

# OVOC

## Installation, Operation and Maintenance

Version 7.6



## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: January-28-2020

## WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

## Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

## Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

## Stay in the Loop with AudioCodes



## Related Documentation

Document Name
<a href="#">Mediant 500 MSBR User's Manual</a>
<a href="#">Mediant 500L MSBR User's Manual</a>
<a href="#">Mediant 500L Gateway and E-SBC User's Manual</a>
<a href="#">Mediant 800B Gateway and E-SBC User's Manual</a>
<a href="#">Mediant 800B MSBR User's Manual</a>
<a href="#">Mediant 1000B Gateway and E-SBC User's Manual</a>

Document Name
<a href="#">Mediant 1000B MSBR User's Manual</a>
<a href="#">Mediant 2600 E-SBC User's Manual</a>
<a href="#">Mediant 3000 User's Manual</a>
<a href="#">Mediant 4000 SBC User's Manual</a>
<a href="#">Mediant 9000 SBC User's Manual</a>
<a href="#">Mediant Software SBC User's Manual</a>
<a href="#">Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center</a>
<a href="#">One Voice Operations Center IOM Manual</a>
<a href="#">One Voice Operations Center Product Description</a>
<a href="#">One Voice Operations Center User's Manual</a>
<a href="#">Device Manager Pro Administrator's Manual</a>
<a href="#">Device Manager Express Administrator's Manual</a>
<a href="#">One Voice Operations Center Security Guidelines</a>
<a href="#">One Voice Operations Center Integration with Northbound Interfaces</a>
<a href="#">One Voice Operations Center Performance Monitoring Guide</a>
<a href="#">One Voice Operations Center Alarms Monitoring Guide</a>
<a href="#">Device Manager for Third-Party Vendor Products Administrator's Manual</a>
<a href="#">Device Manager Agent Installation and Configuration Guide</a>
<a href="#">ARM User's Manual</a>

## Document Revision Record

LTRT	Description
94153	Initial document release for Version 7.4
94154	Updates to Section 'OVOC Software Deliverables' for Virtual Platforms; Update to Section Installing the OVOC on a Virtual Server Platform to clarify that OVA file is for VMware and Zip file for Hyper-V platform. Update to Section "Server Syslog Configuration" with details added for 'Facility' and 'Severity' level configuration.
94155	Updates to Performance and Data Storage table; Section "OVOC Software Deliverables"; Installation and Upgrade procedures (correction to mounting procedure and removed Java related step); Virtual machine upgrade section added for Hyper-V platform and general enhancements to this section.
94157	Updates for patch version 7.4.1000:

LTRT	Description
	Update to the upgrade procedure with tar file. Replaced the “OVOC Maximum Security Implementation” diagram. Updated several old OVOC Server Managerscreens containing string “EMS” to “OVOC”. Replaced OVOC server: Triple Ethernet Interfaces and Physical Ethernet Interfaces Redundancy screens.
94158	Updates for patch version 7.4.2000: Update for the memory for Low Profile Virtual Machine. Update to the upgrade procedure with tar file. Replaced the “OVOC Maximum Security Implementation” diagram. Updated the Firewall table with new ports for alarm forwarding and alarm resync and corrected description for SNMP port 1161. New Appendix added for enhanced Service Provider specifications.
94159	Updates for patch version 7.4.3000: Updates for the Amazon profile, updates to the Service Provider profile for enhanced capabilities. New OVOC Server Manageroptions for managing TLS version and cipher strings. New OVOC Server Managermenu “Apache Security Settings”. Update for the OVOC Web Client minimum requirements. Update to the Performance and Data Storage table. Updates to the Service Provider Enhanced Specifications appendix.
94160	Updates including new procedure for installation of OVOC on the AWS platform, updates to the pre-installation information for AWS and removal of references to the Geo HA configuration.
94161	Update for support for HP DL360p G10 dedicated hardware; correction to the Performance and Data Storage table; update for installing DVD1 without a CD-ROM; correction to the DB Password requirements and removed the HA for dedicated hardware section.
94162	<ul style="list-style-type: none"> <li>■ Updated to Software Version 7.6.125</li> <li>■ Update to Managed VoIP Equipment table for new phone version 445HD; Update to Hardware and Software Requirements table (ESXi version) and browser version support; Firewall table</li> <li>■ Section added: Proxy Settings option; IPP HTTPS Authentication Mode option; Trust Configuration Store; Server Logger Levels</li> </ul>
94163	Update to sections "Upgrading the OVOC server-DVD" and "Proxy Settings"
94164	Correction to Table Caption and Heading for Enhanced Service Providers Specifications Appendix.
94165	<p>Added Sections: Installation and Upgrade Troubleshooting of the Operational Environment; Network Traffic Capture</p> <p>Updated Sections: Managed VoIP Equipment; OVOC server Requirements; Performance and Data Storage; Installing OVOC on the Amazon AWS Platform; Installing OVOC on Microsoft Hyper-V Platform; Installing OVOC on the VMware Platform; Viewing Process Statuses; IPP HTTPS Authentication Mode; Manage IPP Files Service Port (8080); Manage IPPs HTTP Port (8081); Manage IPPs HTTPS Port (8082); Upgrading OVOC on a Virtual Platform; Upgrading the OVOC server on Dedicated Hardware; Upgrading OVOC on a Virtual Platform; Updated Firewall table and diagram; Updated HTTPS diagram.</p>
94166	Added Sections: Installing the OVOC Server from the Microsoft Azure



LTRT	Description
	Marketplace; Managing Devices Behind a NAT; License.
94167	Added Section: Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) 6.5
94169	Updated Sections: Hardware and Software requirements; Firewall table for Websocket server; Websocket server status description; update to License screen and new Floating License Service parameters New Sections: Floating License (Port 912); OVOC WebSocket (Port 915)
94170	New Sections: Configuring Email Forwarding on Microsoft Azure using Microsoft Office 365; Configuring Email Forwarding on Microsoft Azure using SNMP Relay. Updated Section: HTTPS/SSL/TLS Security (clarification of TLS version support)
94171	New Section: Connecting Mediant Cloud Edition (CE) SBC Devices in Azure Deployment; Firewall table text editing; miscellaneous updates Removed Section; "Testing Install Requirements"; Section "Files Verification" promoted to Chapter.

## Table of Contents

<b>1 Overview</b>	<b>1</b>
<b>Part I</b>	<b>2</b>
<b>Pre-installation Information</b>	<b>2</b>
<b>2 Managed VoIP Equipment</b>	<b>3</b>
<b>3 Hardware and Software Specifications</b>	<b>7</b>
OVOC Server Requirements	7
OVOC Client Requirements	9
Bandwidth Requirements	9
OVOC Bandwidth Requirements	9
Voice Quality Bandwidth Requirements	9
Fault Management - Alarms History	10
Performance and Data Storage	11
Skype for Business Monitoring SQL Server Prerequisites	12
<b>4 OVOC Software Deliverables</b>	<b>14</b>
Dedicated Hardware Installation – DVDs 1-3	14
Virtual Appliance and Cloud Options	14
Virtual Machine and Cloud Deployments Upgrade Media	14
<b>Part II</b>	<b>15</b>
<b>OVOC Server Installation</b>	<b>15</b>
<b>5 Installing OVOC Server on the Amazon Web Services (AWS) Platform</b>	<b>16</b>
<b>6 Installing OVOC Server on the Microsoft Azure Platform</b>	<b>22</b>
Managing Devices Behind an Enterprise Firewall or NAT	27
Configuring OVOC as the Email Server on Microsoft Azure	27
Configuring OVOC to Forward Alarms by Email on Microsoft Azure using Microsoft Office 365	27
Configuring OVOC as Email Server on Microsoft Azure using SMTP Relay	28
Connecting Mediant Cloud Edition (CE) SBC Devices in Azure Deployment	30
Step 1: Configuring the OVOC Virtual Machine on Azure Cloud	31
Step 2: Configuring the OVOC Server (EMS Server Manager) on Azure Cloud	32
Step 3: Configuring Mediant Cloud Edition (CE) Device	32
Step 3-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager	32
Step 3-2: Configuring Mediant CE OVOC Communication Settings using Web Interface	33
<b>7 Installing OVOC Server on the Microsoft Hyper-V Virtual Machine</b>	<b>35</b>
Configuring the Virtual Machine Hardware Settings	39
Expanding Disk Capacity	41
Changing MAC Addresses from 'Dynamic' to 'Static'	45
Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster	45
Hyper-V Cluster Site Requirements	46
Add the OVOC VM in Failover Cluster Manager	46
Cluster Host Node Failure on Hyper-V	48

Connecting OVOC Server to Network on HyperV .....	48
<b>8 Installing OVOC Server on a VMware Virtual Machine .....</b>	<b>51</b>
Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) 6.5 .....	51
Configuring the Virtual Machine Hardware Settings .....	52
Configuring OVOC Virtual Machines (VMs) in a VMware Cluster .....	54
VMware Cluster Site Requirements .....	54
Cluster Host Node Failure on VMware .....	56
Connecting OVOC Server to Network on VMware .....	57
<b>9 Installing OVOC Server on Dedicated Hardware .....</b>	<b>59</b>
DVD1: Linux CentOS 7.3 .....	59
Installing DVD1 without a CD-ROM .....	62
DVD2: Oracle DB Installation .....	66
DVD3: OVOC server Application Installation .....	68
<b>10 Files Verification .....</b>	<b>72</b>
Windows .....	72
Linux .....	72
OVOC Server Users .....	72
<b>Part III .....</b>	<b>73</b>
<b>OVOC Server Upgrade .....</b>	<b>73</b>
<b>11 Upgrading OVOC Server on Dedicated Hardware .....</b>	<b>74</b>
Upgrading the OVOC Server-DVD .....	74
Upgrading the OVOC Server using an ISO File .....	76
<b>12 Upgrading OVOC Server on a Virtual Platform .....</b>	<b>79</b>
Step 1: Setup the Virtual Machine .....	79
Setting up VMware Platform for Upgrade .....	79
Setting up Using VMware Remote Console Application (VMRC) .....	82
Setting up Using VMware Server Host for Upgrade .....	85
Setting Up Microsoft Hyper-V Platform for Upgrade .....	86
Step 2: Run the Upgrade Script .....	90
Step 3: Connect the OVOC Server to Network .....	91
VMware Platform .....	91
Hyper-V Platform .....	92
<b>13 Installation and Upgrade Troubleshooting of the Operational Environment</b>	<b>95</b>
<b>Part IV .....</b>	<b>97</b>
<b>OVOC Server Machine Backup and Restore .....</b>	<b>97</b>
<b>14 OVOC Server Backup .....</b>	<b>98</b>
Change Schedule Backup Time .....	98
<b>15 OVOC Server Restore .....</b>	<b>99</b>
<b>Part V .....</b>	<b>100</b>

<b>OVOC Server Manager</b>	<b>100</b>
<b>16 Getting Started</b>	<b>101</b>
Connecting to the OVOC Server Manager	101
Using the EMS Server Manager	103
<b>17 Viewing Process Statuses</b>	<b>104</b>
<b>18 Viewing General Information</b>	<b>106</b>
<b>19 Collecting Logs</b>	<b>108</b>
<b>20 Application Maintenance</b>	<b>110</b>
Start or Restart the Application	110
Stop the Application	111
Web Servers	111
Apache and Tomcat Server Processes	112
Change Schedule Backup Time	112
Restore	112
License	112
OVOC Time License	113
Shutdown the OVOC Server Machine	115
Reboot the OVOC Server Machine	116
<b>21 Network Configuration</b>	<b>117</b>
Server IP Address	117
Ethernet Interfaces	118
OVOC Client Login on all OVOC Server Network Interfaces	118
Add Interface	120
Remove Interface	121
Modify Interface	121
Ethernet Redundancy	121
Add Redundant Interface	123
Remove Ethernet Redundancy	123
Modify Redundant Interface	124
DNS Client	125
NAT	126
Static Routes	126
Proxy Settings	127
SNMP Agent	128
SNMP Agent Listening Port	129
Linux Trap Forwarding Configuration	129
Server SNMPv3 Engine ID	130
<b>22 Date and Time Settings</b>	<b>131</b>
NTP	131
Stopping and Starting the NTP Server	132
Restrict Access to NTP Clients	132
Timezone Settings	132

Date and Time .....	133
<b>23 Security .....</b>	<b>134</b>
OVOC User .....	134
SSH .....	135
SSH Log Level .....	135
SSH Banner .....	136
SSH on Ethernet Interfaces .....	136
Add SSH to All Ethernet Interfaces .....	137
Add SSH to Ethernet Interface .....	137
Remove SSH from Ethernet Interface .....	137
Enable/Disable SSH Password Authentication .....	138
Enable SSH IgnoreUserKnownHosts Parameter .....	138
SSH Allowed Hosts .....	139
Allow ALL Hosts .....	139
Deny ALL Hosts .....	139
Add Hosts to Allowed Hosts .....	140
Remove Host/Subnet from Allowed Hosts .....	141
Oracle DB Password .....	141
OS Users Passwords .....	142
General Password Settings .....	142
Operating System User Security Extensions .....	143
File Integrity Checker .....	145
Software Integrity Checker (AIDE) and Pre-linking .....	145
USB Storage .....	145
Network Options .....	146
Auditd Options .....	147
HTTPS/SSL/TLS Security .....	147
Enable Statistics Report Web Page Secured Connection .....	148
Server Certificates Update .....	149
OVOC Voice Quality Package - OVOC Managed Devices Communication .....	153
HTTP Security Settings .....	154
TLS Version 1.0 .....	154
TLS Version 1.1 .....	155
Show Allowed SSL Cipher Suites .....	155
Edit SSL Cipher Suites Configuration String .....	155
Restore SSL Cipher Suites Configuration Default .....	156
Manage HTTP Service Port (80) .....	156
Manage IPP Files Service Port (8080) .....	156
Manage IPPs HTTP Port (8081) .....	157
Manage IPPs HTTPS Port (8082) .....	157
OVOC Rest (Port 911) .....	157
Floating License (Port 912) .....	157
OVOC WebSocket (Port 915) .....	157
SBC HTTPS Authentication Mode .....	158
Enable Device Manager Pro and NBIF Web Pages Secured Communication .....	158

Change HTTP/S Authentication Password for NBIF Directory .....	159
<b>24 Diagnostics .....</b>	<b>160</b>
Server Syslog Configuration .....	160
Devices Syslog Configuration .....	162
Devices Debug Configuration .....	162
Server Logger Levels .....	163
Network Traffic Capture .....	164
<b>Part VI .....</b>	<b>166</b>
<b>Configuring the Firewall .....</b>	<b>166</b>
<b>25 Configuring the Firewall .....</b>	<b>167</b>
<b>Part VII .....</b>	<b>176</b>
<b>Appendix .....</b>	<b>176</b>
<b>26 Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Servers .....</b>	<b>177</b>
Prerequisites .....	177
Hardware Preparation .....	177
Configuring RAID-0 .....	177
<b>27 Managing Clusters .....</b>	<b>184</b>
Migrating OVOC Virtual Machines in a VMware Cluster .....	184
Moving OVOC VMs in a Hyper-V Cluster .....	185
<b>28 Supplementary Security Procedures .....</b>	<b>189</b>
Installing Custom Certificates on OVOC Managed Devices .....	189
Enterprise Gateways and SBC Devices .....	189
Step 1: Generate a Certificate Signing Request (CSR) .....	189
Step 2: Receive the New Certificates from the CA .....	191
Step 3: Update Device with New Certificate .....	191
Step 4: Update Device's Trusted Certificate Store .....	192
Step 5: Configure HTTPS Parameters on the Device .....	192
Step 6: Reset Device to Apply the New Configuration .....	193
MP-1xx Devices .....	194
Step 1: Generate a Certificate Signing Request (CSR) .....	194
Step 2: Receive the New Certificates from the CA .....	195
Step 3: Update Device with New Certificate .....	196
Step 4: Update Device's Trusted Certificate Store .....	196
Step 5: Configure HTTPS Parameters on Device .....	198
Step 6: Reset Device to Apply the New Configuration .....	198
Cleaning up Temporary Files on OVOC Server .....	199
<b>29 Transferring Files .....</b>	<b>200</b>
<b>30 Verifying and Converting Certificates .....</b>	<b>201</b>
<b>31 Self-Signed Certificates .....</b>	<b>202</b>

Internet Explorer .....	202
Using Mozilla Firefox .....	202
Chrome .....	203
<b>32 Datacenter Disaster Recovery .....</b>	<b>204</b>
Introduction .....	204
Solution Description .....	204
Initial Requirements .....	204
New Customer Configuration .....	205
Data Synchronization Process .....	205
Recovery Process .....	205
<b>33 Service Provider - Enhanced Specifications for VMware Virtual Platform .....</b>	<b>207</b>

# 1 Overview

The One Voice Operations Center (OVOC) provides customers with the capability to easily and rapidly provision, deploy and manage AudioCodes devices and endpoints. Provisioning, deploying and managing these devices and endpoints with the OVOC are performed from a user-friendly Web Graphic User Interface (GUI). This document describes the installation of the OVOC server and its components. It is intended for anyone responsible for installing and maintaining AudioCodes' OVOC server and the OVOC server database.



# Part I

## Pre-installation Information

This part describes the OVOC server components, requirements and deliverables.

## 2 Managed VoIP Equipment

The following products (and product versions) can be managed by this OVOC release:

**Table 2-1: Managed VoIP Equipment**

Product	Supported Software Version
<b>Gateway, SBC and MSBR Devices</b>	
Mediant 9000 SBC	Versions 7.2 (including support for MTC ), 7.0, 6.8
Mediant 4000 SBC	Versions 7.2, 7.0 and 6.8
Mediant 4000B SBC	Version 7.2, 7.0
Mediant 2600 E-SBC	Versions 7.2, 7.0 and 6.8
Mediant 2600B E-SBC	Version 7.2 and 7.0
Mediant Software (Server Edition) SBC	Versions 7.2, 7.0 and 6.8
Mediant Software(Virtual Edition) SBC	Versions 7.2 (including support for MTC), 7.0 and 6.8
Mediant3000 (TP-8410 and TP-6310)	Versions 7.0 (SIP), Version 6.8 (SIP) and Version 6.6 (SIP)
Mediant <b>Cloud Edition</b>	<b>Version 7.2</b>
Mediant 2000 Media Gateways	Version 6.6
<sup>1</sup> Mediant 1000 Gateway	Version 6.6 (SIP)
Mediant 1000B Gateway and E-SBC	Versions 7.2, 7.0, 6.8 and 6.6
Mediant 800B Gateway and E-SBC	Versions 7.2, 7.0, 6.8 and 6.6
<b>Mediant 800C</b>	<b>Version 7.2</b>
Mediant 1000B MSBR	Version 6.6
Mediant800 MSBR	Versions 7.2, 6.8 and 6.6
Mediant500 MSBR	Version 7.2 and 6.8
Mediant 500L MSBR	Versions 7.2 and 6.8
Mediant 500 E-SBC	Version 7.2
Mediant 500L E-SBC	Version 7.2
<sup>2</sup> Mediant 600	Version 6.6

<sup>1</sup>This product does not support Voice Quality Management.

<sup>2</sup>As above

Product	Supported Software Version
MediaPack MP-11x series	Version 6.6 (SIP)
MediaPack MP-124	Rev. D and E – version 6.6 (SIP)
MP- 202D, MP-202R	
MP-204R	
MP-1288	Version 7.2
<b>SBA<sup>1</sup></b>	
Mediant 800B SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.2
Mediant 800C SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.2
Mediant 1000B SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.2
Mediant 2600B SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.0
Mediant800B SBA Lync Server	SBA version 1.1.12.x and later and gateway Version 6.8
Mediant 1000B SBA Lync Server	SBA version 1.1.12.x and later and gateway Version 6.8
Mediant 2000B SBA devices Lync Server	SBA version 1.1.12.x and later and gateway Version 6.8
<b>CloudBond<sup>2</sup></b>	
CloudBond 365 Pro Edition	Version 7.6 with MediantServer version 7.2.100 and later
CloudBond 365 Enterprise Edition	Version 7.6 with MediantServer version 7.2.100 and later
CloudBond 365 Standard+ Edition	Version 7.6 with Mediant800B version 7.2.100 and later
CloudBond 365 Standard Edition	Version 7.6 with Mediant 800B version 7.2.100 and later
User Management Pack 365	Version 7.8

---

<sup>1</sup>As above

<sup>2</sup>To support Voice Quality Management for these devices, customers must add the SBC/Media Gateway platform of these products as standalone devices to OVOC. Once this is done, the SBC/Gateway calls passing through the CloudBond 365 /CCE Appliances can be monitored.

