prompt will appear.

```

The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [Enter] to reboot.

```

6. Press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 7, page 61).
7. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.
8. Log into the VM. The following prompt will appear, followed by The HA Virtual Appliance Menu.

```

=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
    
```

This prompt is just a reminder. Do **not** disable Maintenance Mode at this time. You will disable Maintenance Mode after the upgrade of **both** Nodes to the latest 4.5R1 Patch is complete.

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

```

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

10. Verify that the Patch Number is correct (e.g., Patch Number 2). On the HA Virtual Appliance Menu, select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See [Display Current Node Configuration](#) for more details.

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

```

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

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

```

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

```

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

```

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

5. Enter **0 – Exit** and press **Enter**, to return to the HA Virtual Appliance Menu.

```

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

```

OmniVista will complete the upgrade to the latest 4.5R1 Patch. Before [Enabling Maintenance Mode on the Active Node](#), verify that the cluster is in sync. Enter **2 – Show OV Cluster Status** and make sure the “Data Sync” Field indicates “Up to Date”.

Enable Maintenance Mode on the Active Node

1. Before performing the upgrade to OV 2500 NMS 4.5R2, you must first enable Maintenance Mode on the Active Node. This will enable Maintenance Mode on both nodes in the Cluster. Open a Console on the Active Node.

```

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to enable Maintenance Mode [y;n] (n): y
The configuration has been set
Press [Enter] to continue

Please do not perform any Cluster Configuration actions before disabling Maintenance Mode!!!
Press [Enter] to continue
    
```

4. On the Configure Cluster Menu, enter **0 – Exit** and press **Enter** to return to the HA Virtual Appliance Menu.

```

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

Upgrade the Active Node to 4.5R2

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

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

```
*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.5R2
* [0] Exit
*****
(*) Type your option: _
```

3. Enter **1 - Upgrade to 4.5R2** and press **Enter** to bring up the Upgrade System Options Menu.

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

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the “Install” Prompt. Note that you **must** select **2 – Download and Upgrade**. Option 4 – Upgrade from downloaded package is **not** supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 2

Checking available packages for 4.5R2 operation is in progress...
Upgrade to 4.5R2 release is available after upgrading latest to version/patch of 4.5R1 release
Do you want to continue to check upgrade for 4.5R1 release now [yin] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.5R2.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
Getting upgrade information for 4.5R2...
Upgrade information for 4.5R2
Available Packages
Name       : ovmnse
Arch      : x86_64
Version   : 4.5R2
Release   : 65.0.e17
Size      : 1.4 G
Repo      : CustomRepo1_4.5R2
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 chosen to upgrade to latest build of 4.5R2 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Installation guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y/n] (n):
```

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

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [Enter] to reboot.
```

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

9. [Upgrade the Standby Node to 4.5R2](#). After upgrading the Standby Node, return to this screen and continue with Step 10 below to reboot the Active Node and complete the upgrade process.

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

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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R2 GA
Build Number: 64
Patch Number: 0
Build Date: 09/08/2020
Technical Support Code: alcatel
ov2 login: _
```

12. Log into the VM. The following prompt will appear, followed by The HA Virtual Appliance Menu.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

This prompt is just a reminder. When the upgrade is complete on **both** Nodes (including reboot **and** login on **both** Nodes), you will disable Maintenance Mode on the Active Node.

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

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

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

Upgrade the Standby Node to 4.5R2

```

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

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R1 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: _
    
```

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

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

```

*****
* Upgrade to New Release
*****
* [1] Upgrade to 4.5R2
* [0] Exit
*****
(*) Type your option: _
    
```

3. Enter **1 - Upgrade to 4.5R2** and press **Enter** to bring up the Upgrade System Options Menu.

```

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

4. Enter **2** – **Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the “Install” Prompt. Note that you **must** select **2 – Download and Upgrade**. Option 4 – Upgrade from downloaded package is **not** supported.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R1 GA
Build Number: 51
Patch Number: 2

Checking available packages for 4.5R2 operation is in progress...
Upgrade to 4.5R2 release is available after upgrading latest to version/patch of 4.5R1 release
Do you want to continue to check upgrade for 4.5R1 release now [y/n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.5R2.

```
Getting upgrade information for 4.5R2...
Upgrade information for 4.5R2
Available Packages
Name       : ovmnse
Arch       : x86_64
Version    : 4.5R2
Release    : 65.0.e17
Size       : 1.4 G
Repo       : CustomRepo1_4.5R2
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 chosen to upgrade to latest build of 4.5R2 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): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Install guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y/n] (n): _
```

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

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

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

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

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

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

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

```
The Virtual Appliance has to be restarted for applying new changes
WARNING:
Do NOT proceed with reboot of this node if the other node in the cluster is not upgraded yet.
Proceed with reboot of this node only when both nodes in the cluster are upgraded successfully.
After both nodes are rebooted, you must turn off the Maintenance Mode.

Press [Enter] to reboot.
```

9. Press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 10, page 69).

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

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

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R2 GA
Build Number: 65
Patch Number: 0
Build Date: 09/18/2020
Technical Support Code: alcatel
ool login:
```

11. Log into the VM. The following prompt will appear, followed by The HA Virtual Appliance Menu.

```
=====
Warning: Cluster Maintenance mode is On.
OmniVista will not work correctly until you turn off Cluster Maintenance mode.
=====
```

This prompt is just a reminder. When the upgrade is complete on **both** Nodes (including reboot **and** login on **both** Nodes), you will disable Maintenance Mode on the Active Node.

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

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

When the upgrade is complete on **both** Nodes (including reboot **and** login on **both** Nodes), [disable Maintenance Mode on the Active Node](#). You **must** disable Maintenance Mode on the Active Node to complete the upgrade. Once Maintenance Mode is disabled, the nodes will begin to sync and services will be started on both nodes.

Disable Maintenance Mode on the Active Node

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

1. Go to the HA Virtual Appliance Menu.

```

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

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

```

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

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

```

If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both nodes are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

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

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

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

5. Enter **0 – Exit** and press **Enter**, to return to the HA Virtual Appliance Menu.

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

Verify the Upgrade

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

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

You can now [launch the OmniVista UI](#).

Launching the OmniVista UI

Enter `https://<OVServerIPAddress>` in a supported browser to launch OV 2500 NMS 4.5R2. This is the Virtual IP address that you configured for the cluster.

Important Notes for Stellar APs:

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

Appendix A – Using the Virtual Appliance Menu

To access the Virtual Appliance Menu for a VM, launch the Hypervisor Console. The login prompt is displayed.

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.5R3 GA
Build Number: 67
Patch Number: 0
Build Date: 03/18/2021
Technical Support Code: alcatel
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
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option:
```

The Virtual Appliance Menu provides the following options:

- [1 - Help](#)
- [2 - Configure the Virtual Appliance](#)
- [3 - Run Watchdog Command](#)
- [4 - Upgrade/Backup/Restore VA](#)
- [5 - Change Password](#)
- [6 - Logging](#)
- [7 - Login Authentication Server](#)
- [8 - Power Off](#)
- [9 - Reboot](#)

- [10 - Advanced Mode](#)
- [11 - Set Up Optional Tools](#)
- [12 - Convert to Cluster](#)
- [13 - Join Cluster](#)
- [14 - Troubleshoot](#)
- [0 - Log Out](#)

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

Help

Enter **1** and press **Enter** to bring up help for the Virtual Appliance Menu.

Configure the Virtual Appliance

The “Configure the Virtual Appliance” menu provides the following options:

- [1 - Help](#)
- [2 - Display Current Configuration](#)
- [3 - Configure IPs & Ports](#)
- [4 - Configure Default Gateway](#)
- [5 - Configure Hostname](#)
- [6 - Configure DNS Server](#)
- [7 - Configure Timezone](#)
- [8 - Configure Route](#)
- [9 - Configure Network Size](#)
- [10 - Configure Keyboard Layout](#)
- [11 - Update OmniVista Web Server SSL Certificate](#)
- [12 - Enable/Disable AP SSL Authentication](#)
- [12 - Enable/Disable Admin SSH](#)
- [14 - Configure NTP Client](#)
- [15 - Configure Proxy](#)
- [16 - Change Screen Resolution](#)
- [17 - Configure the Other Network Cards](#)
- [0 - Exit](#)

```
*****
* Configure The Virtual Appliance
*****
* [1] Help
* [2] Display Current Configuration
* [3] Configure IPs and Ports
* [4] Configure Default Gateway
* [5] Configure Hostname
* [6] Configure DNS Server
* [7] Configure Timezone
* [8] Configure Route
* [9] Configure Network Size
* [10] Configure Keyboard Layout
* [11] Update OmniVista Web Server SSL certificate
* [12] Enable/Disable AP SSL Authentication
* [13] Enable/Disable Admin SSH
* [14] Configure NTP Client
* [15] Configure Proxy
* [16] Change screen resolution
* [17] Configure the other Network Cards
* [0] Exit
*****
```

Help

Enter **1** and press **Enter** to bring up help for the Configure The Virtual Appliance Menu.

Display Current Configuration

Enter **2** and press **Enter** to display the current VA configuration. Press **Enter** to return to the Configure The Virtual Appliance Menu.

```
*****
* Current configuration
*****
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.8R1 GA
Build Number: 39
Patch Number: 0
Build Date: 07/31/2023
MMH Version: 4.8.1.16
JPAM Version: 4.8.1.17
ZCS Version: 4.8.1.1
UCC Version: 4.8.1.1

Current OV IP Configuration:
  IP: 10.255.221.27
  Netmask: 255.255.255.0
  NIC: eth0
  MAC: 00:15:5d:dd:4f:4c
  OV Web HTTP Port: 80
  OV Web HTTPS Port: 443
*****
```

Configure IPs and Ports

1. If you want to re-configure the current OV IP, Captive Portal IP and Ports, and optional Additional Web OV IP, enter **3** and press **Enter**. The current configuration will be displayed. Enter **y** and press **Enter** at the first confirmation prompt to re-configure the OV IP and Web Ports.

```

Current OV IP Configuration:
  IP: 10.255.222.98
  Netmask: 255.255.255.0
  NIC: eth0
  MAC: 00:0c:29:c5:f1:32
  OV Web HTTP Port: 80
  OV Web HTTPS Port: 443
Would you like to configure OV IP and OV Web Ports [yin] (n): y
Please input OV IPv4 [10.255.222.98]:
Please input subnet mask [255.255.255.0]:
We have only one unused NIC [eth0-00:0c:29:c5:f1:32], so use it for OV IP too
Please input OV Web HTTP port [80]:
Please input OV Web HTTPS port [443]:
Would you like to configure OV IP with:
  IPv4: 10.255.222.98
  Netmask: 255.255.255.0
  NIC: eth0-00:0c:29:c5:f1:32
  OV Web HTTP Port: 80
  OV Web HTTPS Port: 443
[yin] (y):
  
```

2. Enter an IPv4 IP address and subnet mask.
3. Enter **y** at the confirmation prompt and press **Enter** to confirm the settings.
4. After configuring the OV IP address, configure the OV ports.
5. At the prompt, enter an HTTP value and press **Enter**. Enter an HTTPS value and press **Enter**.
 - HTTP Port (Valid range: 1024 to 65535, Default = 80)
 - HTTPS Port (Valid range: 1024 to 65535, Default = 443)

Note: You can press **Enter** to accept default values. New port values must be unique (i.e., they must differ from any previously-configured ports).
6. Enter **y** and press **Enter** to confirm the settings.
7. At the Captive Portal Configuration Prompt, enter **y** and press **Enter** to configure the Captive Portal Ports, otherwise press **Enter** to continue. The Captive Portal IP address can be the same as the OV IP address or different. However, if you use a different IP address for Captive Portal it is recommended that you use the default ports. If you do not use the default ports, the ports should be >1024.
 - HTTP Port (Valid range: 1024 to 65535, Default = 8080)
 - HTTPS Port (Valid range: 1024 to 65535, Default = 8443)

Note: The default Captive Portal FQDN is "ov2500-upam-cportal.al-enterprise.com". If you want to replace it with your own FQDN you must:

 1. Log into the OmniVista UI.
 2. Go to the UPAM – Captive Portal Certificates page (U PAM – Settings – Captive Portal Certificates).
 - Create a Custom Certificate.
 - Activate the certificate.
8. At the Additional OV Web IP Prompt, enter **y** and press **Enter** to configure an Additional OV Web IP, otherwise press **Enter** to continue. An additional OV Web IP address provides you with another way of accessing the OmniVista UI. It is optional. The OV Web IP address must be

configured on a different NIC and different subnet than the OmniVista IP and Captive Portal IP. If an additional NIC is not available, it cannot be enabled.

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

Important Note: If you change the OV IP address in the VA Menu, the network is NOT touched. For wired devices, you must reconfigure the sFlow receiver, policy server, and SNMP trap station. After changing the IP Address of the OV Server, you must manually push configurations from various applications (Analytics, Policy View QoS, and Notification applications respectively) to inform the network about the new location of the OV Server. For Stellar APs, you must reconfigure the DHCP Server, and reapply WLAN Services and Global Configurations in Unified Access.

Note: If OmniVista is unreachable after you change the OmniVista Server IP address, reboot the OmniVista Server.

Configure Default Gateway

1. Enter **4** and press **Enter** to configure default gateway settings.