Product	Supported Software Version
<b>CCE Appliance<sup>1</sup></b>	
Mediant 800 CCE Appliance	Version 2.1 with Mediant 800B
Mediant Server CCE Appliance	Version 2.1 with Mediant Server
<b>Other Applications</b>	
SmartTAP 360° Recording	Version 4.3
<b>IP Phones</b>	
<b>Supported Software Versions/Models</b>	
400HD Series Lync server	Version 2.0.13 with models 420HD, 430HD 440HD
400HD Series Non-Lync server	From version 2.2.2 with models 420HD, 430HD 440HD and 405
400HD Series Skype for Business	From version 3.0.0 with models 420HD, 430HD 440HD and 405HD
400HD Series Skype for Business	From version 3.0.1 with models 420HD, 430HD 440HD, 405HD and 450HD From version 3.0.2 with models HRS (with Jabra firmware support) From version 3.1.0 with model 445HD
<b>Third-party Vendor Devices</b>	
Spectralink	Spectralink 8440
Polycom	Polycom Trio 8800
	<b>Polycom VVX 410</b>
<b>Jabra Headset Support</b>	Jabra BIZ, Jabra Coach, Jabra DIAL, Jabra Eclipse, Jabra Elite, Jabra Engage, Jabra Evolve, Jabra Handset, Jabra LINK, Jabra Motion, Jabra Pro, Jabra Pulse, Jabra SPEAK, Jabra Sport, Jabra STEALTH, Jabra Steel, Jabra SUPREME. For a complete list of supported Jabra phones, see document Device Manager for Third-Party Vendor Products Administrator's Manual.

---

<sup>1</sup>As above.



- All versions VoIP equipment work with the SIP control protocol.
- **Bold** refers to new product support and version support.

### 3 Hardware and Software Specifications

This section describes the hardware and software specifications of the OVOC server.

#### OVOC Server Requirements

This table below lists the minimum requirements for running the different OVOC server platforms.



For enhanced service provider specifications, refer to Appendix [Service Provider - Enhanced Specifications for VMware Virtual Platform](#) on page 207

**Table 3-1: OVOC Server Minimum Requirements**

Resource	Dedicated OVOC server-Linux OS	AWS	Azure	Virtual OVOC
Hardware	<ul style="list-style-type: none"> <li>■ <b>G8:</b> HP DL360p</li> <li>■ <b>G10:</b> HP DL360p</li> </ul>	—	—	—
Operating System	<ul style="list-style-type: none"> <li>■ <b>G8:</b> Linux CentOS Version 7.3-1611 64-bit, Rev. 18</li> <li>■ <b>G10:</b> Linux CentOS Version 7.3-1611 64-bit, Rev. 19</li> </ul>	Linux CentOS Version 7.3-1611 64-bit, Rev. 19		Linux CentOS Version 7.3-1611 64-bit, Rev. 19
Virtualization platform	—	AWS EC2 Instance Type: c4.xlarge	<ul style="list-style-type: none"> <li>■ High Profile: VM Size: F16s</li> <li>■ Low Profile: VM Size D4s_v3</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware: ESXi 6.7</li> <li>■ VMware HA cluster: VMware ESXi 6.5</li> <li>■ Microsoft Hyper-V Server 2012 R2</li> <li>■ Microsoft Hyper-V Server HA cluster: 2012 R2</li> <li>■ Microsoft</li> </ul>

Resource	Dedicated OVOC server-Linux OS	AWS	Azure	Virtual OVOC
				Hyper-V Server 2016 ■ Microsoft Hyper-V Server 2016 HA cluster
Memory	■ <b>G8:</b> 32 GB RAM ■ <b>G10:</b> 64 GB RAM	30GiB (c4.4xlarge)	■ High Profile: 32 GB (F16s) ■ Low Profile: 16 GB (D4s_v3)	■ Low Profile: 16 GB RAM ■ High Profile: 32 GB RAM
Disk space	■ <b>G8:</b> Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0 ■ <b>G10:</b> Disk: 2x 1.92 TB SSD configured in RAID 0	AWS EBS: General Purpose SSD (GP2) 2TB	■ High Profile: 2 TB SSD ■ Low Profile: 500 GB SSD	■ Low Profile: 500 GB ■ High Profile: 1.2 TB
Processor	■ <b>G8:</b> CPU: Intel Xeon E5-2690 (8 cores 2.9 GHz each) ■ <b>G10:</b> CPU: Intel (R) Xeon(R) Gold 6126 (12 cores 2.60 GHz each)	16 vCPUs (c4.4xlarge)	■ High Profile: 16 vCPUs (F16s) ■ Low Profile: 4 vCPUs (D4s_v3)	■ Low Profile: 1 core with at least 2.5 GHz ■ Low Profile: 2 core with at least 2.0 GHz ■ High Profile: 6 cores with at least 2 GHz
DVD-ROM	Local (G8 only)	—	—	—

- The OVOC server works with the Java Development Kit (JDK) version 1.8 (JDK 1.8 for Linux™).
- The Oracle database used is version 12.1.0.2.

- Flash Version 11 is required for generating Statistics Reports.



- The JDK and Oracle database component versions mentioned above are provided as part of the OVOC installation image.
- The HP ProLiant DL360 G8 server is now End-of-Sale due to Hewlett-Packard's (HP) End-of-Life announcement for this server. AudioCodes will continue supporting the HP ProLiant DL360 G8 server for OVOC Versions 7.4 and 7.6. However, the HP ProLiant DL360 G8 server will no longer be supported from Version 7.8 (expected around Q3/2019). For Versions 7.4 and 7.6, Description Documents relating to patches and Release Notes associated with major releases will include separate capacity information for the HP ProLiant DL360 Gen8 and HP DL360 Gen10 servers.

## OVOC Client Requirements

The table below lists the minimum requirements for running an OVOC web client.

**Table 3-2: OVOC Client Minimum Requirements**

Resource	OVOC Client
Hardware	PC Resolution 1280 x 1024
Operating System	Windows™ 10; Windows 8; Windows 8.1; Windows 7; Windows 7 Enterprise
Memory	8 GB RAM
Disk Space	-
Processor	-
Web Browsers	<ul style="list-style-type: none"> <li>■ Internet Explorer version 11 and higher</li> <li>■ Mozilla Firefox version 39 and higher</li> <li>■ Google Chrome version 79 and higher</li> </ul>
DVD-ROM	-

## Bandwidth Requirements

This section lists the OVOC bandwidth requirements.

### OVOC Bandwidth Requirements

The bandwidth requirement is for OVOC server <-> Device communication. The network bandwidth requirements per device is 500 Kb/sec for faults, performance monitoring and maintenance actions.

### Voice Quality Bandwidth Requirements

The following table describes the upload bandwidth speed requirements for Voice Quality for the different devices. The bandwidth requirement is for OVOC server <-> Device communication.



**Table 3-3: Voice Quality Bandwidth Requirements**

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
SBC		
MP-118	—	—
MP-124	—	—
Mediant 800 Mediant 850	60	135 Kbits/sec
Mediant 1000	150	330 Kbits / sec
Mediant 2000	—	—
Mediant 2600	600	1.3 Mbit/sec
Mediant 3000	1024	2.2 Mbit/sec
Mediant 4000	4,000	8.6 Mbit/sec
Gateway		
MP-118	8	15 Kbits/sec
MP-124	24	45 Kbits/sec
Mediant 800 Mediant 850	60	110 Kbits/sec
Mediant 1000	120	220 Kbits/sec
Mediant 2000	480	880 Kbits/sec
Mediant 2600	—	—
Mediant 3000	2048	3.6 Mbit/sec
Mediant 4000	—	—
Endpoints	—	56 Kbits/sec

## Fault Management - Alarms History

The table below describes the capacities for the history alarms and journal logs.

**Figure 3-1: Alarm and Journal Capacity**

Resource	Capacity
History Alarms	Up to 12 months or ten million alarms
Journal Logs	Up to 12 months
Alarm Forwarding Aggregation in a single email.	Up to 1000 alarms

## Performance and Data Storage

The following table shows the performance and data storage capabilities for the OVOC managed devices for Voice Quality.

**Table 3-4: Performance and Data Storage**

Machine Specifications	HP DL360 Gen10	VMware/Microsoft Hyper-V – High Profile	VMware/Microsoft Hyper-V - Low Profile
OVOC Managed Devices	5,000	5,000	100
Maximum number of managed devices by OVOC (Device Manager Pro only).	10,000	<ul style="list-style-type: none"> <li>■ 30,000 (Device Manager only)<sup>1</sup></li> <li>■ 5,000 – including SBC/gateway management and monitoring</li> </ul>	1,000
RFC 6035 Quality Monitoring for OVOC Managed Devices			
Maximum Number of CAPS (calls attempts per second) per device.	160	120	30
Maximum number of CAPS per server (SBC and Skype for Business).	300	120	30
Maximum concurrent sessions	30,000	12,000	3,000
Maximum number of devices per region	500	300	100
Maximum number of managed devices.	3,000	1,200	100
Maximum number of links between devices.	6,000	2,400	200
Call Details Storage - Detailed information per Call	Up to one year or 80 million calls.	Up to one year or 80 million rows.	Up to one year or 6 million rows.
Calls Statistics Storage - Statistic information storage.	Up to one year or 150 million intervals.	Up to one year or 150 million rows.	Up to one year or 12 million rows.

<sup>1</sup>In normal operation (when devices are remotely managed) 30,000 devices send Keep-alive messages at five minute intervals; however, when managing devices behind a firewall or NAT using the Device Manager agent, a 10% factor (3,000 devices) is deducted for the allocation for these devices. In this case, 90% of the configuration (27,000) is checked every 15 minutes (for remotely managed devices) and 10% is checked every five minutes (for devices managed behind a firewall or NAT).

Machine Specifications	HP DL360 Gen10	VMware/Microsoft Hyper-V – High Profile	VMware/Microsoft Hyper-V - Low Profile
Performance Monitoring			
Maximum number of polled parameters per polling interval per OVOC managed device.	100,000	100,000	50,000
Maximum number of polled parameters per polling interval per OVOC server.	500,000	500,000	50,000
RFC 6035 Quality Monitoring for Endpoints			
Maximum number of CAPS	10	5	1
SIP Call Flow (for SBC calls only)			
Maximum Number of CAPS (calls attempts per second) per server.	100	25	6
Maximum number of stored calls with SIP Call Flow Data	Up to one year or one million calls.	Up to one year or one million calls.	Up to one year or one million calls.
Maximum number of devices	100	100	10
Capacity with SBC Floating License Capability			
Maximum Number of CAPS (calls attempts per second) per server with SIP Call Flow.	90	22	5
Maximum Number of CAPS (calls attempts per second) per server without SIP Call Flow.	270	108	27
Maximum number of devices supported with floating license.	1,000	500	100

## Skype for Business Monitoring SQL Server Prerequisites

The following are the Skype for Business Monitoring SQL Server prerequisites:

The server must be defined to accept login in 'Mix Authentication' mode.

- The server must be configured to collect calls before the OVOC can connect to it and retrieve Skype for Business calls.
- Call Detail Records (CDRs) and Quality of Experience (QoE) Data policies must be configured to capture data.
- Network administrators must be provisioned with the correct database permissions (refer to the *One Voice Operations Center User's Manual*).

- Excel macros must be enabled so that the SQL queries and reports can be run; tested with Excel 2010.
- Detailed minimum requirements for Skype for Business SQL Server can be found in the following link:

<http://technet.microsoft.com/en-us/library/gg412952.aspx>

## 4 OVOC Software Deliverables

This section describes the OVOC software deliverables.

### Dedicated Hardware Installation – DVDs 1-3

This section describes the DVDs supplied in the OVOC software delivery.

- **DVD1:** Operating System DVD for Linux ([OVOC Server Requirements](#) on page 7):
- **DVD2:** Oracle Installation: Oracle installation version 12.1.0.2 DVD for the Linux platform.
- **DVD3:** Software Installation and Documentation DVD for Linux:

The DVD 'SW Installation and Documentation' DVD comprises the following folders:

- 'EmsServerInstall' – OVOC server software, to install on the dedicated Linux based OVOC server machine.
- 'Private\_Labeling' folder – includes all the information required for the OEM to create a new private labeling DVD.
- Documentation – All documentation related to the present OVOC version. The documentation folder includes the following documents and sub-folders:
  - ◆ OVOC Release Notes Document – includes the list of the new features introduced in the current software version as well as version restrictions and limitations.
  - ◆ OVOC Server IOM Manual – Installation, Operation and Maintenance Guide.
  - ◆ OVOC Product Description Document
  - ◆ OVOC User's Manual Document
  - ◆ OVOC Integration with Northbound Interfaces

Installation files can also be downloaded from the Website by registered customers at <https://www.audiocodes.com/services-support/maintenance-and-support>.

### Virtual Appliance and Cloud Options

The OVOC DVD software delivery for the clean installation includes the following folders:

- Clean install
- Documentation

For Amazon Web Services, see [Installing OVOC Server on the Amazon Web Services \(AWS\) Platform](#) on page 16

For Microsoft Azure, see [Installing OVOC Server on the Microsoft Azure Platform](#) on page 22

### Virtual Machine and Cloud Deployments Upgrade Media

The Virtual Machine and Cloud deployments software delivery for upgrades (TAR file) and the documentation set are provided on DVD3 for the VMware, Hyper-V, Amazon Web Services and Microsoft Azure platforms.

Installation files can also be downloaded from the AudioCodes Website by registered customers at <https://www.audiocodes.com/services-support/maintenance-and-support>

# Part II

## OVOC Server Installation

This part describes the testing of the installation requirements and the installation of the OVOC server.

## 5 Installing OVOC Server on the Amazon Web Services (AWS) Platform

This section describes how to install the OVOC server on the AWS platform.



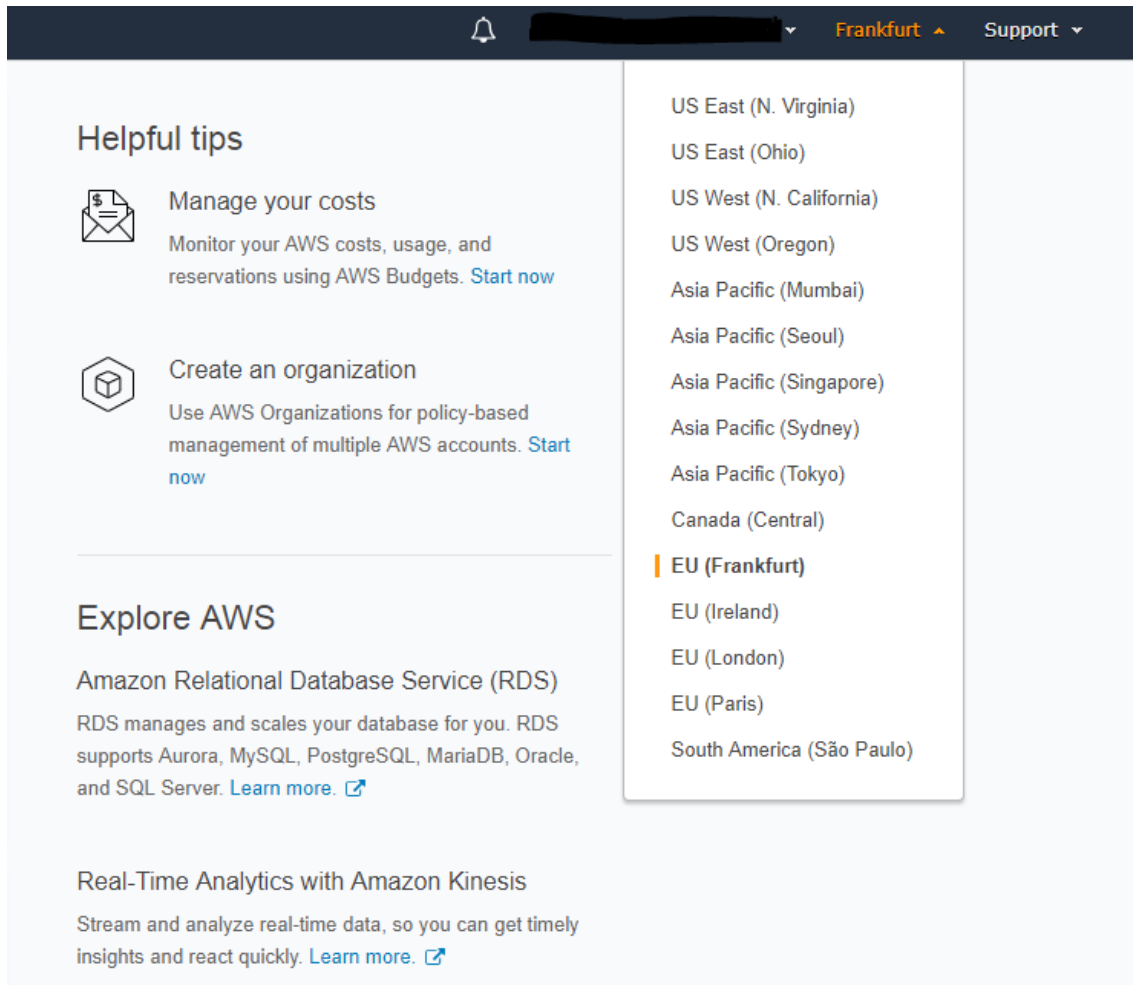
- Ensure that the minimum platform requirements are met (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the installation.
- You should verify the installation files (see [Files Verification](#) on page 72)

➤ **To install OVOC on the AWS platform:**

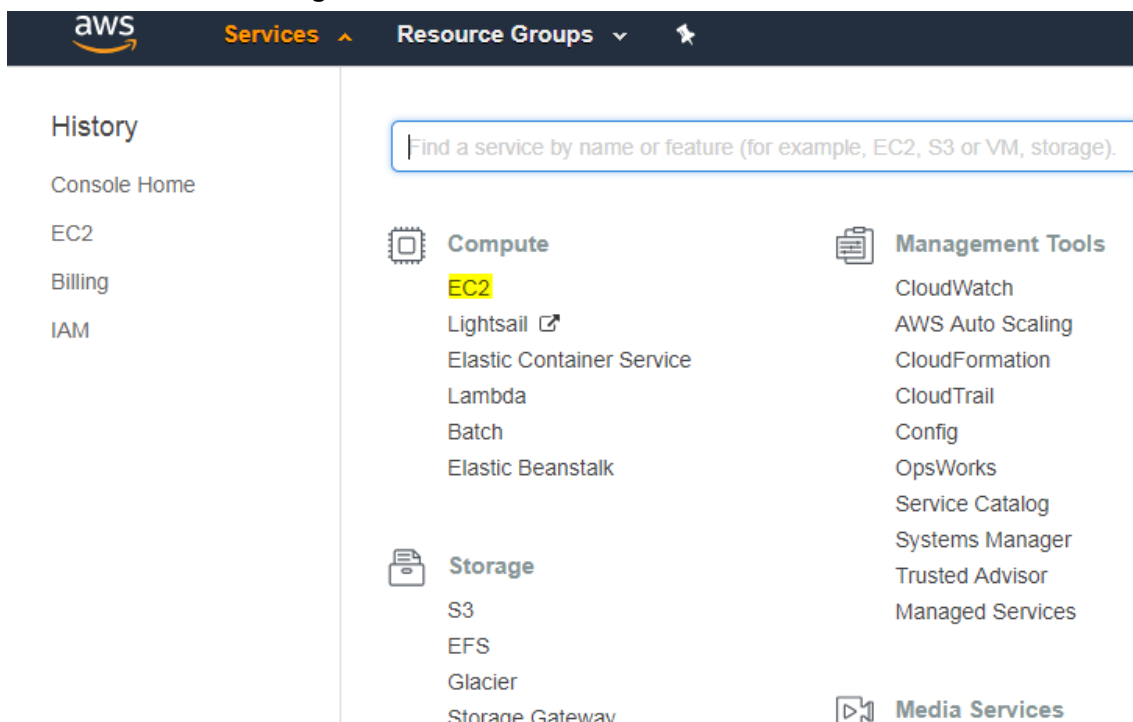
1. Log into your AWS account.
2. Choose one of the following regions:
  - us-west-1 (N. California)
  - us-west-2 (Oregon)
  - us-east-1 (N. Virginia)
  - eu-west-1 (Ireland)
  - eu-central-1 (Frankfurt)



For verifying AMI IDs, refer to <https://services.AudioCodes.com>.