```
*****
* Configure Default Gateway
*****
Please input default gateway v4 [10.255.222.62]:
Would you like to configure:
    default gateway: 10.255.222.62
[y;n] (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 **5** and press **Enter**.

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

2. Enter a hostname (maximum of 15 characters).
3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure DNS Server

1. Enter **6** to specify whether the VM will use a DNS Server.
2. If the VM will use a DNS server, enter **y**, then press **Enter**. Enter the IPv4 address for Server 1 and Server 2, if applicable.

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

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

3. Enter **y** and press **Enter** to confirm the settings. You will be prompted to restart the OV Client Service for the change to take effect. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Timezone

1. Enter **7** and press **Enter** to begin setting up the timezone.

```
*****  
* Configure Timezones *  
*****  
The available timezones list will be shown (press [q] to exit view mode)  
Press [Enter] to continue  
_
```

2. Press **Enter** to display timezones.

```

Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
Africa/Douala
Africa/El_Aaiun
Africa/Freetown
Africa/Gaborone
Africa/Harare
Africa/Johannesburg
Africa/Juba
Africa/Kampala
Africa/Khartoum
Africa/Kigali
Africa/Kinshasa
Africa/Lagos
Africa/Libreville
Africa/Lome
Africa/Luanda
Africa/Lubumbashi
Africa/Lusaka
lines 1-36

```

2. Press **Enter** to scroll through the list. After locating your timezone, press **q** and enter your timezone at the prompt (e.g., America/Los_Angeles). Then press **Enter** to set the timezone and return to the Configure Current Node Menu.

```

America/La_Paz
America/Lima
America/Los_Angeles
Please input timezones [America/Los_Angeles]: America/Los_Angeles
Would you like to set:
    timezones: America/Los_Angeles
[yin] (y):
The configuration has been set
Press [Enter] to continue

```

You can verify the change using the **2 - Display Current Configuration** command.

Configure Route

1. If you want to add a static route from the VM to another network enter **8** and press **Enter**.
2. Add an IPv4 route by entering **3** at the command prompt.

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

At the Main Menu prompt, enter **9** and press **Enter** to display the Configure Network Size Menu, and select one of the options below.

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

- **Configure OV2500 Memory** - Select an option (e.g., Low, Medium, High, Very High) based on the number of devices being managed and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. You will be prompted to restart the Watchdog Service for the change to take effect. See [Required Minimum System Configurations](#) for more information on system configurations for the different network sizes.
- **Configure Swap File** - Select one of the options below:
 - **Show Current Swap Files** - Enter **1** and press **Enter** to display information about any configured Swap Files.
 - **Add Swap File** - Enter the size of the Swap File in MB (Range = 1 - 4096). Enter **y** and press **Enter** at the confirmation prompt.
 - **Delete Swap File** - Select the Swap File you want to delete and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
- **Extend Data Partition** - Follow the steps [below](#) to Extend the Data Partition. By default, OmniVista is partitioned as follows: HDD1:50GB and HDD2:512GB. If you are managing more than 500 devices, it is recommended that you increase the provisioned hard disk. Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. **Insufficient memory or disk space for the chosen network size may cause OV instability.** OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 20GB of memory for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to [Recommended System Configurations](#) for details.

Important Notes:

- When deploying the OmniVista VA for the first time, do not add the new disks in the hypervisor until after OmniVista is configured and rebooted.
- If you have a KVM deployment, when adding new storage, select Bus Type = SATA for new storage in KVM Settings. OmniVista only supports new storage in the SATA format.
- OmniVista on KVM does not detect the first two disks but does detect the third disk onward. For example. If you deployed OmniVista on KVM with "VirtIO disk1" and "VirtIO disk2" and then added three more SATA disks (SATA disk1", "SATA disk2" and "SATA disk3), when you navigate the VA menu to extend the disk space, OmniVista only detects "SATA disk3".
- To extend the disk space for OmniVista on KVM:
 1. Add "SATA disk1" with 1KB capacity because OmniVista will not detect it.
 2. Add "SATA disk2" with 1KB capacity because OV will not detect it.
 3. Add "SATA disk3" with the desired capacity (20GB, 50GB...).
 4. Go to the VA menu and use the "SATA disk3" to extend the disk space.
 5. Do not remove "SATA disk1" and "SATA disk2".

Extending the Data Partition

1. Shut down OmniVista Services from the OV Virtual Appliance console.
 - On the main Virtual Appliance Menu, select **3** – [Run Watchdog Command](#), then select **9** – Shutdown Watchdog. Wait for all services and Watchdog to shut down.
2. Take a VM Snapshot or use the OmniVista Backup Command in the Virtual Appliance Menu.
 - To perform a backup, go to the main Virtual Appliance Menu, select **4** – [Upgrade/Backup/Restore VA](#), select **7** – Backup/Restore OmniVista 2500 NMS Data, then select **3** – Backup Now.
3. Power off the VM from the OV Virtual Appliance console.
 - On the main Virtual Appliance Menu, select **8** – [Power Off](#).
4. Add hardware for additional disk space from the hypervisor.
5. Power on the VM using the hypervisor menu option.
6. Extend the disk from the OV Virtual Appliance console.
 - On the Configure the main Virtual Appliance Menu, select **2** - Configure the Virtual Appliance Menu, select **9** – Configure Network Size, then select **4** – Extend Data Partition.

Notes:

1. Do **not** power off or reset the VM until the operation completes.
2. Always power off VM using the OV Virtual Appliance Menu option.

Configure Keyboard Layout

1. Enter **10** and press **Enter** to specify a keyboard layout.

```

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

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

3. Enter **q** and press **Enter** to quit the view mode. At the prompt, enter a keyboard layout then press **Enter**. Enter **y** at the confirmation prompt and press **Enter**. Press **Enter** to return to The Virtual Appliance Menu.

```

Please input keyboard layout [us]:
Would you like to set:
    keyboard layout: us
[yin] (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-noddeadkeys	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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

ru-cp1251	ruwin_alt-CP1251	ru	it2
lt.l4	ua-utf	bywin-cp1251	bg-cp1251
ru_win	emacs2	dk-latin1	kazakh
br-abnt2	es	pl4	mk0
is-latin1	is-latin1-us	il-phonetic	fi-old
et-nodeadkeys	jp106	lt	ru2
ruwin_ct_sh-UTF-8	pt	se-fi-ir209	gr-pc
lt.baltic	tr_q-latin5	pl3	ua-utf-ws
bashkir	no-dvorak	dvorak-r	dvorak
ANSI-dvorak	dvorak-l	mac-euro	mac-euro2
mac-fr_CH-latin1	mac-us	mac-de-latin1	mac-be
mac-es	mac-pl	mac-se	mac-dvorak
mac-fi-latin1	mac-template	mac-dk-latin1	mac-de-latin1-nodeadkeys
mac-fr	mac-pt-latin1	mac-uk	mac-it
mac-de_CH	sunt4-no-latin1	sunt5-cz-us	sundvorak
sunt5-de-latin1	sunt5-us-cz	sunt5-es	sunt4-fi-latin1
sunkeymap	sunt4-es	sunt5-ru	sunt5-uk
sun-pl	sunt5-fr-latin1	sunt5-fi-latin1	sun-pl-altgraph

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

Update OmniVista Web Server SSL Certificate

To update the OmniVista Web Server SSL Certificate, you must first generate a *.crt and *.key file and use an SFTP Client to upload the files to the VA. Make sure the destination directory is "keys".

- **SFTP User:** cliadmin
- **SFTP Password:** <password when deploying VA>
- **SFTP Port:** 22

1. Enter **11** and press **Enter**.

2. Choose a certificate file (.crt) and enter **y** and press **Enter**. Choose a private key file (.key) and enter **y** and press **Enter**.

```

*****
* Update OmniVista Web Server SSL certificate
*****
* Available certificate(s)
*****
* [1] ov_server.crt
* [0] Exit
*****
(*) Type your option: 1
Would you like to use this certificate?
    [1] ov_server.crt
[y!n] (n): y
*****
* Available private key(s)
*****
* [1] ov_server.key
* [0] Exit
*****
(*) Type your option: 1
Would you like to use this private key?
    [1] ov_server.key
[y!n] (n):

```

Enable/Disable AP SSL Authentication

Enables/Disables AP SSL Authentication. By default, AP SSL Authentication is disabled. However, if you enable AP SSL Authentication and there is a problem with the SSL Certificate, you may want to disable it. Enter **12** and press **Enter**. The status will be displayed (Enabled/Disabled). Follow the prompts to enable or disable AP SSL Authentication. Once services have started/stopped, press **Enter** to return to the Configure the Virtual Appliance Menu.

Enable/Disable Admin SSH

Enter **13** and press **Enter** to enable/disable OmniVista Admin SSH. If enabled, you can log into the OmniVista VM via SSH. If disabled, you can only log in using the Hypervisor Console. Admin SSH is enabled by default.

Configure NTP Client

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

```

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

```

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

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

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

Configure Proxy

OmniVista makes an HTTPS connection to the OmniVista External Repository for upgrade software, Application Visibility Signature Files, and Fleet Supervision). If the OmniVista Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OmniVista to connect to these external sites (Port 443):

- **ALE Central Repository** – ovrepo.fluentnetworking.com
- **AV Repository** – ep1.fluentnetworking.com
- **Fleet Supervision FQDN** – myfleet.ovcirrus.com
- **Call Home Backend** – us.fluentnetworking.com
- **Device Fingerprinting Service** – api.fingerbank.org
- **Web Content Filtering** – api.bcti.brightcloud.com.

1. Enter **154** and press **Enter** to specify whether the VM will use a Proxy Server. Enter **2** and press **Enter** to configure a Proxy Server.

```
*****
* 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
* [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

This command is used to configure an additional network card in OmniVista to discover devices in subnets where the main OmniVista IP address is unreachable. Please note the following scenarios and limitations when configuring and discovering devices via this network card:

- The card must exist in the Hypervisor. If necessary, add a new Network Adapter in the VM Settings in the Hypervisor.
- The new adapter must be the same Adapter Type as first NIC. In other words, eth1, eth0 should be same type.
- Avoid configuring this network card on the same subnet as any existing devices that are already managed by the main OmniVista IP address. Doing so may cause your existing devices to fail to send traps/packets to OmniVista.
- If trap configuration was performed from OmniVista after adding/discovering new devices on a different subnet via this network card, make sure to manually change the trap station on these devices to the new IP address of this network card. This is because OV uses the main OmniVista IP address for the trap station when configuring traps via Notifications - Trap Configuration in OmniVista.

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
[yin] (y): y
The configuration has been set
Press [Enter] to continue
    
```

2. Enter the number of the network card you want to configure (e.g., **1** eth1) and press **Enter**.
3. Enter an IPv4 IP address and mask.
4. Enter **y** and press **Enter** at the confirmation prompt.