**Figure 5-1: Select Region**

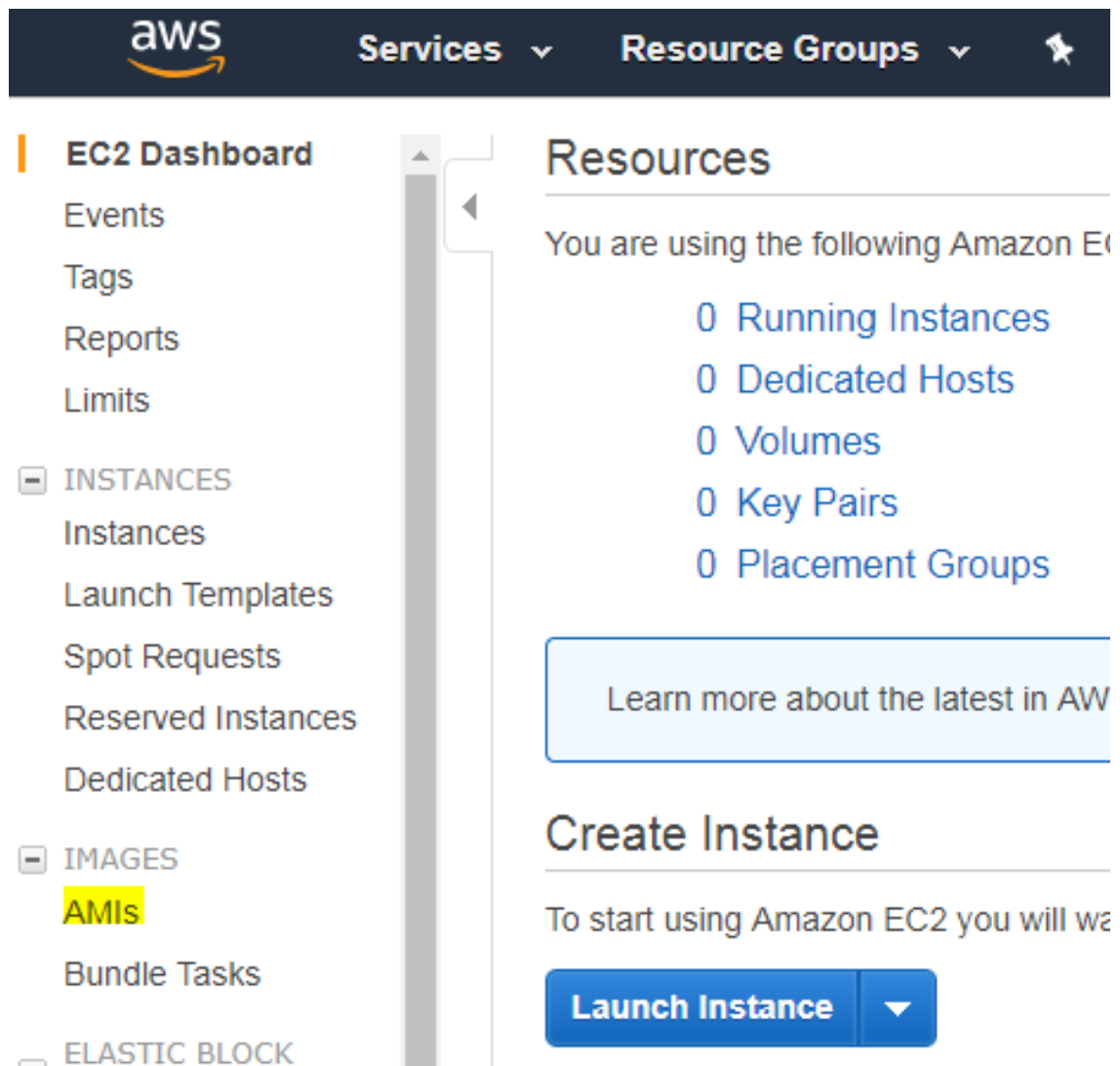
3. In the “Services” menu, choose EC2.

**Figure 5-2: Services Menu - EC2**

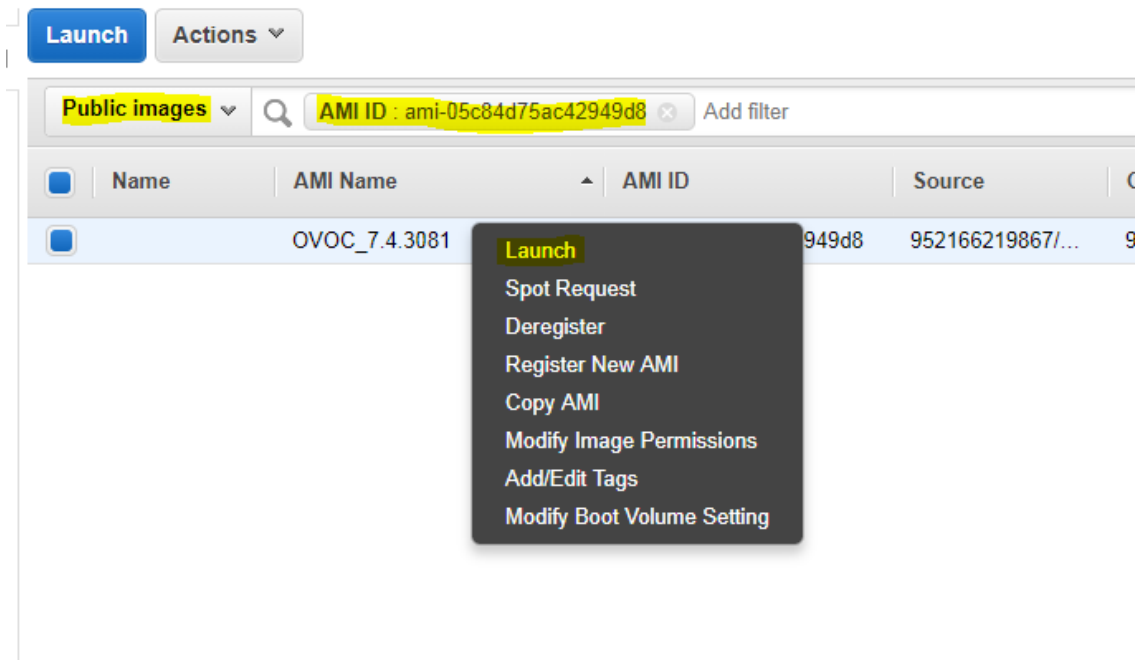
4. In the Dashboard, navigate to IMAGES > AMIs.



Figure 5-3: Images



5. In the search bar, choose Public images and apply the following filter:  
AMI ID : ami-000000000000 replacing ami-000000000000 with the AMI ID you received from AudioCodes according to the region you have chosen.
6. Right-click the AMI and choose Launch.

**Figure 5-4: Launch Public Images**

7. Choose an Instance type. We recommend General purpose or Compute optimized for heavier loads. The Minimum memory requirement for a virtual OVOC instance is 8GB.
8. Configure Instance (Optional). Using this option, you can edit network settings, for example, placement.
9. Configure Security Group. You should select an existing security group or create a new one according to OVOC firewall requirements (see Chapter [Configuring the Firewall](#) on page 167).
10. Click Review and Launch > Review > Launch.
11. In the dialog shown in the figure below, from the drop-down list, choose Proceed without a key pair, check the “I acknowledge ...” check box, then click Launch Instances.

**Figure 5-5: Select an Existing Key Pair**

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel
Launch Instances

12. Click View Instances and wait for the instance to change the state to “running” and the status checks to complete. In the description, note the Public IP address of the instance as highlighted in the figure below.

**Figure 5-6: Instance State and Status Checks**

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-0bed82bb94c0221a8	m4.xlarge	eu-central-1b	running	2/2 checks ...	None	ec2-35-156-251-238.eu...	35.156.251.238

Instance: i-0bed82bb94c0221a8		Public DNS: ec2-35-156-251-238.eu-central-1.compute.amazonaws.com	
Description	Status Checks	Monitoring	Tags
Instance ID	i-0bed82bb94c0221a8	Public DNS (IPv4)	ec2-35-156-251-238.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	35.156.251.238
Instance type	m4.xlarge	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-43-55.eu-central-1.compute.internal
Availability zone	eu-central-1b	Private IPs	172.31.43.55
Security groups	ovoc, view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-9044cbfb
AMI ID	OVOC_7.4.3081 (ami-05c84d75ac42949d8)	Subnet ID	subnet-a66befdb
Platform	-	Network interfaces	eth0

13. Login into the OVOC server by SSH, as 'acems' user and enter password acems.

14. Switch to 'root' user and provide root password (default password is root):

```
su - root
```

**Figure 5-7: Login to OVOC server**

```

root@OVOC-AWS1:~
markk@IL-MARKK-PC ~
$ ssh acems@35.156.251.238
acems@35.156.251.238's password:
Last login: Thu May 24 09:27:17 2018 from 37.142.12.66
[acems@OVOC-AWS1 ~]$ su -
Password:
Last login: Thu May 24 09:27:22 BST 2018 on pts/0
[root@OVOC-AWS1 ~]#

```

15. Type the following command:

```
# EmsServerManager
```

16. In the OVOC Server Manager, change the following default passwords:

- acems OS user (see [OS Users Passwords](#) on page 142)
- root OS user (see [OS Users Passwords](#) on page 142)



Unless you have made special configurations, the AWS instance is in the public cloud and therefore is accessible over the Internet. Consequently, it is highly recommended to change these default passwords to mitigate against security risks.

17. Load OVOC license (see [License](#) on page 112 ).
18. From the Network Configuration menu, choose **NAT**, and then press Enter.
19. Set the OVOC Server's **Public IP address**.
20. Type **y** to confirm the changes.



This step is necessary when SBC devices are deployed outside the cloud. In this case, Single Sign-on to the SBC devices is not supported from OVOC.

21. Stop and start the OVOC server for the changes to take effect.

## 6 Installing OVOC Server on the Microsoft Azure Platform

This chapter describes how to install OVOC on the Microsoft Azure platform from the Microsoft Azure Marketplace.

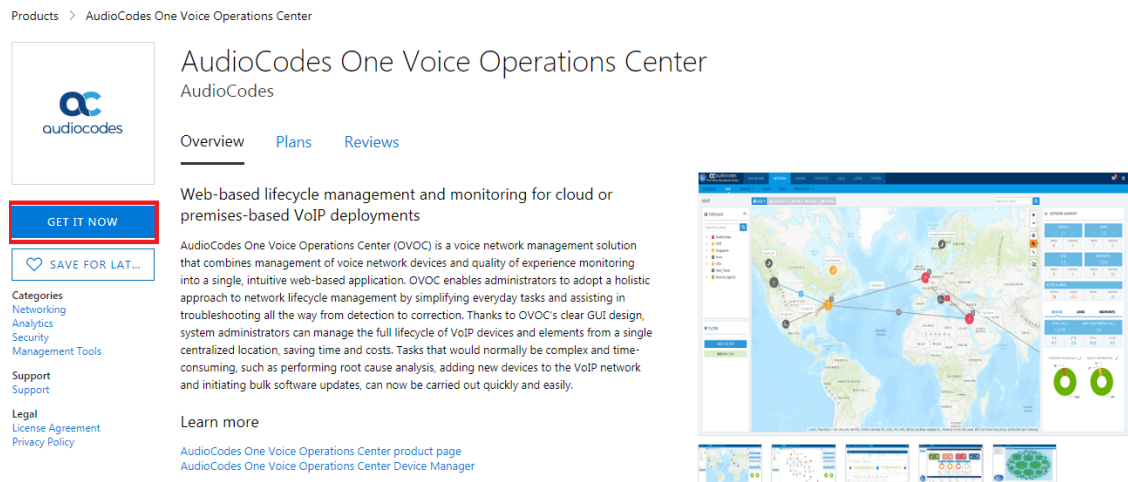


- Ensure that the minimum platform requirements are met (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the installation.
- You should verify the installation files (see [Files Verification](#) on page 72)

### ➤ To install OVOC from the Microsoft Azure Marketplace:

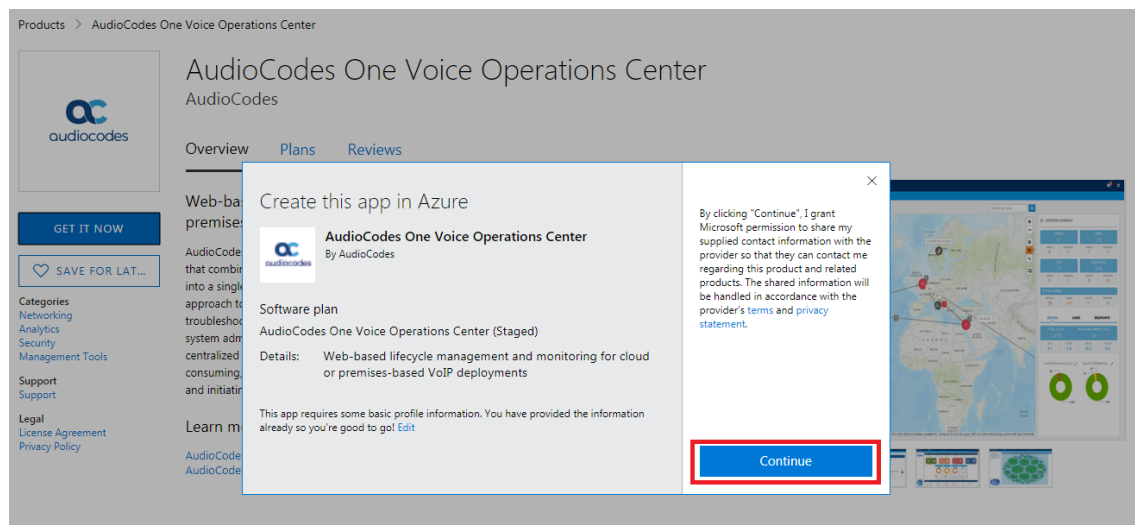
1. In the Azure Marketplace, search for "AudioCodes One Voice Operations Center (OVOC)" and click **Get It Now**.

**Figure 6-1: Get it Now**

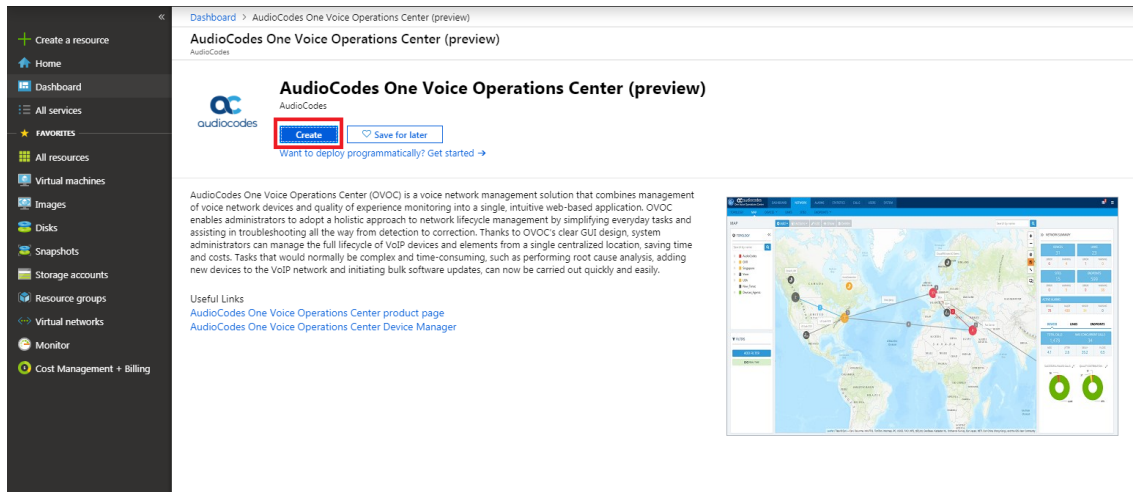


2. Click **Continue**.

**Figure 6-2: Create this App in Azure**



3. You are now logged in to the Azure portal; click **Create**.

**Figure 6-3: Create Virtual Machine**

4. Configure the following:
  - a. Choose your Subscription.
  - b. Choose your Resource Group or create a new one
  - c. Enter the name of the new Virtual Machine.
  - d. Choose the Region.
  - e. Choose the VM Size (F16s is the VM size that is recommended for High performance).
  - f. Choose Authentication Type "Password" and enter username "acovoc" and user-defined password. This user is used for accessing the OVOC server via SSH.

**Figure 6-4: Virtual Machine Details**

Microsoft Azure

Dashboard > AudioCodes One Voice Operations Center (preview) > Create a virtual machine

### Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

**PROJECT DETAILS**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

\* Subscription

\* Resource group  [Create new](#)

**INSTANCE DETAILS**

\* Virtual machine name

\* Region

Availability options

\* Image  [Browse all images](#)

\* Size  16 vcpus, 32 GB memory [Change size](#)

**ADMINISTRATOR ACCOUNT**

Authentication type ☒ Password ☐ SSH public key

\* Username

\* Password

\* Confirm password

[Review + create](#) [Previous](#) [Next : Disks >](#)

5. Click **Next** until **Networking** section to configure the network settings, including the Private and Public IP addresses and Firewall rules (Network Security Group). By default, only ports 22 and 443 are open for inbound traffic (open other ports for managing devices behind a NAT (outside the Azure environment) as required). For more information, see [Managing Devices Behind an Enterprise Firewall or NAT](#) on page 27

**Figure 6-5: Network Settings**

Microsoft Azure

Dashboard > AudioCodes One Voice Operations Center (preview) > Create a virtual machine

### Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

**NETWORK INTERFACE**

When creating a virtual machine, a network interface will be created for you.

**CONFIGURE VIRTUAL NETWORKS**

\* Virtual network AUDCvnet295 [Create new](#)

\* Subnet default (10.0.7.0/24) [Manage subnet configuration](#)

Public IP (new) OVOC-7-6-1000-ip [Create new](#)

NIC network security group ☐ None ☐ Basic ☒ Advanced

This VM image has preconfigured NSG rules

\* Configure network security group (new) OVOC-7-6-1000-nsg [Create new](#)

Accelerated networking ☐ On ☒ Off

The selected image does not support accelerated networking.

**LOAD BALANCING**

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐ Yes ☒ No

[Review + create](#) [Previous](#) [Next : Management >](#)

6. Click Next until **Review+Create** tab, make sure all the settings are correct and click **Create**.



Figure 6-6: Review and Create

Microsoft Azure

Dashboard > AudioCodes One Voice Operations Center (preview) > Create a virtual machine

### Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Advanced Tags **Review + create**

**PRODUCT DETAILS**

AudioCodes One Voice Operations Center  
by AudioCodes  
[Terms of use](#) | [Privacy policy](#)

Standard F16s  
by Microsoft  
[Terms of use](#) | [Privacy policy](#)

**TERMS**

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; and (b) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name: Mark Kemel

\* Preferred e-mail address: Mark.Kemel@audiocodes.com ✓ Match found.

\* Preferred phone number: +97239764373 ✓

**BASICS**

Subscription: Newwave AZURE LAB

Resource group: AUDC

Virtual machine name: OVOC-7-6-1000

Region: West Europe

Availability options: No infrastructure redundancy required

Authentication type: Password

Username: acovoc

**DISKS**

OS disk type: Premium SSD

Use managed disks: Yes

**NETWORKING**

Virtual network: AUDCnet295

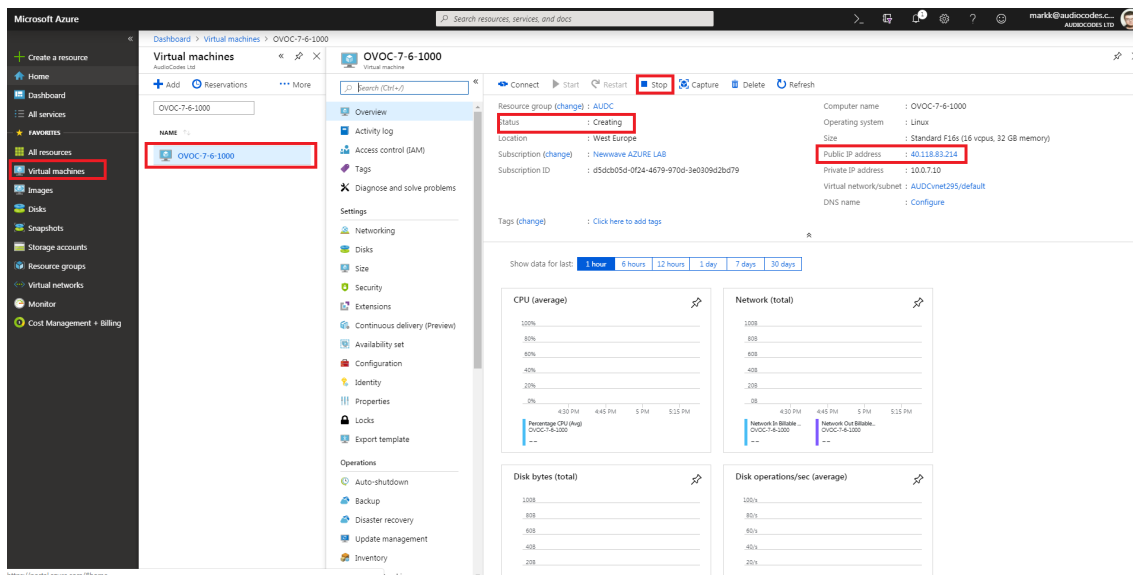
**Create** Previous Next Download a template for automation

7. Navigate to the "Virtual machines" section, where you can, for example, monitor the Virtual Machine creation process and find the Public IP address to access the Virtual Machine.