To add another network card using the VA Menu, the card must exist in the Hypervisor. If necessary, add a new Network Adapter in the VM Settings in the Hypervisor.

Important Note: The new adapter **must** be the same Adapter Type as first NIC. In other words, eth1, eth0 should be same type.

Exit

Enter **0** and press **Enter** to return to the Virtual Appliance Menu.

Run Watchdog Command

The Watchdog command set is used to start and stop managed services used by OmniVista. If you stop certain framework services (e.g., ActiveMQ, Apache Tomcat) or a service that these services depend on, the web server will shut down, and you will have to restart the service manually. You will receive a warning prompt whenever you try to shut down one of these services. To access the Watchdog Command Menu, enter **3** at the command prompt.

```

*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option:
    
```

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.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- **Choose Service Profile** - Used to save memory if certain services are not required for your network (e.g., you are not using Stellar APs in your network or you are not using the Application Visibility application). Note that when you change a service profile, all Watchdog Services will be restarted.
 - **1 - All Features (Default)** - All services are started.
 - **2 - No Stellar, No UPAM** - Services required for Stellar APs and UPAM will not be started.
 - **3 - No Application Visibility** - Services required for the Application Visibility application will not be started.
 - **4 - No IoT** - Services required for the IoT application will not be started.
 - **5 - No SFLOW** - Services required for the Analytics application (Top N Applications and Top N Clients) will not be started.

Note: You can select multiple options at the prompt for options 2 through 5 by entering the number of each option with a space between each number (e.g., 2 4 5)

Upgrade/Backup/Restore VA

The Upgrade VA command set is used to display information about the currently installed OmniVista 2500 NMS software, upgrade OmniVista software, configure the OV Build Repository, and backup/restore OV software. OV software and updates are stored on an external repository (ALE Central Repository). By default, the OV Virtual Appliance points to the ALE Central Repository, which contains the latest builds and software updates. If a proxy has been configured, make sure to configure the proxy to connect to the external repository.

Note: If you have configured and enabled a Custom Repository, you must select option **4 – Enable Repository**, and enable the **ALE Custom Repository** to access the latest software.

```
*****
* Upgrade VA
*****
* [1] Help
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any)
* [3] To New Release
* [4] Enable Repository (Selected - SQARepo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option: _
```

To access the Upgrade VA Menu, enter **4** at the command prompt. The following options are available:

- **To 4.5R3 (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 to upgrade to the latest OV software. Select an option and press **Enter** to display information about the currently installed OmniVista NMS software and download/upgrade an available update.
- **Download and Upgrade** - OV displays information about the currently installed OmniVista NMS software, checks for available updates and downloads and installs the update, if available. (If you are using an Offline Repo, this is the only upgrade

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

option supported. “Download Only” and “Upgrade from a Download Package” are not supported.)

- **Download Only** - OV displays information about the currently installed OmniVista NMS software, checks for available updates and downloads the update, if available.
- **Upgrade from a Download Package** - If you have previously downloaded an update but have not yet installed it, OV will install the downloaded update.

Note: You can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available.

- **To New Release** - Upgrade to a new release. The options and processes are the same as above (“To 4.5R3 Upgrade to Latest Patch of Current Release, if any”). Note that if a new version of the current release is available, you will be prompted to install the latest version of the current release before upgrading to the new release.
- **Enable Repository** - Enable an OV Build Repository. This is the repository that OmniVista 2500 NMS will use to retrieve OV upgrade software. Select a repository from the list, enter **y** and press **Enter** at the confirmation prompt to enable the repository. Only one (1) repository can be enabled at a time.
- **Configure Custom Repositories** - Configure a custom repository. By default, the OV Virtual Appliance points to the external ALE Central Repository, which contains the latest OV software. However, you can configure up to three (3) custom repositories. Select a repository (e.g., [1] "Custom Repo 1" Repository) and press **Enter**. Complete the fields as described below, then enter **y** and press **Enter** at the confirmation prompt:
 - **Repository Name** - User-configured repository name.
 - **Repository URL** - The URL of the custom repository (e.g., 192.168.70.10/repo/centos). Enter the URL only. There is no need to enter the “https://” prefix.

Only one (1) repository can be enabled at a time. The user is responsible for ensuring that the custom repository contains the latest OV software.

- **Configure Update Check Interval** - Configure how often the OmniVista 2500 NMS Server will check the OV Build Repository for updates. You can perform a check immediately or schedule the check to be performed at regular intervals. The results of the scheduled checks are displayed on the Welcome Screen.
 - **Check Now** - Run the Update Check Task immediately and displays the results. Enter **2** and press **Enter**. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. If an upgrade is available, enter **y** and press **Enter** to install the upgrade. Note that you can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available. Also note that if a new release is available (e.g., R01 to R02), and do not have the latest R01 software patches installed, you will first be prompted to install the latest R01 patches, and will then be prompted to install R02.
 - **Check Daily/Weekly/Monthly** - Run the Update Check Task at the configured intervals and displays the results on the Welcome Screen. Select an interval and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
 - **Disable (Default)** - Disable the Update Check Task. Enter **6** and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.

- **Backup/Restore OV2500 NMS Data** - Backup/Restore OmniVista 2500 NMS data. The following options are available:
 - **Configure Backup Retention Policy** - Configure the maximum number of days that you want to retain backups (Range = 1 – 30, Default = 7), and the maximum number of backups that you want to retain (Range = 1 – 30, Default = 5). Backup files are automatically deleted based on the Backup Retention Policy.
 - **Backup Now** - Perform an immediate backup. Enter an optional name for the backup (default = ov2500nms) and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. When the backup is complete, it will be stored in the “backups” Directory with the backup name and the date and time of the backup (<base name>_<yyyy-MM-dd--HH-mm>.bk). If you do not enter a name, the backup will be stored as ov2500nms- yyyy-MM-dd--HH-mm>.bk. (e.g., ov2500nms-2018-11-16--16-21.bk).
 - **Schedule Backup** - You can schedule an automatic backup to begin at a specific time and repeat at a specific daily interval. Enter a time for the backup to begin (HH:mm format) and press **Enter**. Enter the time between backups (Range = 1 – 30 Days, Default = 1) and press **Enter**. You can change the backup schedule at any time.
 - Note:** Scheduled backups utilize the Task Scheduler (Windows) and Cron Job (Linux) utilities. If necessary, these utilities can be used to modify a scheduled backup.
 - Note:** Backup files are automatically deleted based on the Backup Retention Policy. Monitor and maintain the Backup Directory to optimize disk space.
 - **Restore** - Select a backup and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt and press **Enter**.
 - Note:** You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.5R3 configuration using a 4.5R3 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 4.5R3 Backup File residing on a different system, you must change the OV IP address/ports and UPAM IP address/ports of the system on which you are performing the restore to match the OV IP address/ports and UPAM IP address/ports of the system from which the backup file was taken before performing the restore. After the restore is complete, you can use the Configure The Virtual Appliance Menu ([Option 4 - Configure OV IP & OV Ports](#)) to return the restored system to its original OV IP address/ports and UPAM IP address/ports.

For example, if you want to use a backup file on System A to perform a restore on the System B, you must change the OV IP address/ports and UPAM IP address/ports of System B to the OV IP address/ports and UPAM IP address/ports of System A before performing the restore. After the restore is complete, you can use the Configure The Virtual Appliance Menu ([Option 4 - Configure OV IP & OV Ports](#)) to change the OV IP address/ports and UPAM IP address/ports on System B back to their original configuration.
 - **View Backup Configurations** - View the backup retention policies. The policies are configured using Option 2 – **Configure Backup Retention Policy**. Note that if you

have not configured a Backup Retention Policy, the “Maximum Backup Retention Days” and Maximum Backup Retention Files” fields will show “-1”.

Change Password

You can change the Virtual Appliance cliadmin password and/or mongo database password. Enter **5** and press **Enter** to bring up the Change Password Menu.

```
*****
* Change Password
*****
* [1] Help
* [2] Change "cliadmin" Password
* [3] Change Mongo Database Password
* [4] Change Technical Support Code
* [5] Change FTP server Password
* [6] Change "admin" Password for UI
* [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 Technical Support Code (used by Support to access the VM) enter **4**, then press **Enter**. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

To change the password of the “ftp” user of the VA, enter **5**, then press **Enter**. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

To change the “admin” user password for the OmniVista UI login, enter **6**, then press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

Logging

You can view OmniVista 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
* [5] Collect Files in Advanced Mode
* [0] Exit
*****
(*) Type your option: 0
```

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., 10-15-2019) 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-15-10-2019_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-02019-10-15-12-08-43.jar). SFTP to the VA using the "cliadmin" username and password to view the log file (Port 22).
- **Collect Files in Advanced Mode** - Collects and archives tcpdump information to a Zip file in the "chrootadmin" directory with date and time the file was created appended to the file name (e.g., chrootadmin_10-03-2020-11-02-43.zip). 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 OmniVista Login Authentication Server. Enter **7** and press **Enter** to bring up the Login Authentication Server Menu.

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

Note: OmniVista functions stop running following power off. The VM must be powered back on via the VMware client software and you must log back into the VM via the console.

Reboot

Before rebooting the VM, you must stop all OmniVista services using the **Stop All Services** option in the **Run Watchdog Command**. After all services are stopped, enter **9** at the command line to reboot the VM. Confirm reboot by entering **y**. The reboot may take several minutes to complete. When rebooted, you will be prompted to log in through the cliadmin user and password prompts. Note that OmniVista functions continue following reboot.

Advanced Mode

Advanced Mode enables you to use read-only UNIX commands for troubleshooting. Enter **9**, then press **Enter** to bring up the CLI prompt. Enter **exit** and press **Enter** to return to the Virtual Appliance Menu. The following commands are supported:

- /usr/bin/touch
- /usr/bin/mktemp
- /usr/bin/dig
- /usr/bin/cat
- /usr/bin/nslookup
- /usr/bin/which
- /usr/bin/less
- /usr/bin/tail
- /usr/bin/vi
- /usr/bin/tracepath
- /usr/bin/tty
- /usr/bin/systemctl
- /usr/bin/grep
- /usr/bin/egrep
- /usr/bin/fgrep
- /usr/bin/dirname
- /usr/bin/readlink
- /usr/bin/locale
- /usr/bin/ping
- /usr/bin/traceroute
- /usr/bin/netstat
- /usr/bin/id
- /usr/bin/ls

- /usr/bin/mkdir
- /usr/sbin/ifconfig
- /usr/sbin/route
- /usr/sbin/blkid
- /usr/sbin/sshd-keygen
- /usr/sbin/consoletype
- /usr/sbin/ntpdate
- /usr/sbin/ntpq
- /usr/bin/ntpstat
- /usr/bin/abrt-cli
- /usr/sbin/init
- /usr/sbin/tcpdump
- /bin/mountpoint

Set Up Optional Tools

The Setup Optional Tools command set is used to install/upgrade Hypervisor Optional Tools Packages. Enter **11** and Press **Enter** to bring up the Optional Tool Menu.

```
*****
* Optional Tool Of Supervisors Menu
*****
* [1] Help
* [2] VMware Tools
* [3] VirtualBox Guest Additions
* [0] Exit
*****
(*) Type your option: s_
```

Enter the number corresponding to the Hypervisor you are using (**2 – VMWare Tools, 3 - Virtual Box Guest Additions**) and press **Enter**. Information about available packages is displayed. If a new package is available, enter **y** and press **Enter** at the "Would you like to install the package" prompt. The package will automatically be downloaded from the OV Repository and installed (this may take several minutes). When the "Installation Complete" message is displayed, press **Enter** to continue. Press **Enter** again to restart the Virtual Appliance.

Note: The option for Virtual Box Guest tools is for test/experimental purposes only and is not officially supported.

Convert to Cluster

Enter **12** and press **Enter** to convert the Node to a Cluster (High-Availability) Installation. This command prepares the VM to be configured in a Cluster configuration. After selecting this option and confirming the operation, the VM will reboot. When the reboot is complete, log into the VM to complete the conversion.

```
(*) Type your option: 12
OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed converting to cluster?[y|n] (n):
```

See [Converting to a High-Availability Installation](#) for detailed instructions on configuring a High-Availability installation.

Join Cluster

Enter **13** and press **Enter** to have this VM join in a Cluster (High-Availability) Installation. After selecting this option and confirming the operation, the VM will reboot. When the reboot is complete, log into the VM to complete the conversion.

```
All data on this node will be lost and OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed joining cluster?[y;n] (n):
```

See [Converting to a High-Availability Installation](#) for detailed instructions on configuring a High-Availability installation.

Troubleshoot

The Troubleshoot command can be used to address an “LDAP Index Generation” Error. The message indicates that the LDAP Database has been corrupted. Enter **14** and press **Enter** to bring up the Troubleshoot Menu. Enter **1 – Fix LDAP: error code 80 – index generation failed**, and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt to repair and recover the LDAP Database. Once the “Success” message is displayed, press **Enter** to return to the Virtual Appliance Menu.

```
*****
* Troubleshoot
*****
* [1] Fix LDAP: error code 80 - index generation failed
* [0] Exit
*****
(*) Type your option: 1
Please note that LDAP will be restarted.
Do you want to continue [y;n] (n): y
Fixed LDAP successfully.
Press [Enter] to continue
```

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 OmniVista functions continue following logout.

Appendix B – Using the HA Virtual Appliance Menu

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

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

The menus are the same for both Nodes in the Cluster. With the exception of the specific Cluster Menus (Show OV Cluster Status, Configure Cluster and Configure Current Node), any configurations you perform (e.g., Watchdog commands, Upgrade/Backup/Restore commands) are executed on the Node you are logged into.

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

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

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

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

The HA Virtual Appliance Menu provides the following options:

- [1 – Help](#)
- [2 – Show OV Cluster Status](#)
- [3 – Configure Cluster](#)
- [4 – Configure Current Node](#)
- [5 – Run Watchdog Command](#)
- [6 – Upgrade/Backup/Restore VA](#)
- [7 – Logging](#)
- [8 – Setup Optional Tools](#)
- [9 – Advanced Mode](#)

- [10 – Power Off](#)
- [11 – Reboot](#)
- [0 – Log Out](#)

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

Help

Enter **1** and press **Enter** to bring up help for the HA Virtual Appliance Menu.

Show OV Cluster Status

The Cluster Status Screen displays information about the High-Availability Cluster, including Node IP address, Role, and Status. The status will display and the HA Virtual Appliance Menu will return.

```
Cluster Status:
Node      Hostname  Ip Address   Role    Status
Current  ov1      10.255.221.27 Active
Peer     ov2      10.255.221.28 Online
Data sync: Up to Date
```

The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a progress will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes.

Important Note: If a data sync is in progress, it is highly recommended to wait for a data sync to complete before doing performing any configuration on a Node.

Configure Cluster

Enter **3** and press **Enter** to configure the Cluster. The settings you configure in this menu are applied to both Nodes in the Cluster. Note that Cluster settings (Menu Items 3 – 8) can only be configured on the Active Node.

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

The following options are available:

- [1 – Help](#)
- [2 – Display Cluster Configuration](#)
- [3 – Configure Cluster IP](#)
- [4 – Configure Captive Portal Virtual IP](#)
- [5 – Configure Captive Portal Virtual IPv6](#)
- [6 – Configure Additional OV Web Virtual IP](#)
- [7 – Remove Peer Node From Cluster](#)
- [8 – Configure OV Web Ports](#)
- [9 – Configure Portal Web Ports](#)
- [10 – Configure OV SSL Certificate](#)
- [11 – Enable/Disable AP SSL Authentication](#)
- [12 - Configure FTP Password](#)
- [13 – Configure Login Authentication Server](#)
- [14 – Preferred Active Node](#)
- [15 – Manual Failover](#)
- [16 – Cluster Error Check](#)
- [17 - Configure Peer Node's Information](#)
- [18 – Enable Maintenance Mode](#)
- [0 – Exit](#)

Help

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

Display Cluster Configuration

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

```
*****
* Cluster Configuration
*****
Cluster name: ovcluster
OV Virtual IP: 10.255.222.97
Captive Portal Virtual IP: 198.168.0.3
Captive Portal Virtual IPv6: (disabled)
Additional OV Web Virtual IP: (disabled)

Current node IP: 10.255.222.203
Current node hostname: ov1
Peer node IP: 10.255.222.98
Peer node hostname: ov2
Current Preferred Node:

OV Web HTTP Port: 80
OV Web HTTPS Port: 443

Captive Portal Web HTTP Port: 80
Captive Portal Web HTTPS Port: 443
```

Configure Cluster IP

Enter **3** and press **Enter** to configure the Cluster IP address and subnet. You will be prompted to restart services for the change to take effect. Note that if you reconfigure the Cluster IP address you will have to make the applicable network updates. The Cluster IP is only applicable for a Layer 2 HA Configuration.

```
*****
* Configure Cluster IP
*****
* [1] Disable Cluster IP Address
* [2] Re-configure Cluster IP
* [0] Exit
*****
```

To change an existing Cluster IP address, enter **2** and press **Enter** to re-configure the new address. The new IP address **must** be on the same subnet as the Nodes.

It is not recommended to disable the Cluster IP address. However, you can disable the Cluster IP address if you do not want to access the Cluster using this IP address. Enter **1 – Disable Cluster IP Address** and press **Enter** to disable the Cluster IP address. When you disable the Cluster IP address, the Virtual Captive Portal IP and Virtual Additional Web OV IP (if configured) are also disabled.

After disabling the Cluster IP address, you must access OmniVista using the physical IP address of the Active Node. After disabling the Cluster IP address, you can re-enable it and re-configure the Cluster IP address. The new IP address **must** be on the same subnet as the Nodes.

Configure Captive Portal Virtual IP

Enter **4** and press **Enter** to configure the Captive Portal Virtual IP address. Note that if you reconfigure the Captive Portal Virtual IP address you will have to make the applicable network updates. Captive Portal Virtual IP is only applicable for a Layer 2 HA Configuration.

```
*****
* Configure Captive Portal Virtual IP
*****
* [1] Disable Captive Portal Virtual IP
* [2] Re-configure Captive Portal Virtual IP
* [0] Exit
*****
```

If you are not using Captive Portal in your Cluster, you can enable and configure it. To create a new Captive Portal Virtual IP address, enter **1 – Enable Captive Portal Virtual IP** and press **Enter**. Enter the Virtual Captive Portal IP address. Note that the Captive Portal Virtual IP address must be on the same subnet as the current Cluster IP address.

If you are using Captive Portal in your Cluster, you can change the existing Captive Portal Virtual IP address, by entering **2 – Re-configure Captive Portal Virtual IP** and press **Enter** to configure the new address. You will be prompted to restart services for the change to take effect. The new Captive Portal Virtual IP address **must** be on the same subnet as the previous address.

To disable an existing Captive Portal IP address in a Cluster, enter **1 - Disable Captive Portal Virtual IP** and press **Enter**. You will be prompted to restart services for the change to take effect. You can also re-enable and re-configure the Captive Portal Virtual IP address after disabling it.

Configure Captive Portal Virtual IPv6

Enter **5** and press **Enter** to configure the Captive Portal Virtual IPv6 address. You will be prompted to restart services for the change to take effect. Note that if you reconfigure the Captive Portal Virtual IPv6 address you will have to make the applicable network updates. Captive Portal Virtual IPv6 is only applicable for a Layer 2 HA Configuration.

```

*****
* Configure Captive Portal Virtual IPv6 *
*****
* [1] Enable Captive Portal Virtual IPv6 *
* [0] Exit *
*****
    
```

To create a new Captive Portal Virtual IPv6 address, enter **1 – Enable Captive Portal Virtual IPv6** and press **Enter**. To change an existing Captive Portal Virtual IPv6 address, enter **2 – Re-configure Captive Portal Virtual IPv6** and press **Enter** to configure the new address. The new Captive Portal Virtual IPv6 address **must** be on the same subnet as the previous address.

To disable an existing Captive Portal IPv6 address, enter **1 - Disable Captive Portal Virtual IP** and press **Enter**. You will be prompted to restart services for the change to take effect. You can also re-enable and re-configure the Captive Portal Virtual IPv6 address after disabling it.

Configure Additional OV Web Virtual IP

Enter **6** and press **Enter** to configure an Additional OV Web Virtual IP to access the OmniVista UI. You will be prompted to restart services for the change to take effect. The Additional OV Web Virtual IP is only applicable for a Layer 2 HA Configuration.

```

*****
* Configure Additional OV Web Virtual IP *
*****
* [1] Enable Additional OV Web Virtual IP *
* [0] Exit *
*****
    
```

To create a new Additional OV Web Virtual IP, enter **1 – Enable Additional OV Web Virtual IP** and press **Enter**. The Additional OV Web Virtual IP must be on the same subnet as the current static Additional OV Web Virtual IP. If no static Additional OV Web Virtual IP is configured, you will not be able to configure an Additional OV Web Virtual IP.

To change an existing Additional OV Web Virtual IP, enter **2 – Re-configure Additional OV Web Virtual IP** and press **Enter** to configure the new address. The new Additional OV Web Virtual IP address **must** be on the same subnet as the previous address.

To disable an Additional OV Web Virtual IP, enter **1 - Disable Additional OV Web Virtual IP**.

Remove Peer Node From Cluster

Enter **7**, press **Enter**, then enter **y** and press **Enter** at the Confirmation Prompt to remove the Peer Node from the Cluster. The process can take several minutes. When it is complete, a Confirmation Message will appear. Press **Enter** to return to the Configure Cluster Menu.

Note that this command can only be issued on the Active Node. This command is generally used if there is a problem with the Standby Node and you wish to permanently remove it. Once the Node is removed from the Cluster, it is essentially unusable. You cannot connect to it via a browser and it retains the HA Menu, so you cannot have it join another Cluster. However, you can have another Node join the Active Node in a new Cluster Configuration.

Configure OV Web Ports

Enter **8** and press **Enter** to configure the OmniVista Web HTTP/HTTPS ports. At the prompts, enter the IPv4 IP address and subnet mask; enter **y** and press **Enter** at the confirmation prompt, then press **Enter** to continue. At the prompts, enter the HTTP Port and the HTTPS Port (Defaults = HTTP - 80, HTTPS - 443). Enter **y** and press **Enter** at the confirmation prompt.

You will be prompted to restart the Watchdog Service for the change to take effect. Note that new port values must be unique (i.e., they must differ from any previously-configured ports).

```
*****
* Configure 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
[y;n] (y):
The configuration has been set
Press [Enter] to continue
```

Configure Portal Web Ports

Enter **9** and press **Enter** to configure the Portal Web Ports. Enter the Captive Portal HTTP and HTTPS port numbers. Press **Enter** to continue. You will be prompted to restart services for the change to take effect.

Note: The default Captive Portal FQDN is "ov2500-upam-cportal.al-enterprise.com". If you want to replace it with your own FQDN you must:

1. Log into the OmniVista UI.
2. Go to the UPAM – Captive Portal Certificates page (U PAM – Settings – Captive Portal Certificates).
 - Create a Custom Certificate.
 - Activate the Certificate.

```
*****
* Configure Captive Portal Web Ports
*****
Please input Captive Portal Web HTTP port [80]:
Please input Captive Portal Web HTTPS port [443]:
Would you like to configure:
    Captive Portal Web HTTP port: 80
    Captive Portal Web HTTPS port: 443
[y;n] (y):
The configuration has been set
Press [Enter] to continue
```

Configure OV SSL Certificate

To update the OmniVista Web Server SSL Certificate, you must first generate a *.crt and *.key file and use an SFTP Client to upload the files to the VA. Make sure the destination directory is "keys".