After the Deployment process has completed, the Virtual Machine may not be accessible via SSH for the configured IP address, or its status may appear as hanging in the "Creating" state for a long time. Consequently, you should **stop** the Virtual Machine and **restart**, after which time it should be accessible.

Figure 6-7: Azure Deployment Process Complete



## Managing Devices Behind an Enterprise Firewall or NAT

If you are managing devices behind an Enterprise firewall or NAT in a remote enterprise network (deployed remotely outside of the Microsoft Azure Network), then these devices should be deployed using the following methods:

- **OVOC Managed Devices:** Automatically with full automatic detection. Refer to Section "Adding AudioCodes Devices Automatically" in the OVOC User's Manual.
- **Device Manager Managed Devices (AudioCodes and Jabra devices):** Using the Device Manager Agent which is deployed locally in the enterprise network. The Agent application enables secured two-way communication between OVOC and devices. Refer to Device Manager Agent Installation and Configuration Guide. .



Firewall rules should be configured in the remote Enterprise network to open the following ports:

- SNMP UDP port 1161 used for listening to incoming Keep-alive messages from OVOC Managed devices.
- HTTPS Port 443 used for listening to incoming Keep-alive messages from Device Manager Managed devices in the Device Manager Agent deployment.

## Configuring OVOC as the Email Server on Microsoft Azure

This section describes how to configure OVOC to forward alarms by email on Microsoft Azure. These steps are necessary in order to overcome Microsoft Azure security restrictions for sending emails outside of the Microsoft Azure domain. The following options can be configured:

- [Configuring OVOC to Forward Alarms by Email on Microsoft Azure using Microsoft Office 365 below](#)
- [Configuring OVOC as Email Server on Microsoft Azure using SMTP Relay on the next page](#)

### Configuring OVOC to Forward Alarms by Email on Microsoft Azure using Microsoft Office 365

This section describes how to configure OVOC to forward alarms by email on Microsoft Azure through the configuration of a user account on the Microsoft Office 365 platform. Replace OFFICE365\_USERNAME and PASSWORD with an existing customer's Office 365 username and password.



The Office 365 user name is not necessarily the email address.

#### ➤ Do the following:

1. Configure the Exim service on the OVOC server:
  - a. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
  - b. Switch to 'root' user and provide root password (default password is root):

```
su - root
```

- c. Backup the exim configuration file:

```
cp /etc/exim/exim.conf /etc/exim/exim.conf.bak
```

- d. Edit the exim configuration file:

```
vim /etc/exim/exim.conf
```

- e. After the line "begin routers:" add the following configuration:

```
begin routers
send_via_outlook:
  driver = manualroute
  domains = ! +local_domains
  transport = outlook_smtp
  route_list = "*" smtp.office365.com::587 byname"
  host_find_failed = defer
  no_more
```

- f. After the line "begin transports", add the following configuration:

```
begin transports
outlook_smtp:
  driver = smtp
  hosts = smtp.office365.com
  hosts_require_auth = <; $host_address
  hosts_require_tls = <; $host_address
```

- g. After the line "begin authenticators", replace Username and Password with your Office 365 username and password:

```
begin authenticators
outlook_login:
  driver = plaintext
  public_name = LOGIN
  client_send = : OFFICE365_USERNAME : PASSWORD
```

- h. Restart the exim service:

```
systemctl restart exim
```



If following the restart, the alarm forwarding is still not working, edit `/root/.muttrc`, and replace the default email address `set from = OVOC@audiocodes.com` with the proper email address of the owner of the `OFFICE365_USERNAME` account, because the Outlook SMTP server may block this default address if it verifies that the sender email does not match the specified mailbox user name.

## Configuring OVOC as Email Server on Microsoft Azure using SMTP Relay

This section describes how to configure OVOC to forward alarms by email on Microsoft Azure using SMTP Relay. This setup is recommended by Microsoft, and SendGrid is one of the available

options. SendGrid service can be easily configured in the Azure Portal and in addition, includes a free tier subscription, supporting up to 25,000 emails per month.

➤ **Do the following:**

1. Create SendGrid service on the Azure platform:
  - a. Open [portal.azure.com](https://portal.azure.com)
  - b. Go to "SendGrid Accounts" section, ( via Search or in "All services" section).
  - c. Click **Add**.
  - d. Fill in the following fields:
    - ◆ Name: Choose a name
    - ◆ Password
    - ◆ Subscription
    - ◆ Resource Group (create a new one or choose existing)
    - ◆ Pricing tier: choose Free or one of the other plans
    - ◆ Contact Information
    - ◆ Read legal terms
  - e. Click **Create**.
  - f. Wait for the service to be created.
  - g. Go back to "SendGrid Accounts", click on the new account name
  - h. Click the "Configurations" section in the **Settings** tab.
  - i. Copy the Username – it will be used in the next step along with the password (format `azure_xxxxxxxx@azure.com`)
2. Configure the Exim service on the OVOC server:
  - a. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
  - b. Switch to 'root' user and provide root password (default password is root):

```
su - root
```

- c. Backup the exim configuration file:

```
cp /etc/exim/exim.conf /etc/exim/exim.conf.bak
```

- d. Edit the exim configuration file:

```
vim /etc/exim/exim.conf
```

- e. After the line "begin transports", add the following configuration:

```
begin transports
sendgrid_smtp:
  driver = smtp
  hosts = smtp.sendgrid.net
  hosts_require_auth = <; $host_address
  hosts_require_tls = <; $host_address
```

- f. After the line "begin routers", add the following configuration:

```
begin routers
send_via_sendgrid:
  driver = manualroute
  domains = ! +local_domains
  transport = sendgrid_smtp
  route_list = "*" smtp.sendgrid.net::587 byname"
  host_find_failed = defer
  no_more
```

- g. After the line "begin authenticators", add the following configuration, replacing Username and Password with your SendGrid User/Pass:

```
begin authenticators
sendgrid_login:
  driver = plaintext
  public_name = LOGIN
  client_send = : Username : Password
```

- h. Save the file and exit back to the command line.  
i. Restart the Exim service.

```
systemctl restart exim
```

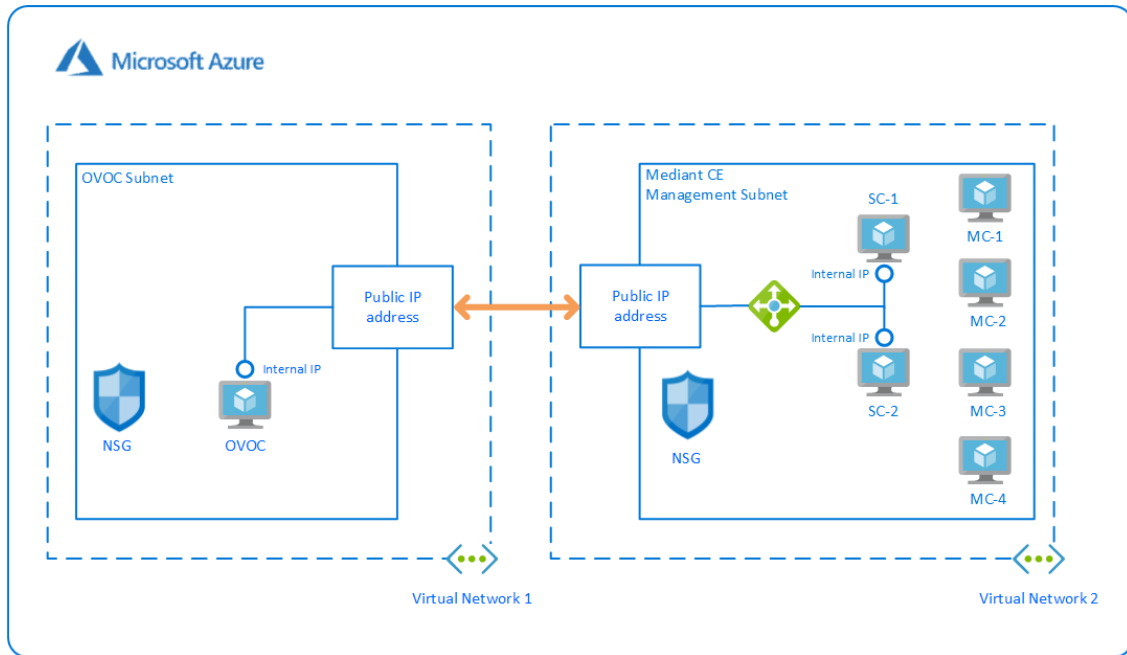
- j. Check that the alarm forwarding by email functions correctly.



You can access the SendGrid Web interface using the same username/password, where among other features you can find an Activity log, which may be useful for verifying issues such as when emails are sent correctly; however, are blocked by a destination email server.

## Connecting Mediant Cloud Edition (CE) SBC Devices in Azure Deployment

This section describes the procedure for establishing a secure connection between the OVOC server which is installed in the Azure Cloud and Mediant Cloud Edition (CE) SBC devices which are also deployed in the Azure Cloud. The figure below illustrates this topology. Note that communication between OVOC and Mediant CE SBC devices is carried over the public IP addresses on both sides, requiring NAT translation from internal to public IP addresses. The Mediant CE SBC devices must be added to OVOC using Automatic Detection.

**Figure 6-8: Microsoft Azure Topology**

This procedure includes the following steps:

- [Step 1: Configuring the OVOC Virtual Machine on Azure Cloud](#) below
- [Step 2: Configuring the OVOC Server \(EMS Server Manager\) on Azure Cloud](#) on the next page
- [Step 3: Configuring Mediant Cloud Edition \(CE\) Device](#) on the next page

## Step 1: Configuring the OVOC Virtual Machine on Azure Cloud

This section describes how to configure the inbound port rules for the OVOC virtual machine deployed in the Azure Cloud.

### ➤ To configure the OVOC Virtual Machine on the Azure platform:

1. Open the Azure portal (<http://portal.azure.com>)
2. Navigate to Virtual Machines screen.
3. Locate the OVOC virtual machine.
4. In the Networking screen, configure the following inbound port rules (for **Network Security**):

Protocol	Port	Description
UDP	162	SNMP trap listening port on the OVOC server.
UDP	1161	Keep-alive - SNMP trap listening port on the OVOC server used for NAT traversal.
TCP	5000	Communication for control, media data reports and SIP call flow messages sent from Mediant Cloud Edition (CE) SBC.
TCP (TLS)	5001	TLS secured communication for control, media data reports and SIP call flow messages sent from Mediant Cloud Edition (CE) SBC.
NTP	123	NTP server port (configure the OVOC server's Public IP address as the NTP server-see <a href="#">Step 2: Configuring the OVOC Server (EMS Server Manager) on Azure Cloud</a> on the next page)

The screen below shows an example of the configured Security Group.

**Figure 6-9: OVOC Network Security Group**

Inbound port rules   Outbound port rules   Application security groups   Load balancing						
Network security group qa-evgenyz-OVOC-External-vm-nsg (attached to network interface: qa-evgenyz-ovoc-exte52) Impacts 0 subnets, 1 network interfaces						
Priority	Name	Port	Protocol	Source	Destination	Action
1000	HTTP	80	Any	Any	Any	Allow
1010	HTTPS	443	TCP	Any	Any	Allow
1020	SSH	22	TCP	Any	Any	Allow
1030	snmp-162	161-162	UDP	Any	Any	Allow
1040	snmp-1161	1161	UDP	Any	Any	Allow
1050	VQM-TCP	5000	TCP	Any	Any	Allow
1060	VQM-TLS	5001	Any	Any	Any	Allow
1070	NTP	123	Any	Any	Any	Allow
1080	OVOC-HTTPS-Additional	9400	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

## Step 2: Configuring the OVOC Server (EMS Server Manager) on Azure Cloud

This section describes how to configure the OVOC Server's Public IP address as the OVOC NAT IP address for the OVOC virtual machine deployed in the Azure Cloud.

### ➤ To configure the OVOC Server's NAT:

1. Login to the EMS Server Manager (see [Connecting to the OVOC Server Manager](#) on page 101).
2. From the Network Configuration menu, choose **NAT**, and then press Enter.
3. Set the OVOC Server's **Public IP address**.
4. Type **y** to confirm the changes.
5. Stop and start the OVOC server for the changes to take effect.

## Step 3: Configuring Mediant Cloud Edition (CE) Device

This step describes how the configure actions required on the Mediant CE to connect to the OVOC server that is deployed in the Azure Cloud.

- Configure the SNMP connection between the Mediant CE and the OVOC Server using the Stack Manager ([Step 3-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager](#) below)
- Configure Mediant CE and OVOC communication settings using the Mediant CE Web interface ([Step 3-2: Configuring Mediant CE OVOC Communication Settings using Web Interface](#) on the next page)

### Step 3-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager

This step describes how to configure the SNMP communication between the OVOC server deployed in the Azure Cloud and the Mediant CE using the Stack Manager.

### ➤ To configure the Stack Manager:

1. Login to the Web interface of the Stack Manager that was used to create Mediant Cloud Edition (CE) SBC. Refer to *Stack Manager for Mediant CE SBC User's Manual*.
2. Click the "Mediant CE stack".
3. Click the **Modify** button and append 161/udp port (for SNMP traffic) to "Management Ports" parameter.
4. Click **Update** to apply the new configuration.

**Figure 6-10: Modify Stack**

**Modify stack**

Automatic scaling  
scale-out step: 1

**Signaling Components**

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Management Ports: 22/tcp,80/tcp,443/tcp,161/udp

Signaling Ports: 5060/udp,5060/tcp,5061/tcp

**Media Components**

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

**Network Subnets**

Signaling 1 subnet:

Modify Cancel

### Step 3-2: Configuring Mediant CE OVOC Communication Settings using Web Interface

This section describes how to configure the communication settings between the Mediant CE device and the OVOC server deployed in the Azure Cloud.

➤ **To configure the Mediant Cloud Edition (CE) SBC for Azure:**

1. Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
2. Open the Quality of Experience Settings screen (**Setup** Menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience** > **Quality of ExperienceSettings**).
3. Click **Edit** and configure the **Keep-Alive Time Interval** to 1.
4. Click **Apply** to apply the changes.
5. Open the TIME & DATE page (**Setup** menu > **Administration** tab ) and set the OVOC server Public IP address (for the Microsoft Azure site where the OVOC server is installed) as the NTP server.



Configure the same OVOC Public IP address as the NAT IP address in the EMS Server Manager (see below).

6. Click **Apply** to apply the changes.
7. Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPAddress/AdminPage) and configure the following ini parameters:



```
SendKeepAliveTrap = 1  
KeepAliveTrapPort = 1161
```

8. Reset the device for your settings to take effect (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

## 7 Installing OVOC Server on the Microsoft Hyper-V Virtual Machine

The Microsoft Hyper-V Virtual Machine installation package is provided on **DVD 5** ([Virtual Appliance and Cloud Options](#) on page 14).

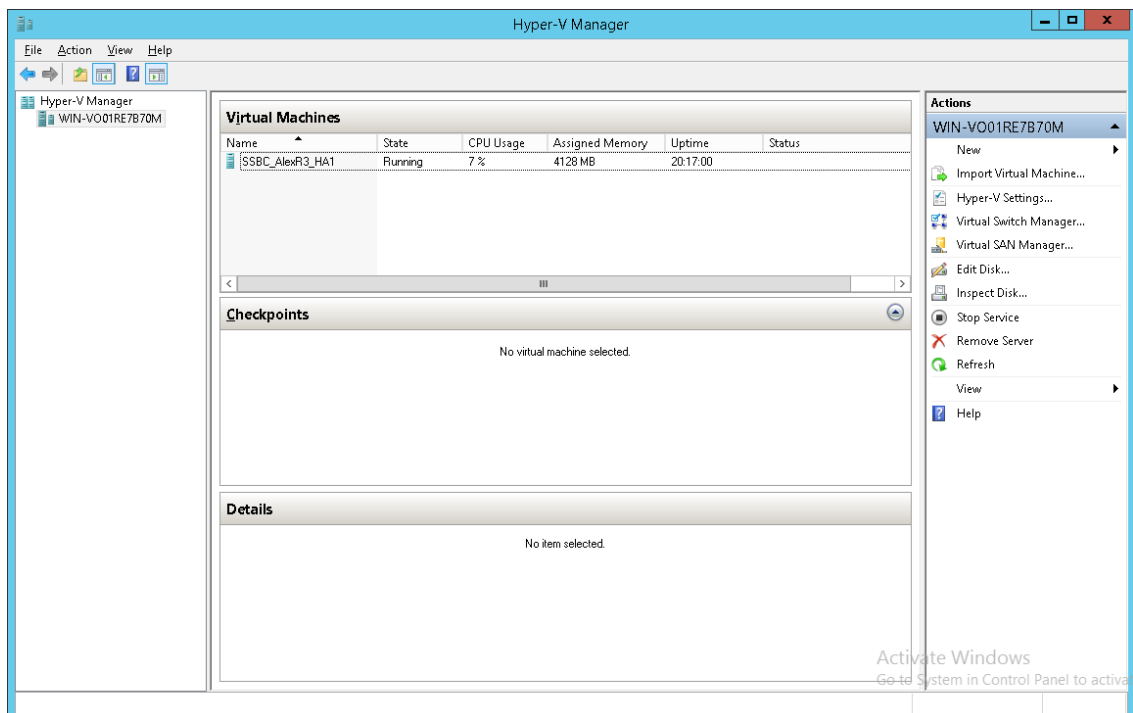


- The OVOC server supports the VMware vSphere High Availability (HA) feature.
- Ensure that the minimum platform requirements are met (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the installation.
- For obtaining the installation files, see [OVOC Software Deliverables](#) on page 14. Note that you should also verify these files (see [Files Verification](#) on page 72)