- **SFTP User:** cliadmin
- **SFTP Password:** <password when deploying VA>

- **SFTP Port: 22**

1. Enter **10** and press **Enter**.
2. Choose a certificate file (.crt) and enter **y** and press **Enter**. Choose a private key file (.key) and enter **y** and press **Enter**.

```
*****
* Update OmniVista Web Server SSL certificate
*****
* Available certificate(s)
*****
* [1] ov_server.crt
* [0] Exit
*****
(*) Type your option: 1
Would you like to use this certificate?
    [1] ov_server.crt
[y!n] (n): y
*****
* Available private key(s)
*****
* [1] ov_server.key
* [0] Exit
*****
(*) Type your option: 1
Would you like to use this private key?
    [1] ov_server.key
[y!n] (n):
```

Enable/Disable AP SSL Authentication

Enables/Disables AP SSL Authentication. By default, AP SSL Authentication is disabled. However, if you enable AP SSL Authentication and there is a problem with the SSL Certificate, you may want to disable it. Enter **11** and press **Enter**. The current status will be displayed (Enabled/Disabled). Follow the prompts to enable or disable AP SSL Authentication. Once services have started/stopped, press **Enter** to return to the Configure the Virtual Appliance Menu.

Configure FTP Password

Enter **10** and press **Enter** to configure an FTP password for the Node. At the prompt, enter the old password, then enter and confirm the new password. You will be prompted to restart services for the change to take effect.

Configure Login Authentication Server

Enter **13** and press **Enter** to view/change the OmniVista Login Authentication Server.

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

Preferred Active Node

Enter **14** and press **Enter** to change the preferred Active Node. The Preferred Active Node is the Node that will be set following a system failure. When the system returns, the Preferred Active Node will be the Active Node when the system returns.

Select **1** to clear the current Active Node. This will remove the current Preferred Active Node setting, meaning there will be no Preferred Active Node in the case of a system failure. If no Preferred Active Node is set, the system will decide on the Active Node following a system failure. By default, no Preferred Active Node is set.

Select **2** or **3** to change the current Active Node. Enter **y** and press **Enter** at the Confirmation Prompt to clear the current Preferred Active Node and set the new one.

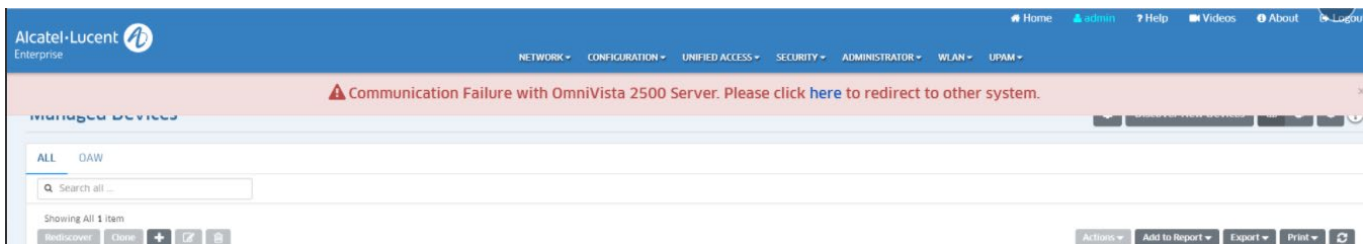
```
*****
* Preferred Active Node
*****
Current Preferred Node:

Choose Your Option
[1] Clear Preferred Active Node
[2] Set Preferred Active Node: ov1
[3] Set Preferred Active Node: ov2
[0] Exit
(*) Type your option:
```

Manual Failover

Enter **15** and press **Enter** to manually initiate a failover to the Inactive Node. The current Inactive Node will become the Active Node. The process can take several minutes. After the failover is complete, the services on the Standby Node will be running. The previously Active Node will now be the Standby Node (with the upam, radius, and nginx services “Stopped”). A Banner will appear at the top of the UI warning that a “Communication Failure” has occurred.

- If you are using a Layer 2 Configuration, you can access OmniVista using the same Cluster IP address.
- If you are using a Layer 3 Configuration, the banner will contain a link to connect to the new Active Node, as shown below.



Cluster Error Check

Enter **16** and press **Enter** to bring up the Check Cluster Error Menu.

```
*****
* Check Cluster Error
*****
* [1] Check multi Active nodes error - Force this node to be Active node
* [2] Check sync percentage suspended, inconsistent between nodes and services' status issue
* [3] Fix status: Syncing (as replication:PausedSyncT..
* [0] Exit
*****
(*) Type your option: █
```

Configure Peer Node's Information

Enter **17** and press **Enter** to change the IP address and Hostname (maximum of 15 characters) of the Peer Node. It is **not** recommended to re-configure the Peer Node once a cluster is initialized. If you change the configuration, you must take a backup of OmniVista and contact Customer Support to re-configure the Cluster.

Enable Maintenance Mode

Enter **18** and press **Enter** to enable Maintenance Mode to perform an upgrade/disk extension on the VMs (Node 1 and Node 2). You only have to execute the command on one of the nodes. It will then be enabled on both Nodes.

Exit

Enter **0** and press **Enter** to exit to the Configure Cluster Menu and return to the HA Virtual Appliance Menu.

Configure Current Node

Enter **4** and press **Enter** to configure the Current Node (the Node that you are logged into).

```
*****
* Configure Current Node
*****
* [1] Help
* [2] Display Current Node Configuration
* [3] Configure Default Gateway
* [4] Configure DNS Server
* [5] Configure Timezone
* [6] Configure Route
* [7] Configure Keyboard Layout
* [8] Configure NTP Client
* [9] Configure Proxy
* [10] Configure Screen Resolution
* [11] Configure "cliadmin" Password
* [12] Configure "root" Secret Text
* [13] Enable/Disable Admin SSH
* [14] Configure MongoDB Password
* [15] Configure IPs & Ports
* [16] Configure Hostname
* [17] Extend Partitions
* [18] Configure Network Size
* [19] Troubleshoot
* [20] Configure Another NIC(s)
* [21] Configure "admin" Password for UI
* [0] Exit
*****
(*) Type your option: _
```

The following options are available:

[1 – Help](#)

[2 – Display Current Node Configuration](#)

[3 – Configure Default Gateway](#)

- [4 – Configure DNS Server](#)
- [5 – Configure Timezone](#)
- [6 – Configure Route](#)
- [7 – Configure Keyboard Layout](#)
- [8 – Configure NTP Client](#)
- [9 – Configure Proxy](#)
- [10 – Configure Screen Resolution](#)
- [11 – Configure “cliadmin” Password](#)
- [12 – Configure “root” Secret Text](#)
- [13 – Enable/Disable Admin SSH](#)
- [14 – Configure MongoDB Password](#)
- [15 – Configure IPs and Ports](#)
- [16 – Configure Host Name](#)
- [17 – Extend Data Partitions](#)
- [18 – Configure Network Size](#)
- [19 – Troubleshoot](#)
- [20 – Configure Another NIC\(s\)](#)
- [21 – Configure “admin” Password for UI](#)
- [0 – Exit](#)

Help

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

Display Current Node Configuration

Enter **2** and press **Enter** to display the configuration for the Node.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

```
*****
* Current Node Configuration
*****
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R1 GA
Build Number: 55
Patch Number: 0
Build Date: 06/20/2019
WMA Version: 3.1.15.15
UPAM Version: 3.1.33.17

OU IPv4 Address: 10.255.222.203
NetMask: 255.255.255.0
Hostname: ovl

Default gateway: 10.255.222.62

Timezone: America/Los_Angeles

lvdata LUM Size: 50G
lvdata LUM Available (Free) Space: 41G
lvdatasync LUM Size: 206G
lvdatasync LUM Available (Free) Space: 188G

Network Size: Low (lower than 500) devices

DNS Server: DNS is not set!

Keyboard Layout: us

Proxy Status: Enabled
```

Configure Default Gateway

1. Enter **3** and press **Enter** to configure default gateway settings.

```
*****
* Configure Default Gateway
*****
Please input default gateway v4 [10.255.222.62]:
Would you like to configure:
    default gateway: 10.255.222.62
[yin] (y):
The configuration has been set
Press [Enter] to continue
```

2. Enter an IPv4 default gateway.
3. Press **Enter** to confirm the settings. You will be prompted to restart services. Press **Enter**.

Configure DNS Server

1. Enter **4** to specify whether the VM will use a DNS Server.
2. If the VM will use a DNS server, enter **y**, then press **Enter**. Enter the IPv4 address for Server 1 and Server 2, if applicable.

```
*****
* Configure DNS Server
*****
Would you like to use dns servers [y/n] (n): y
(*) Please input dns server 1: 192.168.70.226
Would you like to use dns server 2 [y/n] (n): y
(*) Please input dns server 2: 192.168.1.3
Would you like to configure:
    dns server 1: 192.168.70.226
    dns server 2: 192.168.1.3
[y/n] (y): _
```

Note: If **n** (No) is selected, all DNS Servers will be disabled. If **y** is selected, after DNS servers are set, you may be prompted to restart ovclient service if it was already running.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu. You will be prompted to restart the OV Client Service for the change to take effect.

Configure Timezone

1. Enter **5** and press **Enter** to begin setting up the timezone.

```
*****
* Configure Timezones
*****
The available timezones list will be shown (press [q] to exit view mode)
Press [Enter] to continue
_
```

2. Press **Enter** to display timezones.

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
Africa/Douala
Africa/El_Aaiun
Africa/Freetown
Africa/Gaborone
Africa/Harare
Africa/Johannesburg
Africa/Juba
Africa/Kampala
Africa/Khartoum
Africa/Kigali
Africa/Kinshasa
Africa/Lagos
Africa/Libreville
Africa/Lome
Africa/Luanda
Africa/Lubumbashi
Africa/Lusaka
lines 1-36
```

3. Press **Enter** to scroll through the list. After locating your timezone, press **q** and enter your timezone at the prompt (e.g., America/Los_Angeles). Then press **Enter** to set the timezone and return to the Configure Current Node Menu.

```
America/La_Paz
America/Lima
America/Los_Angeles
Please input timezones [America/Los_Angeles]: America/Los_Angeles
Would you like to set:
    timezones: America/Los_Angeles
[yin] (y):
The configuration has been set
Press [Enter] to continue
```

You can verify the change using the **(2) Display Current Node Configuration** command.

Configure Route

1. If you want to add a static route from the VM to another network enter **6** and press **Enter**.
2. Add an IPv4 route by entering **3** at the command prompt.

```

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

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

Configure Keyboard Layout

1. Enter **7** and press **Enter** to specify a keyboard layout.

```

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

2. Press **Enter** to see the list of keyboard layouts.
3. Enter **q** and press **Enter** to quit the view mode. At the prompt, enter a keyboard layout then press **Enter**. Enter **y** at the confirmation prompt and press **Enter**.

```

Please input keyboard layout [us]:
Would you like to set:
    keyboard layout: us
[yin] (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-latin1-1k450	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

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

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_cp1k-CP1251	ttwin_ct_sh-UTF-8	ru1
ruwin_ctrl-KOI8-R	ru-ms	no	us-acentos
pl2	sv-latin1	br-latin1-abnt2	et
ru-cp1251	ruwin_alt-CP1251	ru	it2
lt.l4	ua-utf	bywin-cp1251	bg-cp1251
ru_win	emacs2	dk-latin1	kazakh
br-abnt2	es	pl4	mk0
is-latin1	is-latin1-us	il-phonetic	fi-old
et-nodeadkeys	jp106	lt	ru2
ruwin_ct_sh-UTF-8	pt	se-fi-ir209	gr-pc
lt.baltic	tr_q-latin5	pl3	ua-utf-ws
bashkir	no-dvorak	dvorak-r	dvorak
ANSI-dvorak	dvorak-l	mac-euro	mac-euro2
mac-fr_CH-latin1	mac-us	mac-de-latin1	mac-be
mac-es	mac-pl	mac-se	mac-dvorak
mac-fi-latin1	mac-template	mac-dk-latin1	mac-de-latin1-nodeadkeys
mac-fr	mac-pt-latin1	mac-uk	mac-it
mac-de_CH	sunt4-no-latin1	sunt5-cz-us	sundvorak
sunt5-de-latin1	sunt5-us-cz	sunt5-es	sunt4-fi-latin1
sunkeymap	sunt4-es	sunt5-ru	sunt5-uk
sun-pl	sunt5-fr-latin1	sunt5-fi-latin1	sun-pl-altgraph

4. Press **Enter** to return to the Configure The Configure Current Node Menu.

Configure NTP Client

1. Enter **8** and press **Enter** to configure an NTP Server.

```

*****
* Configure NTP Client *
*****
* [1] Help *
* [2] Configure NTP Server IP *
* [3] Status NTP Client *
* [4] Disable NTP Client *
* [5] Enable NTP Client *
* [0] Exit *
*****
(*) Type your option:

```

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

3. Enter the IP address of the NTP Server and press **Enter**.
4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure Current Node Menu. You can enable the server when you create it, or enable it at a later time using option **5**.