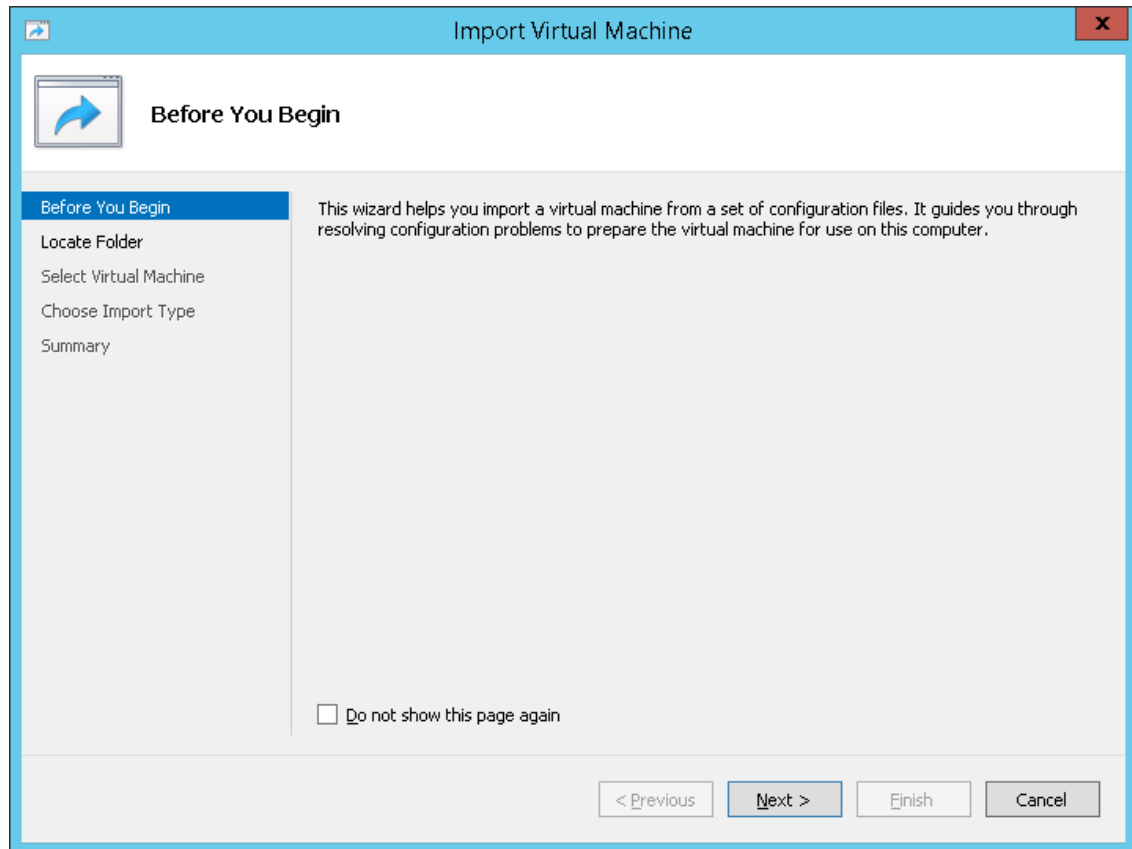
### ➤ To install the OVOC server on Microsoft Hyper-V:

1. Transfer the ZIP file containing the Microsoft Hyper-V Virtual Machine installation package from the AudioCodes **DVD 5** to your PC (see Appendix [Transferring Files](#) on page 200 for instructions on how to transfer files).
2. Open Hyper-V Manager by clicking **Start > Administrative Tools > Hyper-V Manager**; the following screen opens:

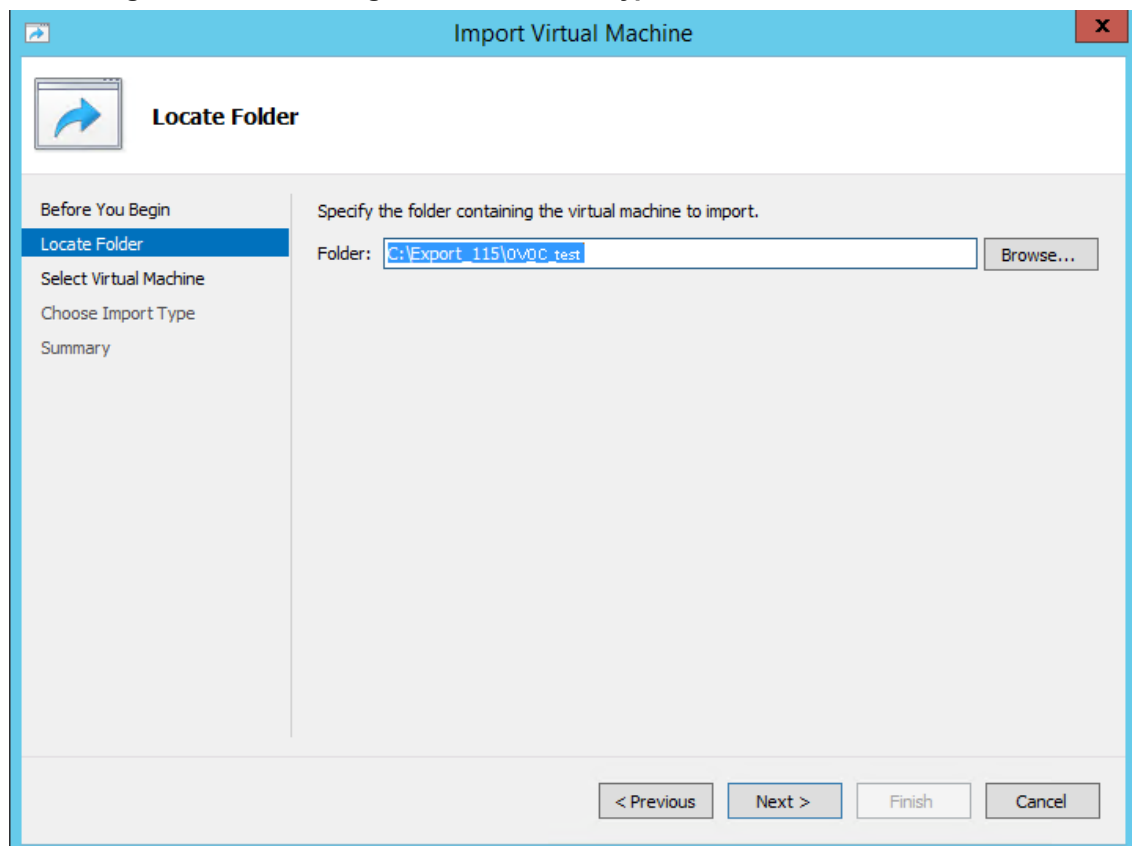
**Figure 7-1: Installing the OVOC server on Hyper-V – Hyper-V Manager**



3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

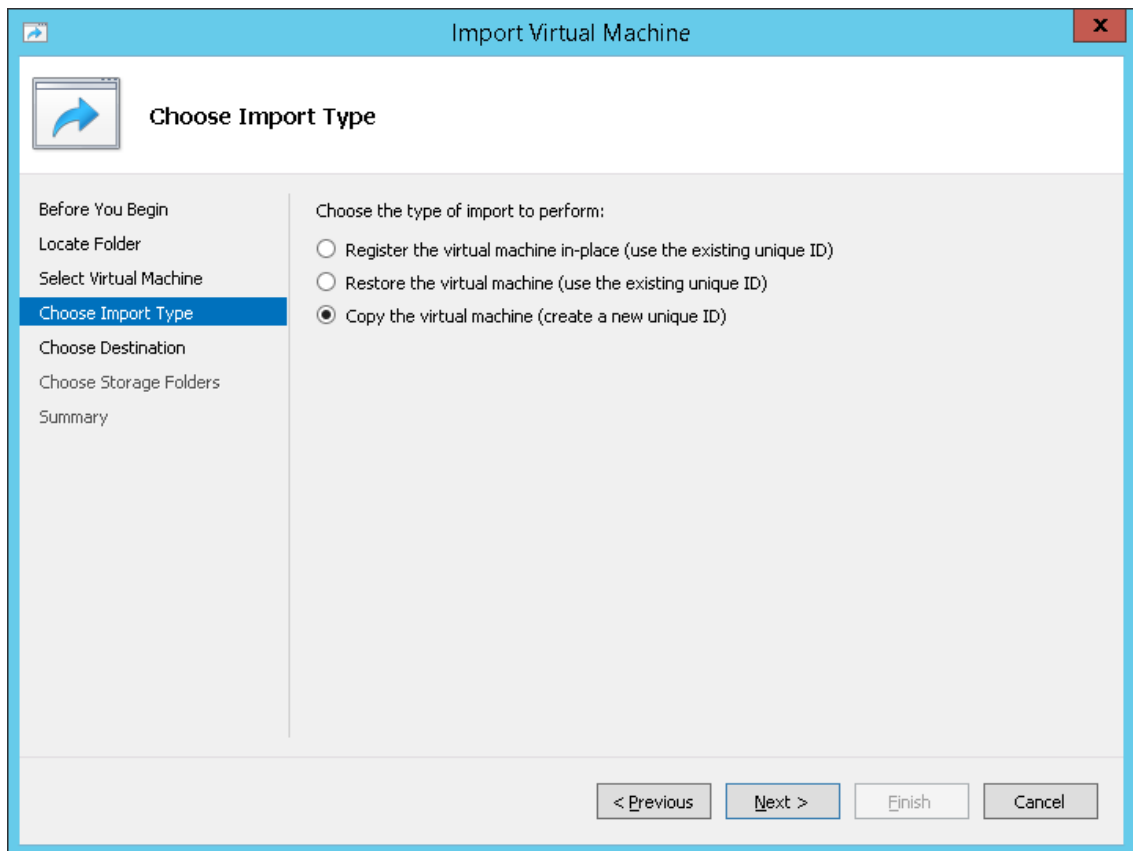
**Figure 7-2: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard**

4. Click **Next**; the Locate Folder screen opens:

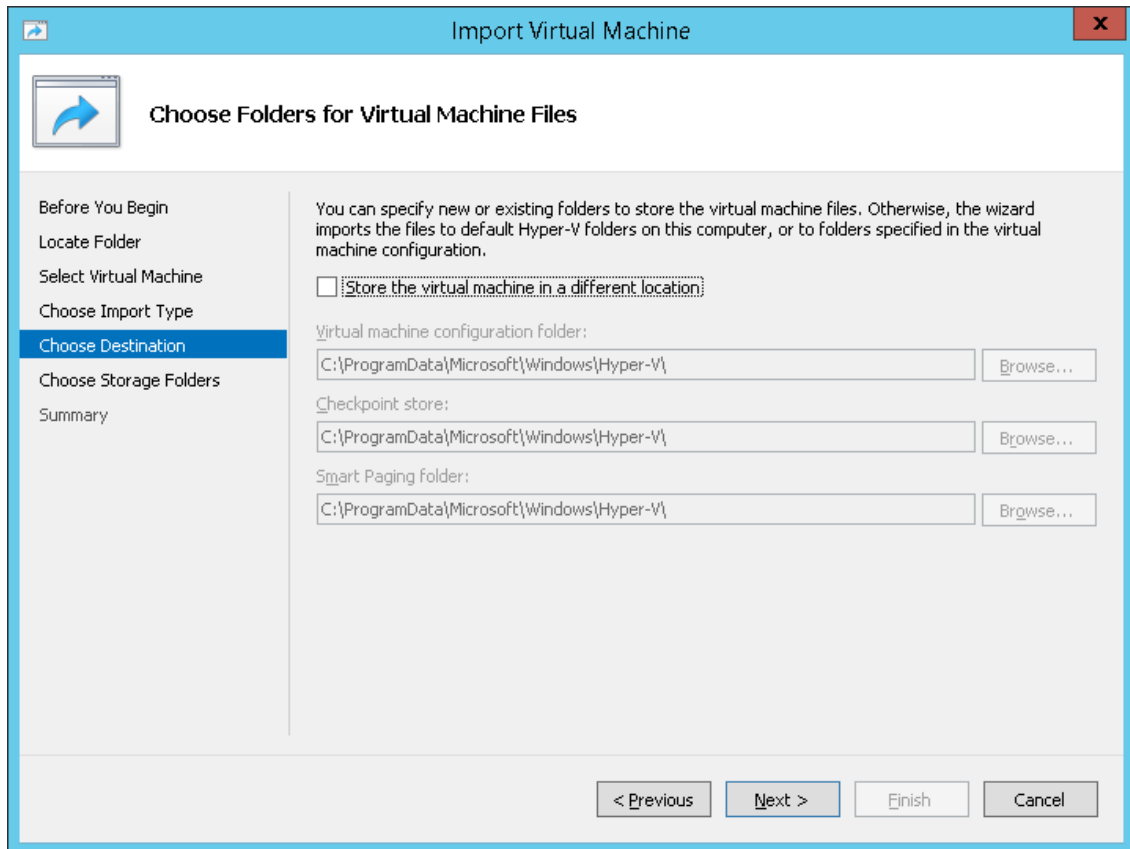
**Figure 7-3: Installing OVOC server on Hyper-V – Locate Folder**

5. Enter the location of the VM installation folder (extracted from the zip file), and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

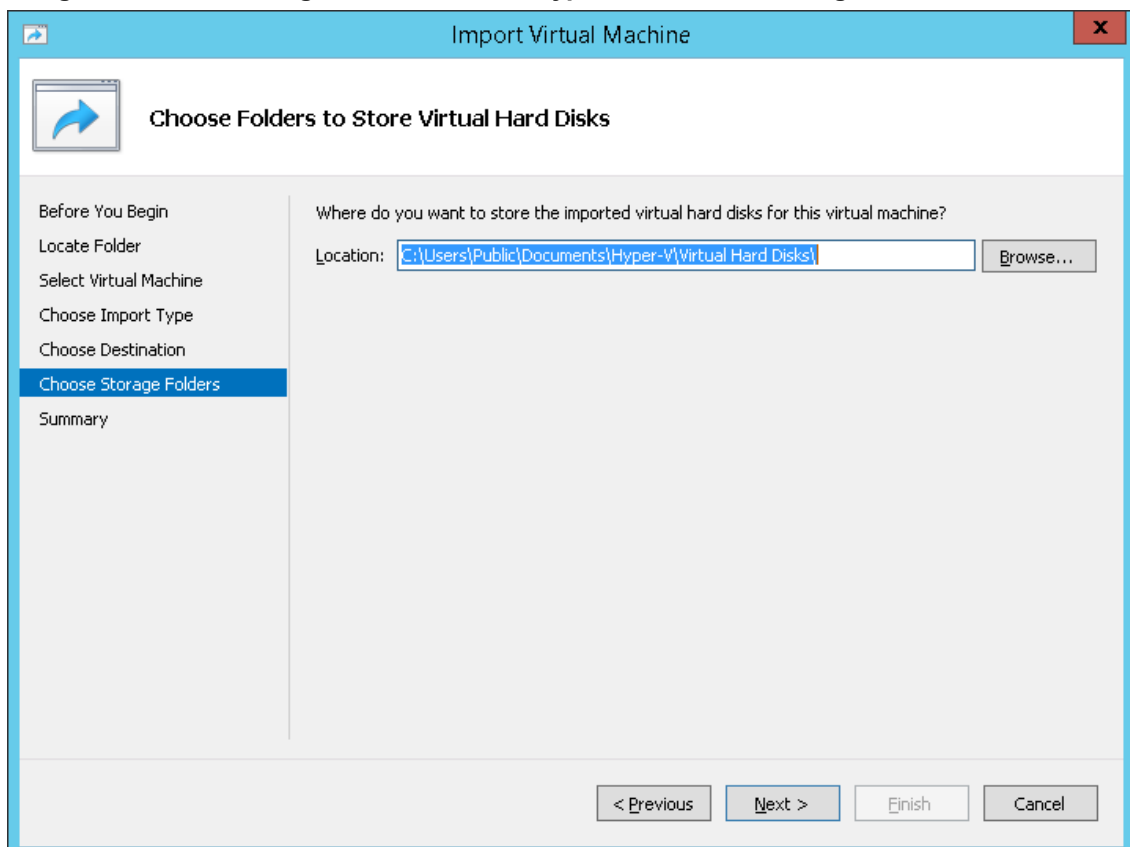
**Figure 7-4: Installing OVOC server on Hyper-V – Choose Import Type**



7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

**Figure 7-5: Installing OVOC server on Hyper-V – Choose Destination**

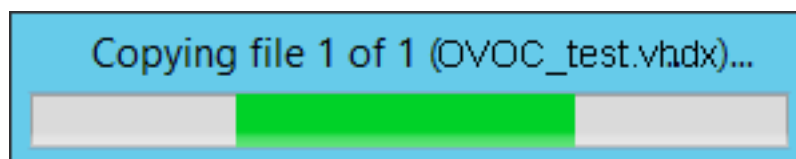
8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

**Figure 7-6: Installing OVOC server on Hyper-V – Choose Storage Folders**

9. Select the Storage Folder for the Virtual Hard Disk, and then click **Next**; the Summary screen opens.
10. Click **Finish** to start the creation of the VM; a similar installation progress indicator is shown:

**Figure 7-7: File Copy Progress Bar**

This process may take approximately 30 minutes to complete.



11. Proceed to [Configuring the Virtual Machine Hardware Settings](#) below.

## Configuring the Virtual Machine Hardware Settings

This section shows how to configure the Virtual Machine's hardware settings.

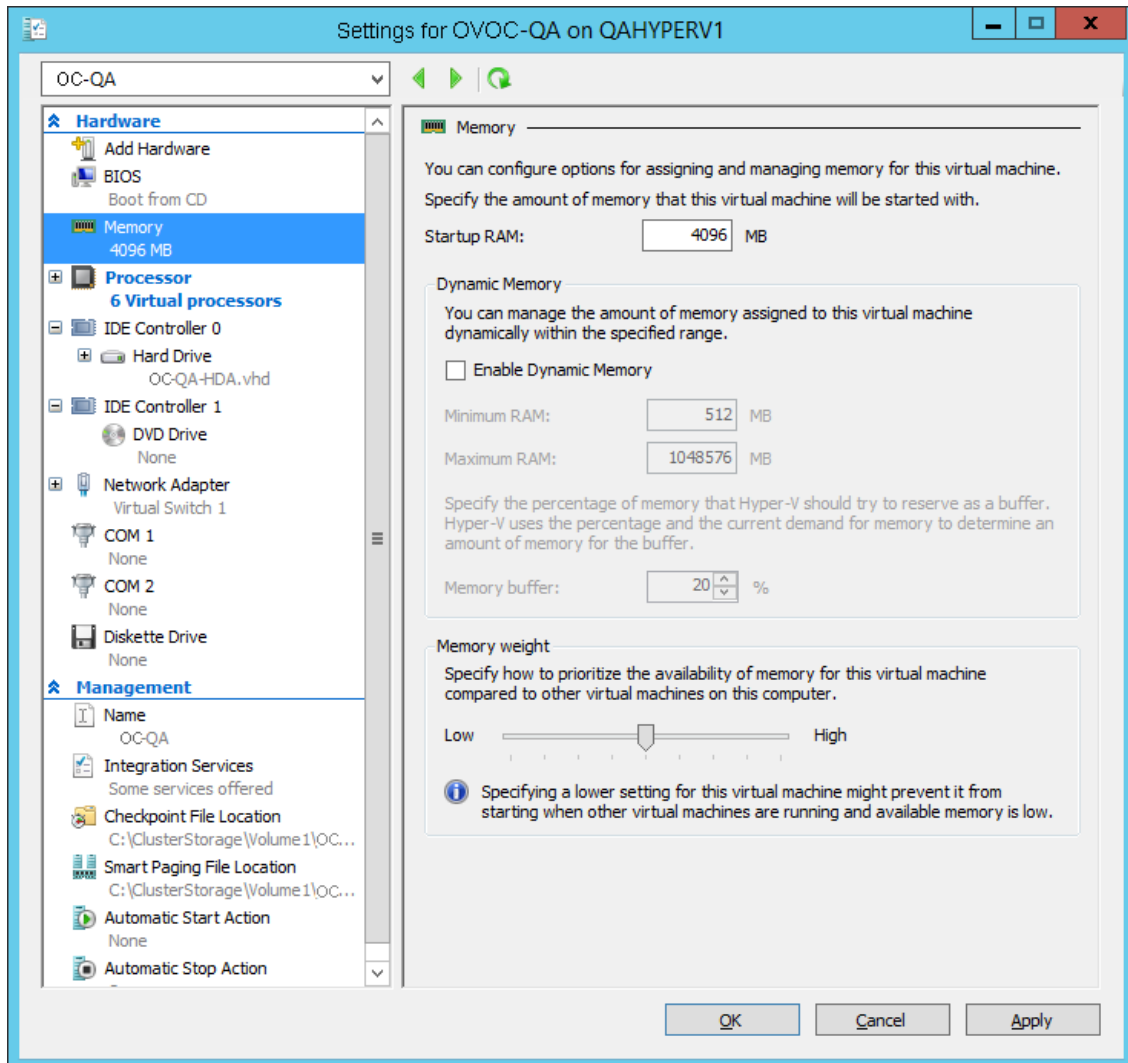
Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see [Hardware and Software Specifications](#) on page 7.

**Table 7-1: Virtual Machine Configuration**

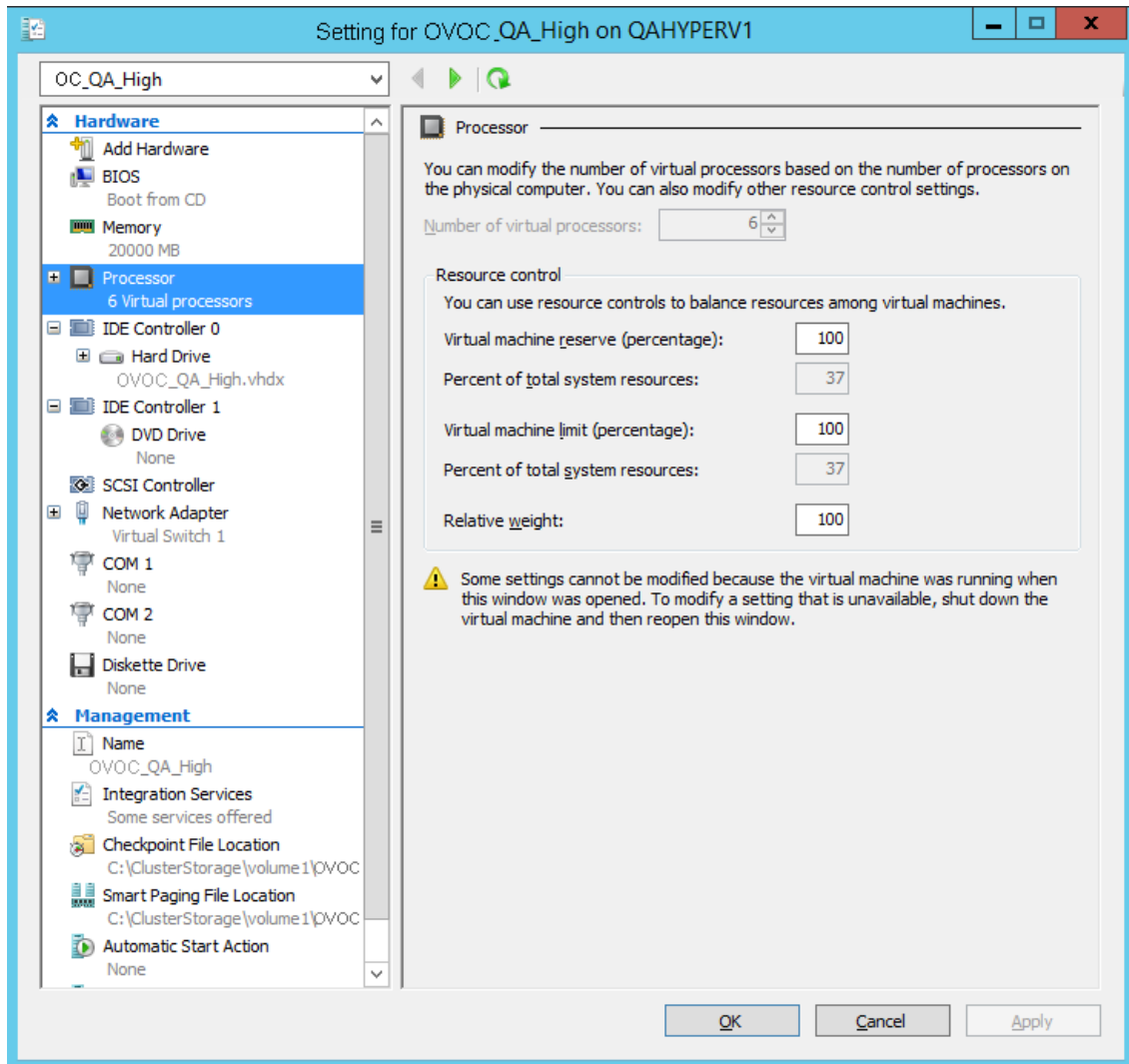
Required Parameter	Value
Disk size	
Memory size	
CPU cores	

### ➤ To configure the VM for OVOC server:

1. Locate the new OVOC server VM in the tree in the Hyper-V Manager, right-click it, and then select **Settings**; the Virtual Machine Settings screen opens:

**Figure 7-8: Adjusting VM for OVOC server – Settings - Memory**

2. In the Hardware pane, select **Memory**, as shown above, enter the 'Startup RAM' parameter as required, and then click **Apply**.
3. In the Hardware pane, select **Processor**; the Processor screen shown in the figure below opens.

**Figure 7-9: Adjusting VM for OVOC server - Settings - Processor**

4. Set the 'Number of virtual processors' parameters as required.
5. Set the 'Virtual machine reserve (percentage)' parameter to **100%**, and then click **Apply**.
  - Once the hard disk space allocation is increased, it cannot be reduced.
  - If you wish to create OVOC VMs in a Cluster environment that supports High Availability and you are using shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster ([Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster](#) on page 45).

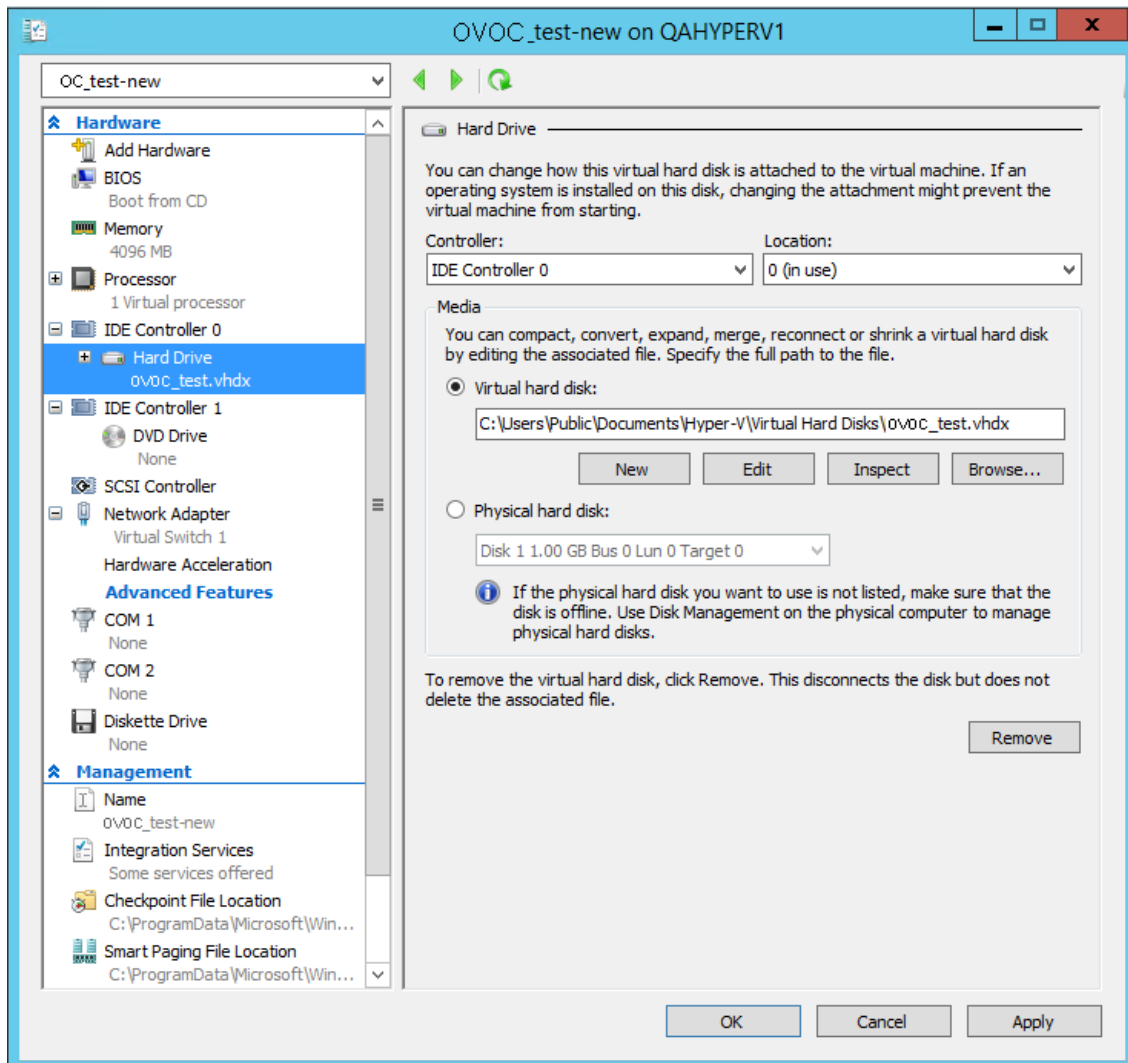
## Expanding Disk Capacity

The OVOC server virtual disk is provisioned by default with a minimum volume. In case a higher capacity is required for the target OVOC server then the disk can be expanded.

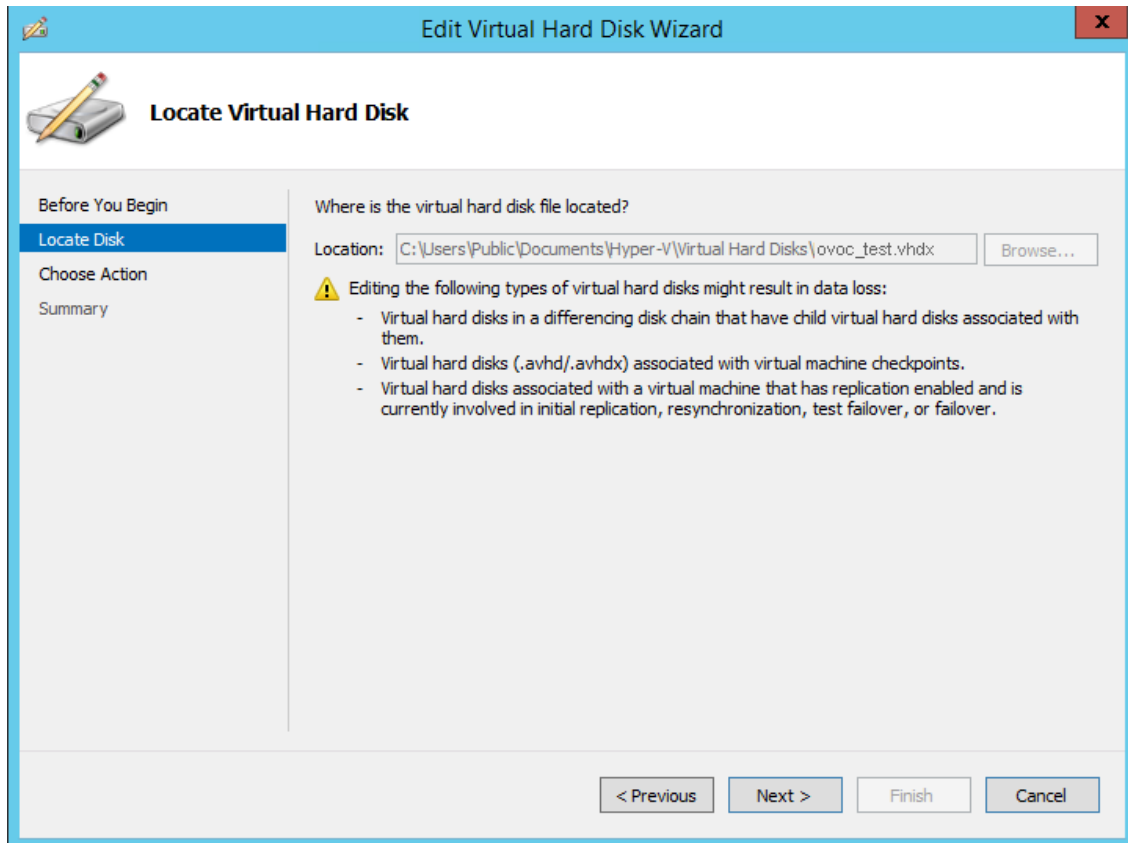
### ➤ To expand the disk size:

1. Make sure that the target OVOC server VM is not running - Off state.
2. Select the Hard Drive, and then click **Edit**.

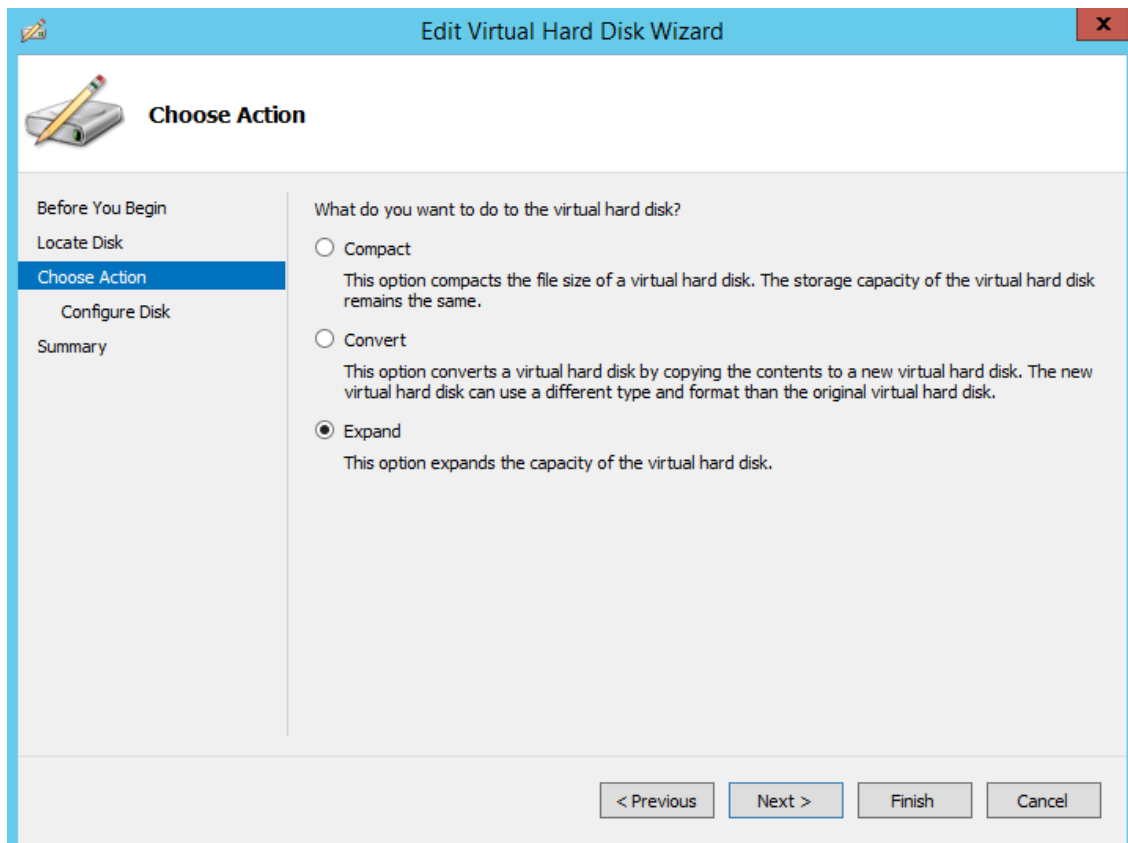


**Figure 7-10: Expanding Disk Capacity**

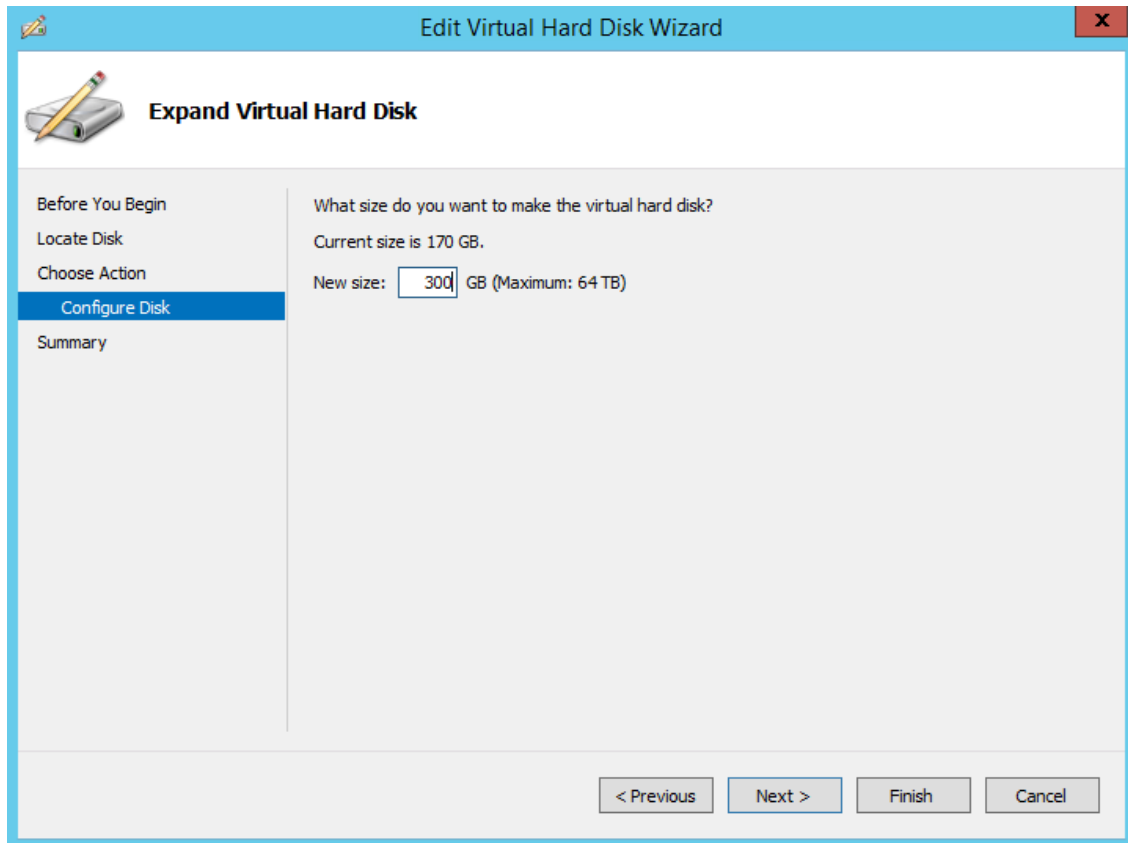
The Edit Virtual Disk Wizard is displayed as shown below.

**Figure 7-11: Edit Virtual Hard Disk Wizard**

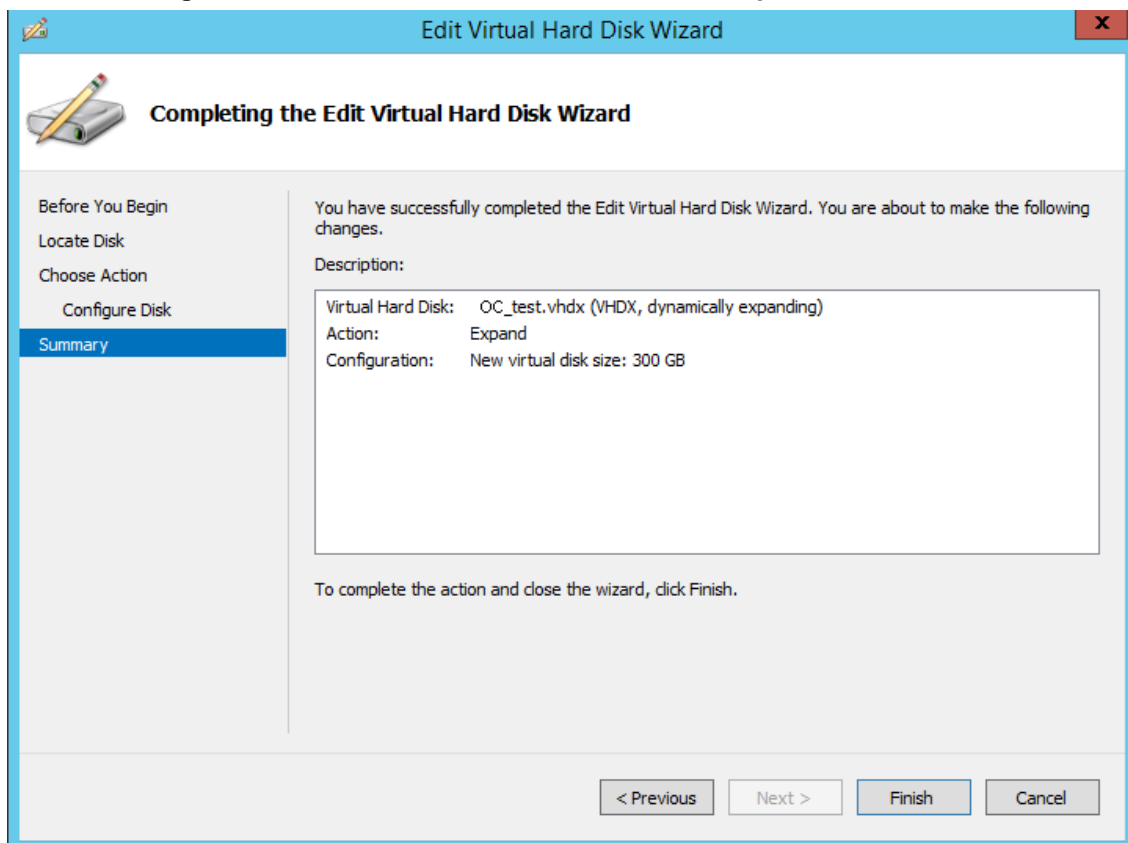
3. Click **Next**; the Choose Action screen is displayed:

**Figure 7-12: Edit Virtual Hard Disk Wizard-Choose Action**

4. Select the **Expand** option, and then click **Next**; the Expand Virtual Hard Disk screen opens.

**Figure 7-13: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk**

5. Enter the required size for the disk, and then click **Next**; the Summary screen is displayed.

**Figure 7-14: Edit Virtual Hard Disk Wizard-Completion**

6. Verify that all of the parameters have been configured, and then click **Finish**. The settings window will be displayed.
7. Click **OK** to close.