Configure Proxy

OmniVista makes an HTTPS connection to the OmniVista External Repository for upgrade software, Application Visibility Signature Files, and Fleet Supervision. If the OmniVista Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OmniVista to connect to these external sites (Port 443):

- **ALE Central Repository** – ovrepo.fluentnetworking.com
- **AV Repository** – ep1.fluentnetworking.com
- **Call Home Backend** – us.fluentnetworking.com
- **Device Fingerprinting Service** – api.fingerbank.org
- **Web Content Filtering** – api.bcti.brightcloud.com.

1. Enter **9** and press **Enter** to specify whether the VM will use a Proxy Server. Enter **2** and press **Enter** to configure a Proxy Server.

```
*****
* Configure Proxy
*****
* [1] Help
* [2] Setup Proxy
* [3] Enable/Disable Proxy
* [0] Exit
*****
(*) Type your option: _
```

2. If a proxy has already been configured, the current configuration is displayed. Enter the Proxy Server IP address, along with the port (e.g., 8080).

```
Current proxy configuration:
  IP: 10.255.10.80
  Port: 8080
  Username:
  Password:
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:
[yin] (y): _
```

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

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

Change Screen Resolution

1. Enter **10** and press **Enter** to configure the VA screen resolution.

```
*****
* Change screen resolution
*****
* [1] 800x600
* [2] 1024x768
* [0] Exit
*****
(*) Type your option:
```

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

Configure “cliadmin” Password

Enter **11** and press **Enter** to change the “cliadmin” password for the Node VM. At the prompt, enter the new password and press **Enter**. Re-enter the password and press **Enter**.

```
You must remember the new passwords in order to manage the Virtual Appliance and OmniVista.
Length of new password must be >= 8 and <= 30 characters
Enter new password:
Retype password:
Changing password for user cliadmin.
passwd: all authentication tokens updated successfully.
```

Configure “root” Secret Text

Enter **12** and press **Enter** to change the password of the “root” user of the VA. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

Enable/Disable Admin SSH

Enter **13** and press **Enter** to enable/disable OmniVista Admin SSH. If enabled, you can log into the OmniVista VM via SSH. If disabled, you can only log in using the Hypervisor Console. Admin SSH is enabled by default.

Configure MongoDB Password

Enter **14** and press **Enter** to change the MongoDB password. You have two options when changing the mongo database password.

```
You must remember the new passwords in order to manage the MongoDB.
Press [Enter] to continue
Would you like to change password for
    [1] Mongo administrator
    [2] Ngnms application user
Provide your option [1 OR 2]: _
```

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

Configure IPs and Ports

Enter **15** and press **Enter** to change the IP address and ports of the current Node. It is not recommended that you change the configuration of the Cluster once it has been initialized. If a

Cluster has already been initialized, you must take a backup of OmniVista and contact Customer Support to re-configure the Cluster.

Configure Hostname

Enter **16** and press **Enter** to change the Hostname of the current Node (maximum of 15 characters).

Extend Data Partitions

Enter **17** and press **Enter** to add an additional hard disk and extend the current data partitions. By default, OmniVista is partitioned as follows: HDD1:50GB and HDD2:512GB. If you are managing more than 500 devices, it is recommended that you increase the provisioned hard disk.

Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. **Insufficient memory or disk space for the chosen network size may cause OV instability.** OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 20GB of memory for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to [Recommended System Configurations](#) for details. Follow the steps [below](#) to Extend the Data Partition.

Important Notes:

- If you have a KVM deployment, when adding new storage, select Bus Type = SATA for new storage in KVM Settings. OmniVista only supports new storage in the SATA format.
- OmniVista on KVM does not detect the first two disks but does detect the third disk onward. For example. If you deployed OmniVista on KVM with "VirtIO disk1" and "VirtIO disk2" and then added three more SATA disks (SATA disk1", "SATA disk2" and "SATA disk3), when you navigate the VA menu to extend the disk space, OmniVista only detects "SATA disk3".
- To extend the disk space for OmniVista on KVM:
 1. Add "SATA disk1" with 1KB capacity because OmniVista will not detect it.
 2. Add "SATA disk2" with 1KB capacity because OV will not detect it.
 3. Add "SATA disk3" with the desired capacity (20GB, 50GB...).
 4. Go to the VA menu and use the "SATA disk3" to extend the disk space.
 5. Do not remove "SATA disk1" and "SATA disk2".

Extending the Data Partition

1. Shut down OmniVista Services on the Active Node:
 - On the main HA Virtual Appliance Menu, select **5** – [Run Watchdog Command](#), then select **9**– Shutdown Watchdog. Stop All Services. Wait for all services and Watchdog to shut down.
2. Shut down OmniVista Services on the Standby Node:

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- On the main HA Virtual Appliance Menu, select **5** - Run Watchdog Command, then select **9** - Shutdown Watchdog. Wait for all services and Watchdog to shut down.
3. Take a VM Snapshot of the Active Node VM or use the OmniVista Backup Command in the Virtual Appliance Menu.
 - To perform a backup, go to the main Virtual Appliance Menu, select **6** – [Upgrade/Backup/ Restore VA](#), select **7** – Backup/Restore OmniVista 2500 NMS Data, then select **3** – Backup Now.
 4. Take a VM Snapshot of the Standby Node VM or use the OmniVista Backup Command in the Virtual Appliance Menu.
 - To perform a backup, go to the main Virtual Appliance Menu, select **6** – [Upgrade/Backup/ Restore VA](#), select **7** – Backup/Restore OmniVista 2500 NMS Data, then select **3** – Backup Now.
 5. Power off the Active Node from the HA Virtual Appliance console. Wait until the VM is completely powered off.
 - On the main HA Virtual Appliance Menu, select **10** – [Power Off](#).
 6. Power off the Standby Node from the HA Virtual Appliance console. Wait until the VM is completely powered off.
 - On the main HA Virtual Appliance Menu, select **10** – [Power Off](#).
 7. Add new virtual disks for additional disk space from the hypervisor for both the Active and Standby Nodes. Note that editing the size of existing virtual disks is not supported.
 8. Power on the Active Node using the hypervisor menu option. Wait for all services to come up.
 9. Power on the Standby Node using the hypervisor menu option. Wait for all services to come up.
 10. Enable Maintenance Mode on the Active Node. (Note that if you are already in Maintenance Mode, for example, you are in the process of upgrading, this step is not necessary.)
 - On the main HA Virtual Appliance Menu, select **3** – Configure Cluster, then select **18** – [Enable Maintenance Mode](#).
 11. Extend the disk on both the Active and Standby Nodes. Note that after extending the disk on the Active Node, you will be prompted to extend the disk on the Standby Node.
 - On the main HA Virtual Appliance Menu, select **4** - Configure Current Node, then select **17** – Extend Partitions. Select “OmniVista Data Partition” for the Logical Volume Type.
 12. Disable Maintenance Mode on the Active Node:
 - On the main HA Virtual Appliance Menu, select **3** – Configure Cluster Menu, then select **18** – [Disable Maintenance Mode](#). After you disable Maintenance Mode, the two nodes will sync. This can take 10 – 20 minutes.

Notes:

1. Do **not** power off or reset the VMs until the operation completes.
2. Always power off VM nodes using the HA Virtual Appliance Menu option.
3. The following error message appears after the node is powered off from the Virtual

Appliance Menu (after Shutdown Watchdog):

```
Error while retrieving MBean of type com.alu.ov.ngnms.nms.watchdog.jmx.WatchdogServiceMBean
```

Configure Network Size

Enter **18** and press **Enter** to configure the Node memory settings. Select an option (e.g., Low, Medium, High, Very High) based on the number of devices being managed and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. You will be prompted to restart the Watchdog Service for the change to take effect.

```
*****
* 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)
[0] Exit
(*) Type your option: _
```

Troubleshoot

The Troubleshoot command can be used to address an “LDAP Index Generation” Error. The message indicates that the LDAP Database has been corrupted. Enter **19** and press **Enter** to bring up the Troubleshoot Menu. Enter **1 – Fix LDAP: error code 80 – index generation failed**, and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt to repair and recover the LDAP Database. Once the “Success” message is displayed, press **Enter** to return to the Virtual Appliance Menu.

```
*****
* Troubleshoot
*****
* [1] Fix LDAP: error code 80 - index generation failed
* [0] Exit
*****
(*) Type your option: 1
Please note that LDAP will be restarted.
Do you want to continue [y/n] (n): y
Fixed LDAP successfully.
Press [Enter] to continue
```

Configure Another NIC(s)

1. To change the configuration of another NIC, enter **20** and press **Enter** to bring up the Configure the other Network Cards Menu.

```
*****
* Configure the other Network Cards
*****
Choose the number of network card to configure:
[1] eth1-00:0c:29:ff:9a:23
[0] Exit
(*) Type your option: █
```

2. Enter the number of the NIC you want to configure (for example, **1 – Eth1-00:0c:29:ff:9a:23**) and press **Enter**.

3. Enter an IPv4 IP address and mask.

4. Enter **y** and press **Enter** at the confirmation prompt.

Configure “admin” Password for UI

Enter **21** and press **Enter** to change the “admin” password for the OmniVista UI login. At the prompt, enter the new password and press **Enter**. Re-enter the password and press **Enter**.

```
Start changing password for admin UI
Note: Changing the 'admin' user password from this menu will not end any active sessions.
To terminate them, log in to the UI and reset the password again.
New Password for admin user:
Confirm Password for admin user:

Changing admin password for UI...
Password updated successfully.
```

Exit

Enter **0** and press **Enter** to exit to the Configure Current Node Menu and return to the HA Virtual Appliance Menu.

Run Watchdog Command

The Watchdog command set is used to start and stop managed services used by OmniVista. If you stop certain framework services (e.g., ActiveMQ, Apache Tomcat) or a service that these services depend on, the web server will shut down, and you will have to restart the service manually. You will receive a warning prompt whenever you try to shut down one of these services.

To access the Watchdog CLI Command Menu, enter **5** at the command prompt.

```
*****
* 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
* [10] Choose Service Profile
* [0] Exit
*****
(*) Type your option:
```

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.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

- **Stop All Services** - Stop all services. Enter **y** and press **Enter** at the confirmation prompt.
- **Restart All Services** - Stop and restart all services. Enter **y** and press **Enter** at the confirmation prompt.
- **Start a Service** - Starts a single service. Enter the service name at the prompt and press **Enter**. At the "Start Tree" option, enter **y** and press **Enter** to start all dependent services; enter **n** if you do not want to start dependent services. Press **Enter** at the confirmation prompt to start the service(s).
- **Stop a Service** - Stops a single service. Enter the service name at the prompt and press **Enter**. At the "Stop Tree" option, enter **y** and press **Enter** to stop all dependent services; enter **n** if you do not want to stop dependent services. Press **Enter** at the confirmation prompt to stop the service(s).
- **Start Watchdog** - Starts the Watchdog Service, which starts all services.
- **Shutdown Watchdog** - Stops the Watchdog Service, which stops all services.
- **Choose Service Profile** - Used to save memory if certain services are not required for your network (e.g., you are not using Stellar APs in your network or you are not using the Application Visibility application). Note that when you change a service profile, all Watchdog Services will be restarted.
 - **1 - All Features (Default)** - All services are started.
 - **2 - No Stellar, No UPAM** - Services required for Stellar APs and UPAM will not be started.
 - **3 - No Application Visibility** - Services required for the Application Visibility application will not be started.
 - **4 - No IoT** - Services required for the IoT application will not be started.
 - **5 - No SFLOW** - Services required for the Analytics application (Top N Applications and Top N Clients) will not be started.