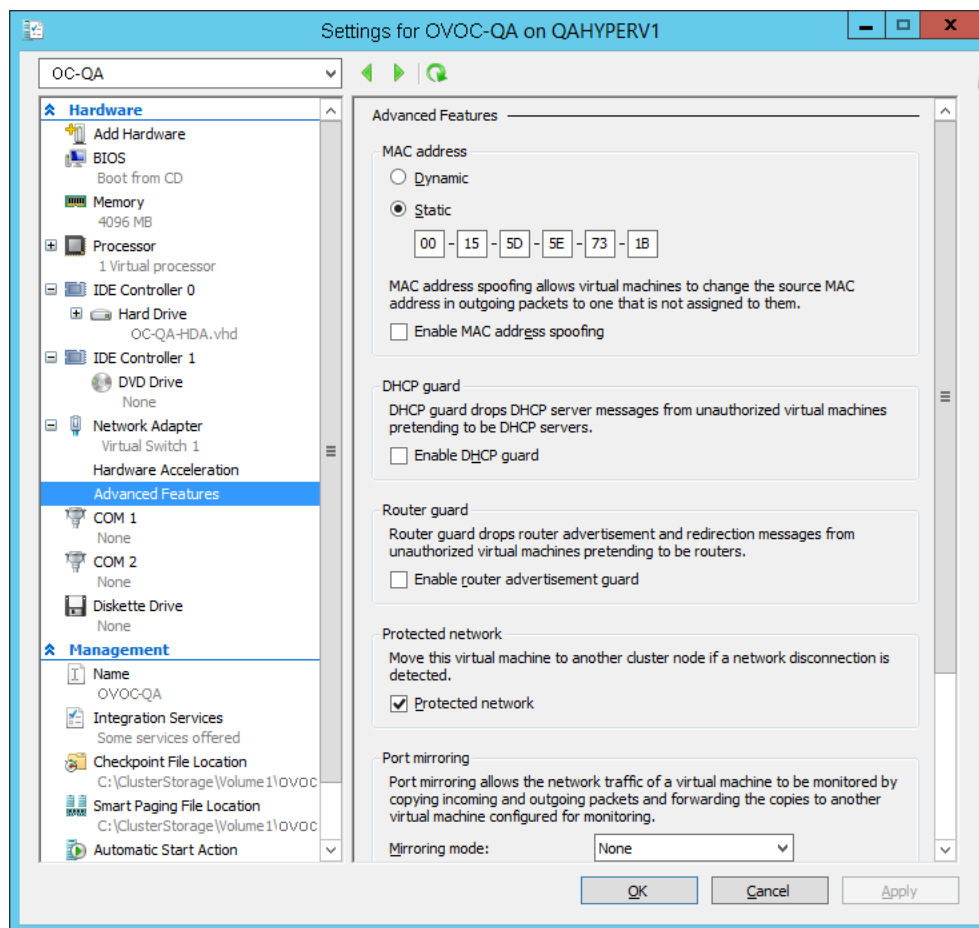
## Changing MAC Addresses from 'Dynamic' to 'Static'

By default, the MAC addresses of the OVOC server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license. To prevent this from occurring, MAC Addresses should be changed from 'Dynamic' to 'Static'.

### ➤ To change the MAC address to 'Static' in Microsoft Hyper-V:

1. Shutdown the OVOC server ( [Shutdown the OVOC Server Machine](#) on page 115).
2. In the Hardware pane, select **Network Adapter** and then **Advanced Features**.
3. Select the MAC address 'Static' option.
4. Repeat steps 2 and 3 for each network adapter.

**Figure 7-15: Advanced Features - Network Adapter – Static MAC Address**



## Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster

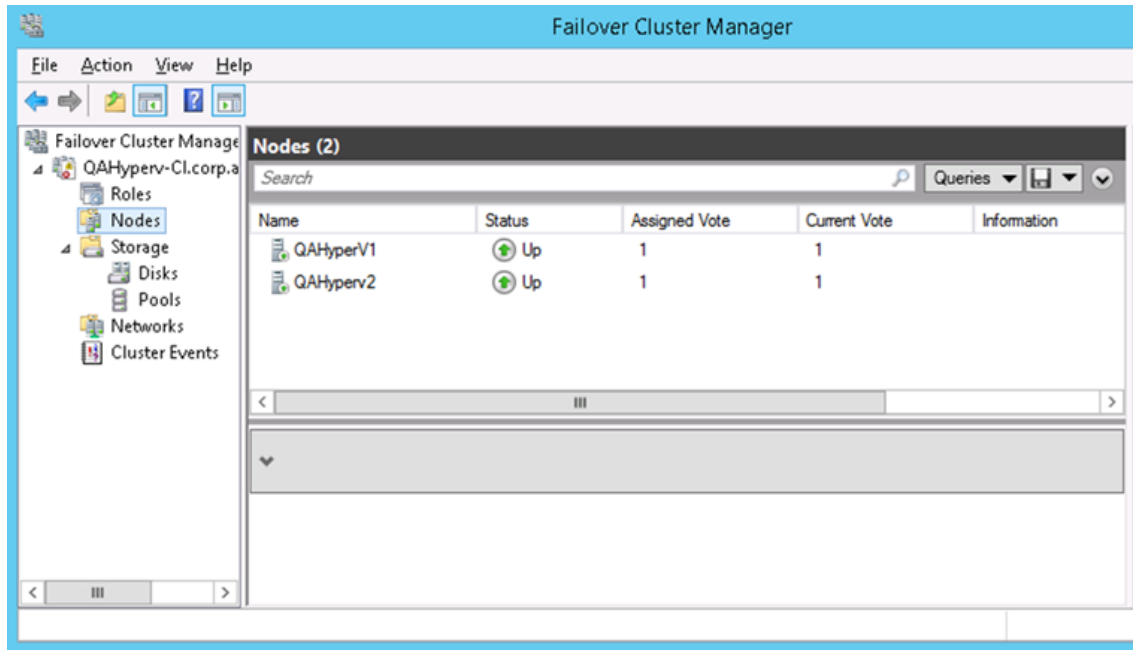
This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

## Hyper-V Cluster Site Requirements

Ensure that your Hyper-V cluster site meets the following requirements:

- The configuration process assumes that your Hyper-V failover cluster contains at least two Windows nodes with installed Hyper-V service.
- The cluster should be connected to a shared network storage of iSCSI type or any other supported type. For example, “QAHyperv” contains two nodes.

**Figure 7-16: Hyper-V-Failover Cluster Manager Nodes**



- The OVOC VM should be created with a hard drive which is situated on a shared cluster storage.

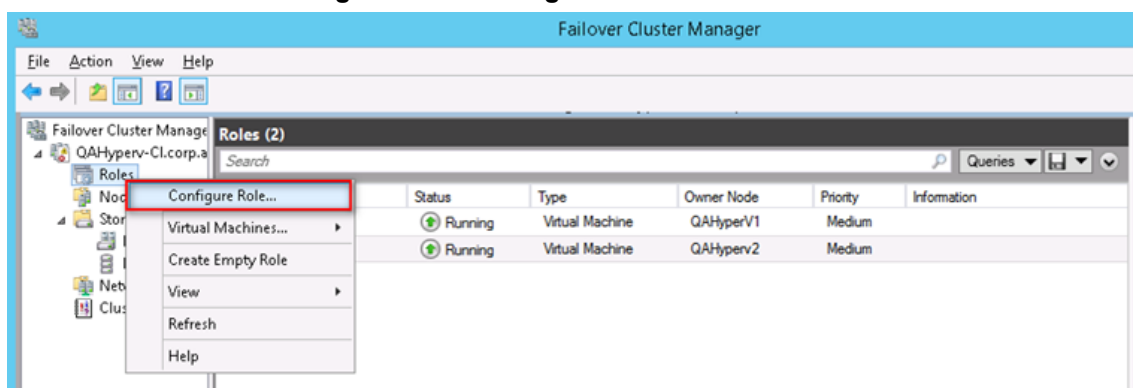
## Add the OVOC VM in Failover Cluster Manager

After you create the new OVOC VM, you should add the VM to a cluster role in the Failover Cluster Manager.

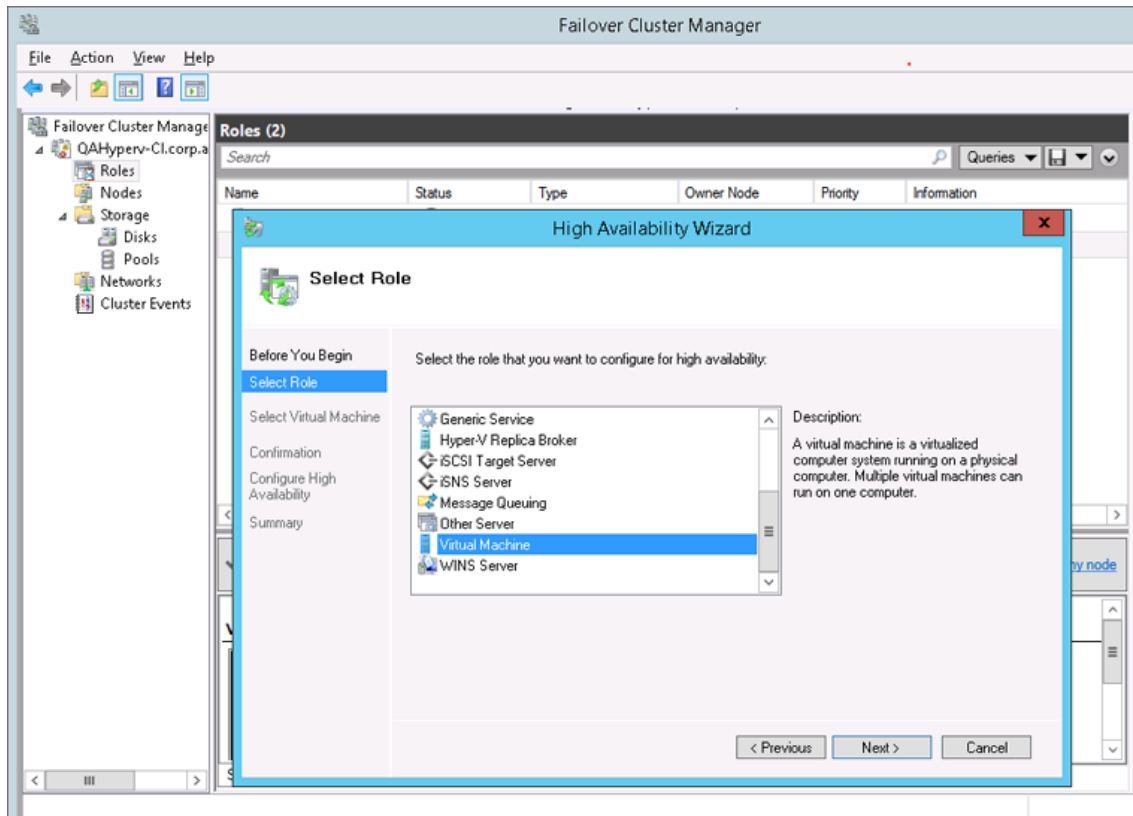
### ➤ To add the OVOC VM in Failover Cluster Manager:

1. Right-click “Roles” and in the pop up menu, choose **Configure Role**:

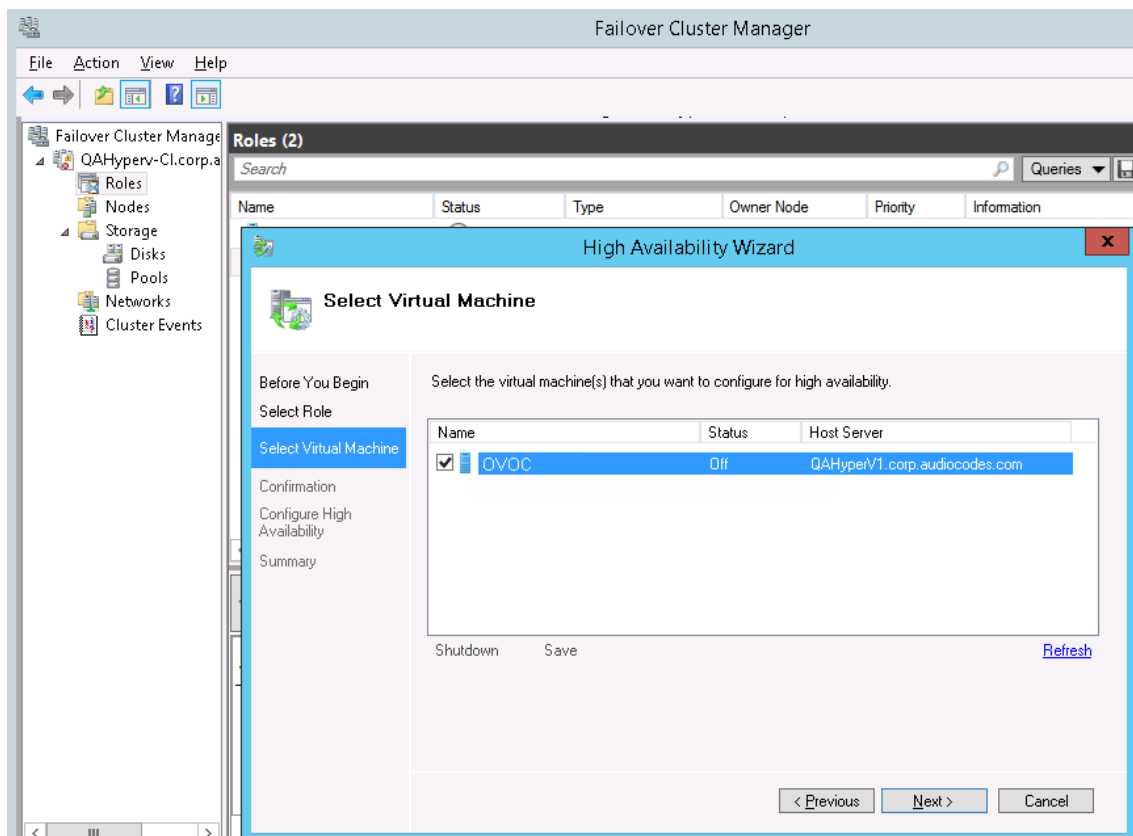
**Figure 7-17: Configure Role**



2. In the Select Role window, select the **Virtual Machine** option and then click **Next**.

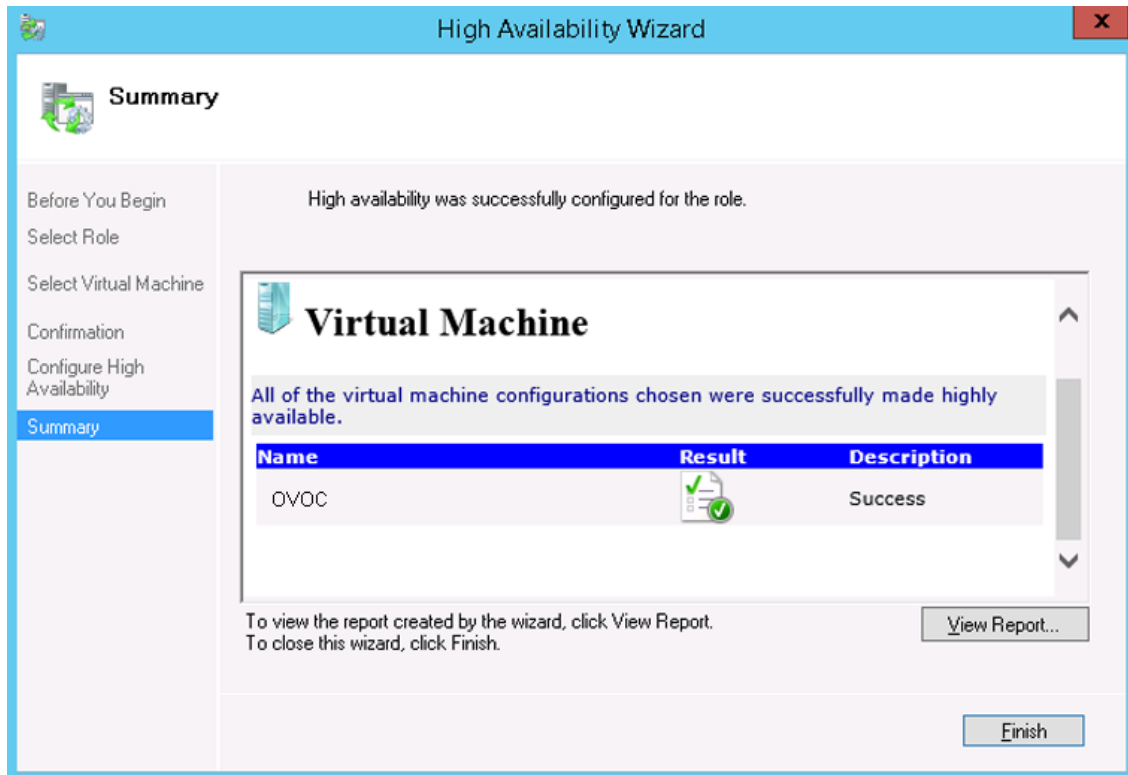
**Figure 7-18: Choose Virtual Machine**

A list of available VMs are displayed; you should find the your new created OVOC VM:

**Figure 7-19: Confirm Virtual Machine**

3. Select the check box, and then click **Next**.

At the end of configuration process you should see the following:

**Figure 7-20: Virtual Machine Successfully Added**

4. Click **Finish** to confirm your choice.

Now your OVOC VM is protected by the Windows High Availability Cluster mechanism.



If you wish to manually move the OVOC VMs to another cluster node, see Appendix [Managing Clusters](#) on page 184.

## Cluster Host Node Failure on Hyper-V

In case a host node where the VM is running fails, then the VM is restarted on the redundant cluster host node automatically.



When one of the cluster hosts fails, the OVOC VM is automatically moved to the redundant server host node. During this process, the OVOC VM is restarted and consequently any running OVOC process are dropped. The move process may take several minutes.

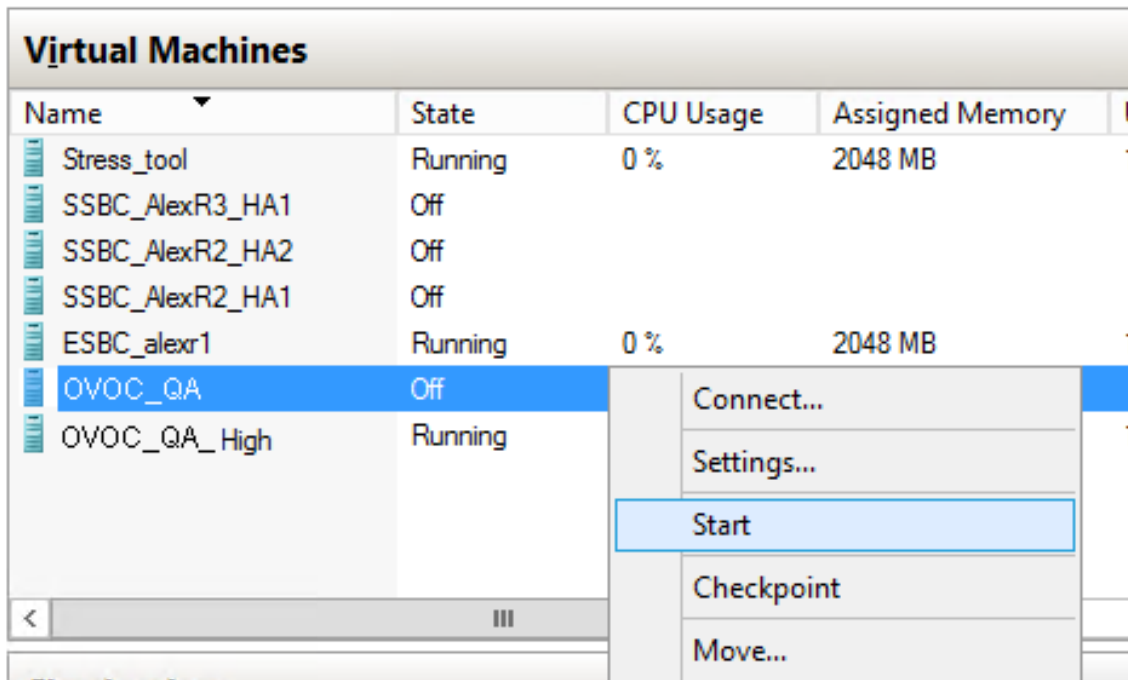
## Connecting OVOC Server to Network on HyperV

After installation, the OVOC server is assigned, a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network interface card connected to the 'trusted' virtual network switch during the OVOC server installation. You need to change this IP address to suit your IP addressing scheme.