Note: You can select multiple options at the prompt for options 2 through 5 by entering the number of each option with a space between each number (e.g., 2 4 5)

Upgrade/Backup/Restore VA

The Upgrade VA command set is used to display information about the currently-installed OmniVista 2500 NMS software, upgrade OmniVista software, configure the OV Build Repository, and backup/restore OV software. OV software and updates are stored on an external repository (ALE Central Repository). By default, the OV Virtual Appliance points to the ALE Central Repository, which contains the latest builds and software updates. If a proxy has been configured, make sure to configure the proxy to connect to the external repository.

Note: If you have configured and enabled a Custom Repository, you must select option **4 – Enable Repository**, and enable the **ALE Custom Repository** to access the latest software.

```

*****
* Upgrade VA *****
* [1] Help *****
* [2] To 4.5R3 (Upgrade to Latest patch of Current Release, if any) *****
* [3] To New Release *****
* [4] Enable Repository (Selected - SQARepo) *****
* [5] Configure Custom Repositories *****
* [6] Configure "Update Check Interval" (Selected - Disabled) *****
* [7] Backup/Restore OmniVista 2500 NMS Data *****
* [0] Exit *****
*****
(*) Type your option: _

```

To access the Upgrade VA Menu, enter 6 at the command prompt. The following options are available:

- **To 4.5R3 (Upgrade to Latest Patch of Current Release, if any)** - Displays information about the currently-installed OmniVista NMS software (e.g., Release Number, Build Number). It also checks for, and displays information about, any available updates. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. Select an option and press **Enter** to display information about the currently-installed OmniVista NMS software and download/upgrade an available update.
- **Download and Upgrade** - OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads and installs the update, if available. (If you are using an Offline Repo, this is the only upgrade option supported. "Download Only" and "Upgrade from a Download Package" are not supported.)
- **Download Only** - OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads the update, if available.
- **Upgrade from a Download Package** - If you have previously downloaded an update but have not yet installed it, OV will install the downloaded update.
 - Note:** You can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available.
- **To New Release** - Upgrade to a new release. The options and processes are the same as above ("To 4.5R3 (Upgrade to Latest Patch of Current Release, if any)"). Note that if a new version of the current release is available, you will be prompted to install the latest version of the current release before upgrading to the new release.
- **Enable Repository** - Enable an OV Build Repository. This is the repository that OmniVista 2500 NMS will use to retrieve OV upgrade software. Select a repository from the list, enter **y** and press **Enter** at the confirmation prompt to enable the repository. Only one (1) repository can be enabled at a time.
- **Configure Custom Repositories** - Configure a custom repository. By default, the OV Virtual Appliance points to the external ALE Central Repository, which contains the latest OV software. However, you can configure up to three (3) custom repositories. Select a repository (e.g., [2] "Custom Repo 1" Repository) and press **Enter**. Complete the fields as described below, then enter **y** and press **Enter** at the confirmation prompt:
 - **Repository Name** - User-configured repository name.
 - **Repository URL** - The URL of the custom repository (e.g., 192.168.70.10/repo/centos). Enter the URL only. There is no need to enter the "https://" prefix.

Only one (1) repository can be enabled at a time. The user is responsible for ensuring that the custom repository contains the latest OV software.

- **Configure Update Check Interval** - Configure how often the OmniVista 2500 NMS Server will check the OV Build Repository for updates. You can perform a check immediately or schedule the check to be performed at regular intervals. The results of the scheduled checks are displayed on the Welcome Screen.
 - **Check Now** - Run the Update Check Task immediately and displays the results. Enter **2** and press **Enter**. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. If an upgrade is available, enter **y** and press **Enter** to install the upgrade. Note that you can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available. Also note that if a new release is available (e.g., R01 to R02), and do not have the latest R01 software patches installed, you will first be prompted to install the latest R01 patches, and will then be prompted to install R02.
 - **Check Daily/Weekly/Monthly** - Run the Update Check Task at the configured intervals and displays the results on the Welcome Screen. Select an interval and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
 - **Disable (Default)** - Disable the Update Check Task. Enter **6** and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
- **Backup/Restore OV2500 NMS Data** - Backup/Restore OmniVista 2500 NMS data. The following options are available. Note that Backup/Restore is only supported on HA Installations on Release 4.5R1 and later.
 - **Configure Backup Retention Policy** - Configure the maximum number of days that you want to retain backups (Range = 1 – 30, Default = 7), and the maximum number of backups that you want to retain (Range = 1 – 30, Default = 5). Backup files are automatically deleted based on the Backup Retention Policy.
 - **Backup Now** - Perform an immediate backup. Enter an optional name for the backup (default = ov2500nms) and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. When the backup is complete, it will be stored in the “backups” Directory with the backup name and the date and time of the backup (<base name>_<yyyy-MM-dd--HH-mm>.bk). If you do not enter a name, the backup will be stored as ov2500nms- yyyy-MM-dd--HH-mm>.bk. (e.g., ov2500nms-2018-11-16--16-21.bk).
 - **Schedule Backup** - You can schedule an automatic backup to begin at a specific time and repeat at a specific daily interval. Enter a time for the backup to begin (HH:mm format) and press **Enter**. Enter the time between backups (Range = 1 – 30 Days, Default = 1) and press **Enter**. You can change the backup schedule at any time.
 - Note:** Scheduled backups utilize the Task Scheduler (Windows) and Cron Job (Linux) utilities. If necessary, these utilities can be used to modify a scheduled backup.
 - Note:** Backup files are automatically deleted based on the Backup Retention Policy. Monitor and maintain the Backup Directory to optimize disk space.
- **Restore** - Select a backup and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt and press **Enter**.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

Note: You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.5R3 configuration using a 4.5R3 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 4.5R3 Backup File residing on a different system, you must change the OV IP address/ports and UPAM IP address/ports of the system on which you are performing the restore to match the OV IP address/ports and UPAM IP address/ports of the system from which the backup file was taken before performing the restore. After the restore is complete, you can use the Configure Cluster Menu to return the restored system to its original OV IP address/ports and UPAM IP address/ports.

For example, if you want to use a backup file on System A to perform a restore on the System B, you must change the OV IP address/ports and UPAM IP address/ports of System B to the OV IP address/ports and UPAM IP address/ports of System A before performing the restore. After the restore is complete, you can use the Configure Cluster Menu to change the OV IP address/ports and UPAM IP address/ports on System B back to their original configuration.

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

Logging

You can view OmniVista Logs using the “Logging” option. Enter **7**, then press **Enter**.

```
*****
* Configure Logging
*****
* [1] Help
* [2] Change Log Level
* [3] Collect Log Files
* [4] Collect JUM Information
* [5] Collect Files in Advanced Mode
* [0] Exit
*****
(*) Type your option: 0
```

The following options are available:

- **Change Log Level** - Changes the logging level for OV services. Enter the number corresponding to the OV service for which you want to change the logging level (e.g. 13 - ovsip) and press **Enter**. Enter the number corresponding to the package for which you want to change the logging level (e.g. 1 - com.alu.ov.ngms.sip.service) and press **Enter**. Enter the number corresponding to the log level you want to set (e.g., 2 - DEBUG) and press **Enter**.
- **Collect Log Files** - Collects all log files from a specific date to the current date. Enter the date from which you want to collect log files in dd-MM-yyyy format (e.g., 10-15-2018) and press **Enter**. When finished, a "Collecting completed" message is displayed. The log files are stored in a zip file in the "logs" Directory with the date and time the logs were collected appended to the file name (e.g., ovlogs-15-10-2019_12-04-19.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-02019-10-15-12-19-43.jar). SFTP to the VA using the "cliadmin" username and password to view the log file (Port 22).
- **Collect Files in Advanced Mode** - Collects and archives tcpdump information to a Zip file in the "chrootadmin" directory with date and time the file was created appended to the file name (e.g., chrootadmin_10-03-2020-11-02-43.zip). SFTP to the VA using the "cliadmin" username and password to view the log file (Port 22).

Set Up Optional Tools

Enter **8**, then press **Enter** to bring up the Setup Optional Tools command set. The Setup Optional Tools command set is used to install/upgrade Hypervisor Optional Tools Packages.

```
*****
* Optional Tool Of Supervisors Menu
*****
* [1] Help
* [2] VMware Tools
* [3] VirtualBox Guest Additions
* [0] Exit
*****
(*) Type your option: s_
```

Enter the number corresponding to the Hypervisor you are using (**2 – VMWare Tools, 3 - Virtual Box Guest Additions**) and press **Enter**. Information about available packages is displayed. If a new package is available, enter **y** and press **Enter** at the "Would you like to install the package" prompt. The package will automatically be downloaded from the OV Repository and installed (this may take several minutes). When the "Installation Complete" message is displayed, press **Enter** to continue. Press **Enter** again to restart the Virtual Appliance.

Note: The option for Virtual Box Guest tools is for test/experimental purposes only and is not officially supported.

Advanced Mode

Advanced Mode enables you to use read-only UNIX commands for troubleshooting. Enter **9**, then press **Enter** to bring up the CLI prompt. Enter **exit** and press **Enter** to return to the Virtual Appliance Menu. The following commands are supported:

- /usr/bin/touch
- /usr/bin/mktemp
- /usr/bin/dig
- /usr/bin/cat
- /usr/bin/nslookup
- /usr/bin/which
- /usr/bin/less
- /usr/bin/tail
- /usr/bin/vi

- /usr/bin/tracepath
- /usr/bin/tty
- /usr/bin/systemctl
- /usr/bin/grep
- /usr/bin/egrep
- /usr/bin/fgrep
- /usr/bin/dirname
- /usr/bin/readlink
- /usr/bin/locale
- /usr/bin/ping
- /usr/bin/traceroute
- /usr/bin/netstat
- /usr/bin/id
- /usr/bin/ls
- /usr/bin/mkdir
- /usr/sbin/ifconfig
- /usr/sbin/route
- /usr/sbin/blkid
- /usr/sbin/sshd-keygen
- /usr/sbin/consoletype
- /usr/sbin/ntpdate
- /usr/sbin/ntpq
- /usr/bin/ntpstat
- /usr/bin/abrt-cli
- /usr/sbin/init
- /usr/sbin/tcpdump
- /bin/mountpoint

Power Off

Before powering off the VM, you must stop all services using the **Stop All Services** option in the **Run Watchdog Command**. After all the services are stopped, enter **10** at the command line to power off the VM. Confirm the power is off by entering **y**. The power off may take several minutes to complete.

Note: OmniVista functions stop running following power off. The VM must be powered back on via the VMware client software and you must log back into the VM via the console.

Reboot

Before rebooting the VM, you must stop all services using the **Stop All Services** option in the **Run Watchdog Command**. After all services are stopped, enter **11** at the command line to reboot the VM. Confirm reboot by entering **y**. The reboot may take several minutes to complete.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

When rebooted, you will be prompted to log in through the cliadmin user and password prompts. Note that OmniVista functions continue following reboot.

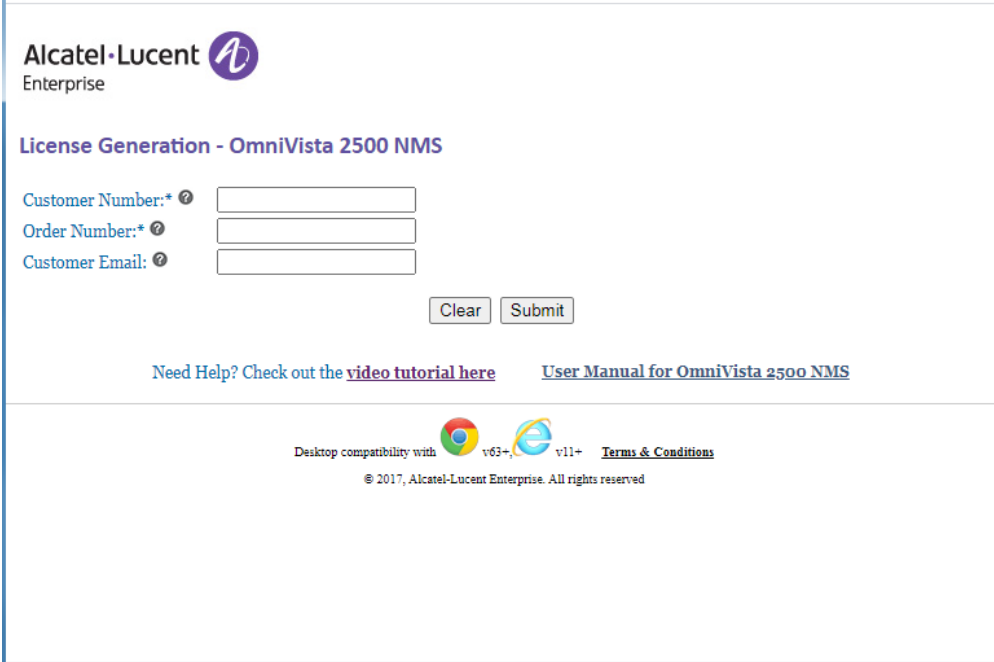
Log Out

To log out of the VM and return to the cliadmin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OmniVista functions continue following logout.

Appendix C – Generating an Evaluation License

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

1. Go to <https://lds.al-enterprise.com/ARB/loadOmniVistaLicGeneration.action>.



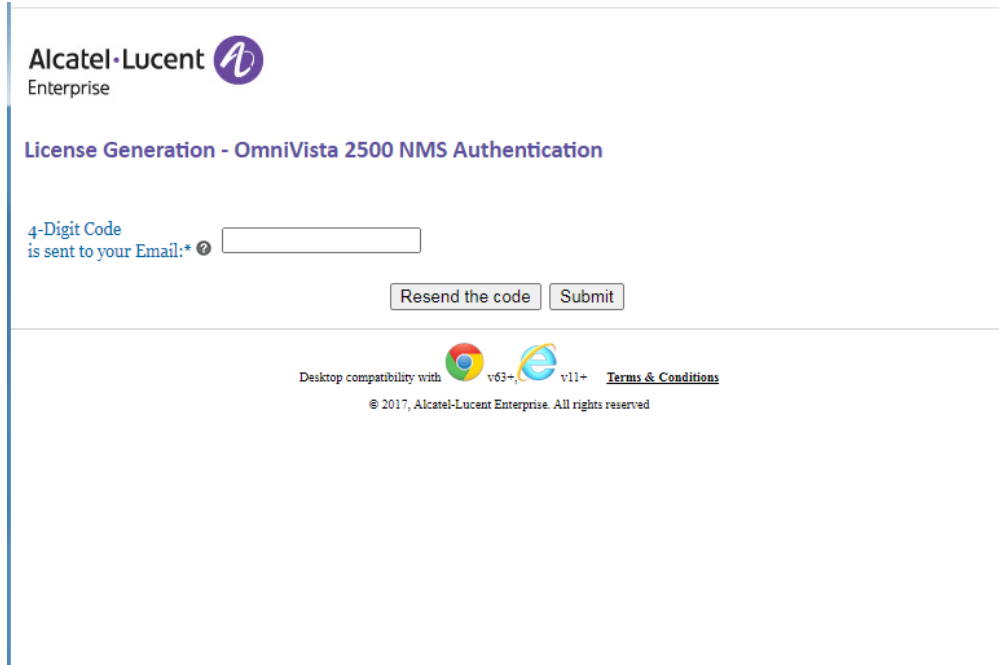
The screenshot shows a web form titled "License Generation - OmniVista 2500 NMS" from Alcatel-Lucent Enterprise. The form includes three input fields: "Customer Number:*" with a help icon, "Order Number:*" with a help icon, and "Customer Email:" with a help icon. Below the fields are "Clear" and "Submit" buttons. At the bottom of the form, there are links for "Need Help? Check out the video tutorial here" and "User Manual for OmniVista 2500 NMS". The footer contains compatibility information for Chrome (v63+) and Internet Explorer (v11+), a "Terms & Conditions" link, and a copyright notice: "© 2017, Alcatel-Lucent Enterprise. All rights reserved".

2. Complete the fields as described below, then click **Submit**.

- **Customer ID** – 99999
- **Order Number** – evaluation
- **Customer Email** – Enter your contact email.

A 4-Digit Code will be sent to your e-mail. The following screen will appear.



OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



Alcatel-Lucent Enterprise

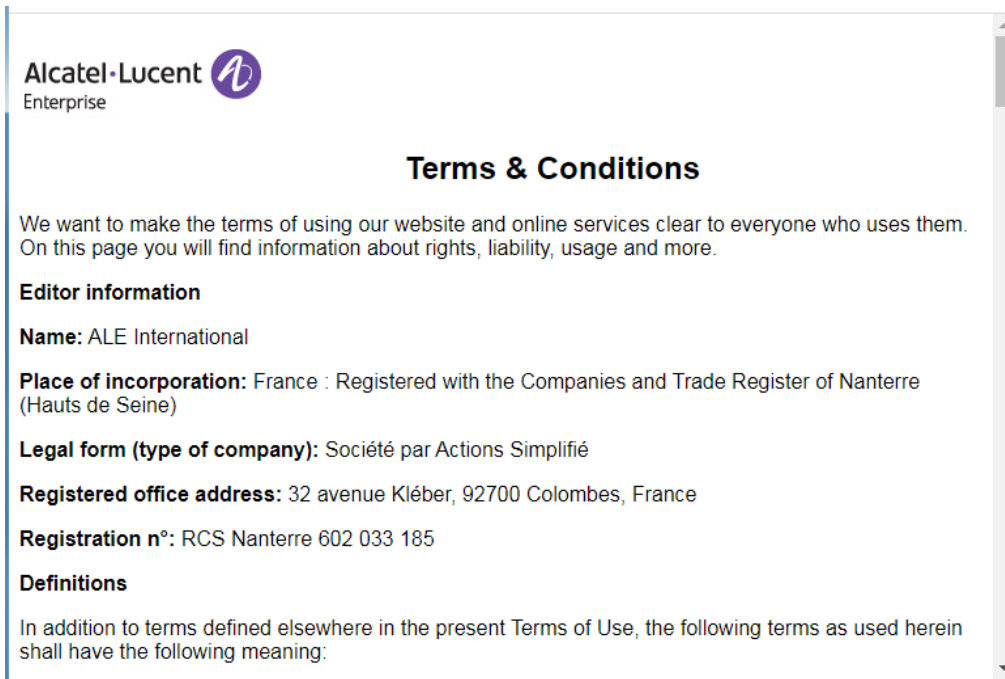
License Generation - OmniVista 2500 NMS Authentication

4-Digit Code is sent to your Email.*

Desktop compatibility with  v63+,  v11+ [Terms & Conditions](#)

© 2017, Alcatel-Lucent Enterprise. All rights reserved

3. Enter the 4-Digit Code sent to your e-mail, and click **Submit**. A Terms and Conditions notice will display.



Alcatel-Lucent Enterprise

Terms & Conditions

We want to make the terms of using our website and online services clear to everyone who uses them. On this page you will find information about rights, liability, usage and more.

Editor information

Name: ALE International

Place of incorporation: France : Registered with the Companies and Trade Register of Nanterre (Hauts de Seine)

Legal form (type of company): Société par Actions Simplifié

Registered office address: 32 avenue Kléber, 92700 Colombes, France

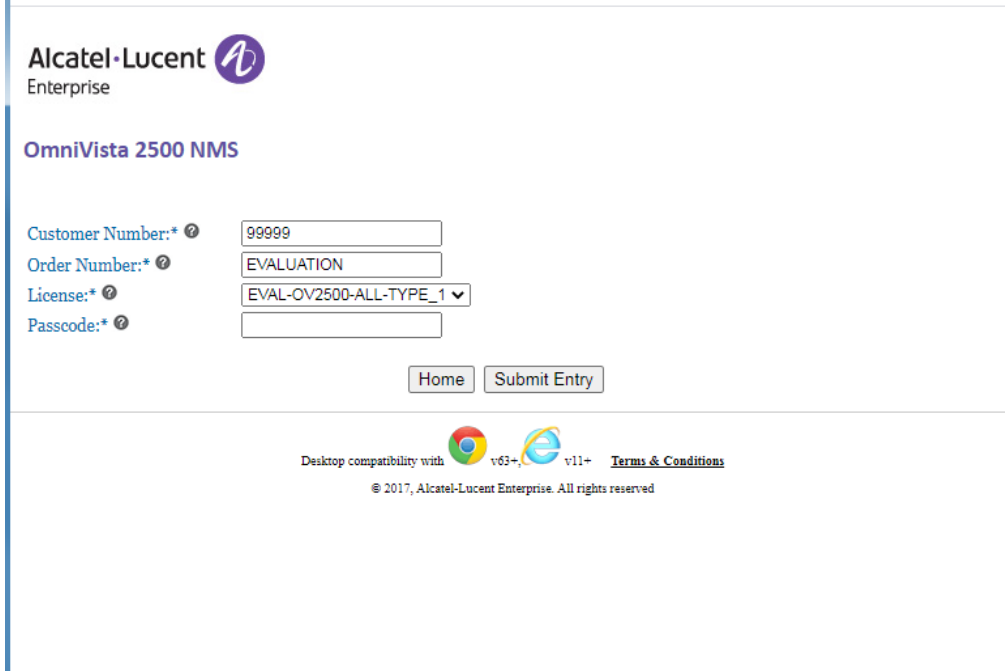
Registration n°: RCS Nanterre 602 033 185

Definitions

In addition to terms defined elsewhere in the present Terms of Use, the following terms as used herein shall have the following meaning:

4. Read through the Terms and Conditions. At the bottom of the screen click on the “Accept All Terms and Conditions” checkbox, and click **Accept**. The following screen will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide



The screenshot shows the Alcatel-Lucent Enterprise logo at the top left. Below it, the text "OmniVista 2500 NMS" is displayed. The form contains four input fields: "Customer Number:*" with the value "99999", "Order Number:*" with the value "EVALUATION", "License:*" with a dropdown menu showing "EVAL-OV2500-ALL-TYPE_1", and "Passcode:*" which is empty. Below the fields are two buttons: "Home" and "Submit Entry". At the bottom of the form, there is a compatibility notice: "Desktop compatibility with" followed by icons for Chrome (v63+), Internet Explorer (v11+), and a link to "Terms & Conditions". A copyright notice "© 2017, Alcatel-Lucent Enterprise. All rights reserved" is at the very bottom.

Note: Steps 2 - 4 above are only applicable the first time you apply for an Evaluation License (provide your e-mail ID, complete the security process by entering the 4-digit unique code, and accept the Terms and Conditions). Once your e-mail ID is verified, if you enter your e-mail ID again to generate an Evaluation License, you do not have to go through Steps 2 – 4. After Step 1, the screen above will appear and you can continue to Step 5 below.

5. Complete the fields as described below, then click **Submit Entry**.

- **Customer ID** – 99999 (pre-filled)
- **Order Number** – EVALUATION (pre-filled)
- **License** – EVAL-OV2500-ALL-TYPE_1 (pre-selected)
- **Passcode** – omnivista

The following screen will appear.

OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide

The screenshot shows the Alcatel-Lucent Enterprise logo at the top left. Below it is the title "OmniVista 2500 NMS License Registration". The form contains four input fields: "Site Name:*" with the value "EVALUATION", "Company Name:*", "Phone:", and "Customer Email:*" with the value "john.brewster@al-enterpris". Below the fields are three buttons: "Home", "Clear", and "Generate License". At the bottom, there is a desktop compatibility notice with icons for Chrome v63+ and Edge v11+, a link to "Terms & Conditions", and a copyright notice: "© 2017, Alcatel-Lucent Enterprise. All rights reserved".

6. Complete the fields as described below, then click **Generate License**.

- **Site Name** – EVALUATION (pre-filled)
- **Company Name** – Company name to be used for the license
- **Phone** – Contact phone number
- **Customer Email** – E-mail address to which the license will be sent.

The license will be downloaded to your computer. (The license file will also be e-mailed to the address you entered in the screen above.)

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