### ➤ To reconfigure the OVOC server IP address:

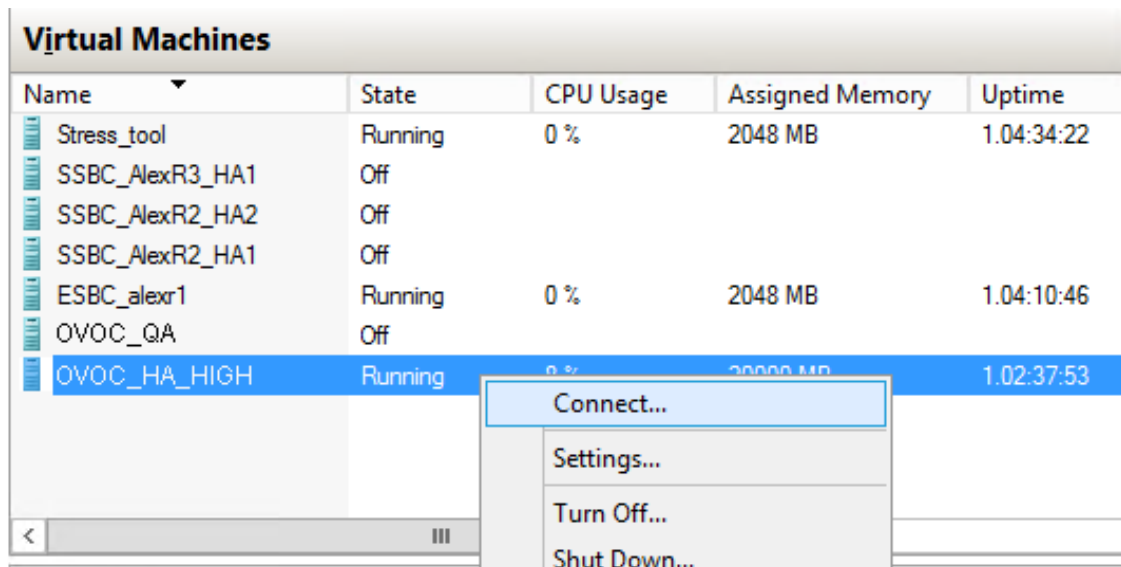
1. Start the OVOC server virtual machine, on the Hyper-V tree, right-click the OVOC server, and then in the drop-down menu, choose **Start**.

Figure 7-21: Power On Virtual Machine



2. Connect to the console of the running server by right-clicking the OVOC server virtual machine, and then in the drop-down menu, choose **Connect**.

Figure 7-22: Connect to OVOC server Console



3. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Start the OVOC Server Manager utility by specifying the following command:

```
# EmsServerManager
```

6. Set the OVOC server network IP address to suit your IP addressing scheme ([Server IP Address](#) on page 117).



7. Perform other configuration actions as required using the OVOC Server Manager ([Getting Started](#) on page 101).

## 8 Installing OVOC Server on a VMware Virtual Machine

This section describes how to install the OVOC server on the VMware vSphere platform. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in [Configuring the Virtual Machine Hardware Settings](#) on page 39). The upgrade time depends on the hardware machine where the VMware vSphere platform is installed. The VMware Virtual Machine installation package is provided on **DVD 5** ([Virtual Appliance and Cloud Options](#) on page 14).



- Ensure that the minimum platform requirements are met (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the installation.
- For obtaining the installation files, see [OVOC Software Deliverables](#) on page 14. Note that you should verify the installation files (see [Files Verification](#) on page 72).

### Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) 6.5

This section describes how to deploy the OVOC image with the VMware ESXi 6.5 Web client. The procedure described below is necessary due a limitation on the VMware ESXi 6.5 WEB client for decompressing OVA images . This procedure is run using the VMware OVF tool that can be installed on any Linux machine.



The cause of this limitation is attributed solely to the VMware ESXi 6.5 platform. Download the OVF tool software and documentation from <https://www.vmware.com/support/developer/ovf/>

#### ➤ To run VMware OVF tool:

1. Open the VMware OVF tool.
2. Enter the following commands and press Enter:

```
ovftool --disableVerification --noSSLVerify --name=$VMname --datastore=datastore2 -
dm=thin --acceptAllEulas --powerOn $ovaFilePath
vi://$user:$password@$VMwareHOSTIPAddress
```

Where:

\$VMname is the name of the VMware Host machine

\$user:\$password is the user and password of the VMware Host machine

\$VMwareHOSTIPAddress is the IP address of the VMware Host machine

#### Example

```
ovftool --disableVerification --noSSLVerify --name=OVOC --datastore=datastore1 -dm=thin -
-acceptAllEulas --powerOn /tmp/ovoc_server_7.6.1116.ova vi://root:blabla@172.17.135.9
```

The following progress is displayed:

```
Opening OVA source: /data1/7.4/DVD5/7.4.2094/OVOC-VMware-7.4.2094.ova
Opening VI target: vi://root@172.17.135.9:443/
Deploying to VI: vi://root@172.17.135.9:443/
Disk progress: 10%
...
```

```
Transfer Completed
The manifest validates
Powering on VM: FirstDeploy
Task Completed
Warning:
- No manifest entry found for: 'OVOC-VMware-7.4.2094-disk1.vmdk'.
Completed successfully
```

## Configuring the Virtual Machine Hardware Settings

This section shows how to configure the Virtual Machine's hardware settings.

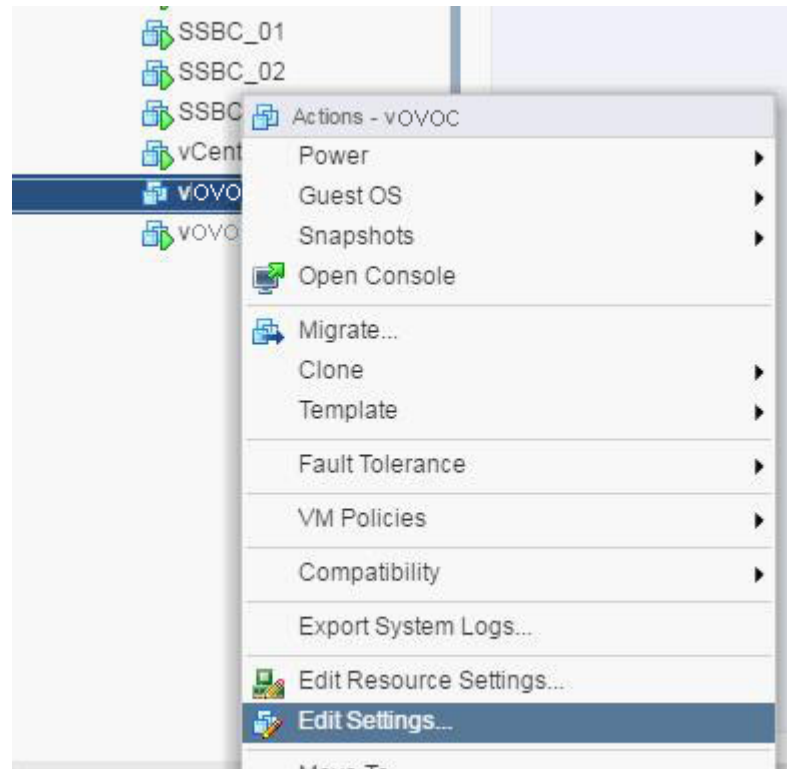
Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see [Hardware and Software Specifications](#) on page 7.

**Table 8-1: Virtual Machine Configuration**

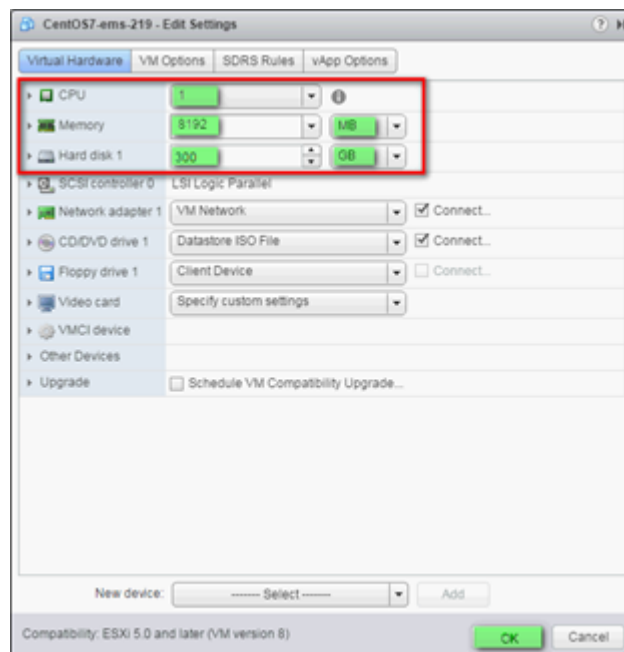
Required Parameter	Value
Disk size	
Memory size	
CPU cores	

➤ **To configure the virtual machine hardware settings:**

1. Before powering up the machine, go to the virtual machine **Edit Settings** option.




**Figure 8-1: Edit Settings option**

2. In the **CPU**, **Memory** and **Hardware** tabs set the required values accordingly to the desired OVOC server VMware Disk Space allocation. ( [Hardware and Software Specifications](#) on page 7), and then click **OK**.

**Figure 8-2: CPU, Memory and Hard Disk Settings**

- Once the hard disk space allocation is increased, it cannot be reduced to a lower amount.
  - If you wish to create OVOC VMs in a cluster environment supporting High Availability and you are using shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster ([Configuring OVOC Virtual Machines \(VMs\) in a VMware Cluster](#) on the next page).
3. **Wait** until the machine reconfiguration process has completed.

**Figure 8-3: Recent Tasks**

Recent Tasks						
Name	Target	Status	Requested Start Time	Start Time	Completed Time	
 Reconfigure virtual machine	 AudioCodes OVOC	 Completed	21/05/2012 11:03:39	21/05/2012 11:03:39	21/05/2012 11:03:41	

## Configuring OVOC Virtual Machines (VMs) in a VMware Cluster

This section describes how to configure OVOC VMs in a VMware cluster.

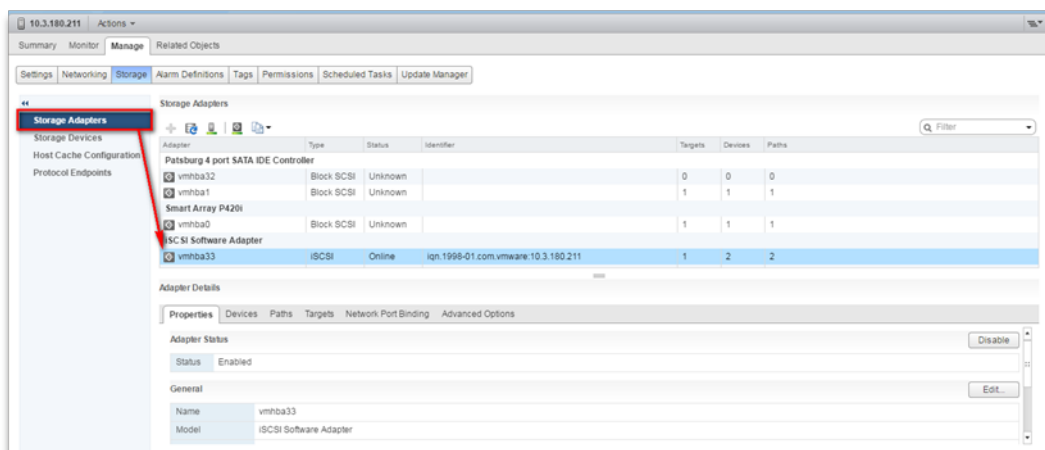
### VMware Cluster Site Requirements

Ensure that your VMware cluster site meets the following requirements:

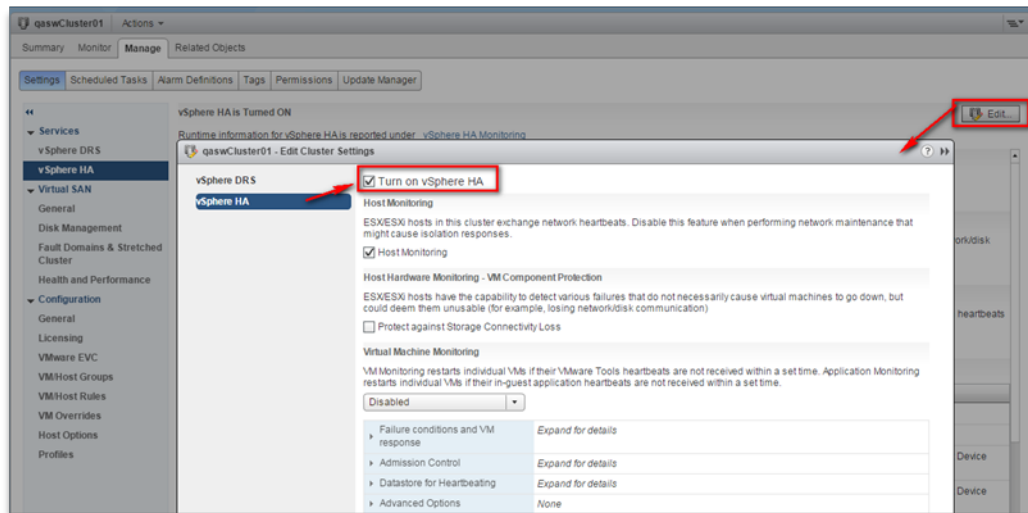
- The configuration process assumes that you have a VMware cluster that contains at least two ESXi servers controlled by vCenter server.
- The clustered VM servers should be connected to a shared network storage of type iSCSI or any other types supported by VMware ESXi.

For example, a datastore “QASWDatacenter” which contains a cluster named “qaswCluster01” and is combined of two ESXi servers ( figure below).

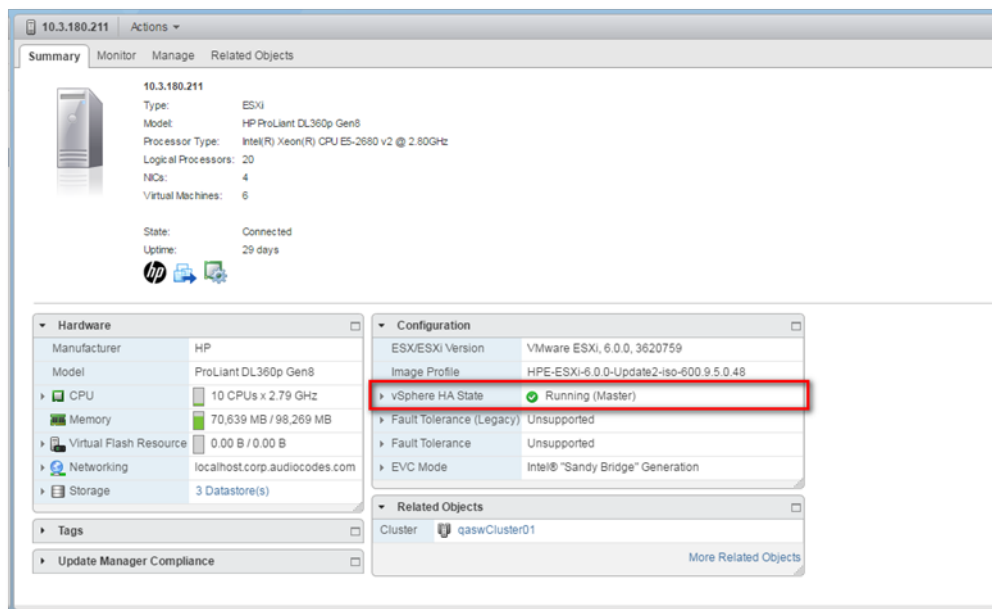
- Verify that Shared Storage is defined and mounted for all cluster members:

**Figure 8-4: Storage Adapters**

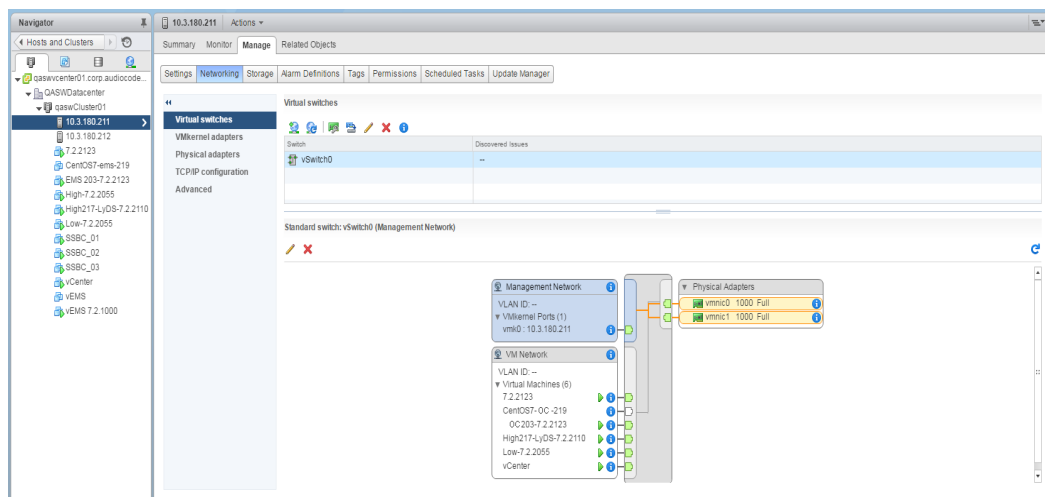
- Ensure that the 'Turn On vSphere HA' check box is selected:

**Figure 8-5: Turn On vSphere HA**

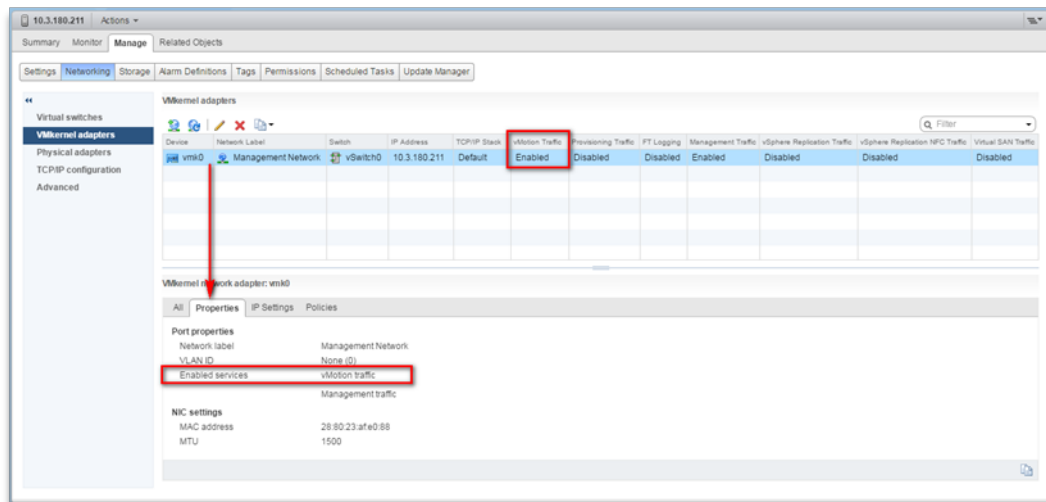
- Ensure that HA is activated on each cluster node:

**Figure 8-6: Activate HA on each Cluster Node**

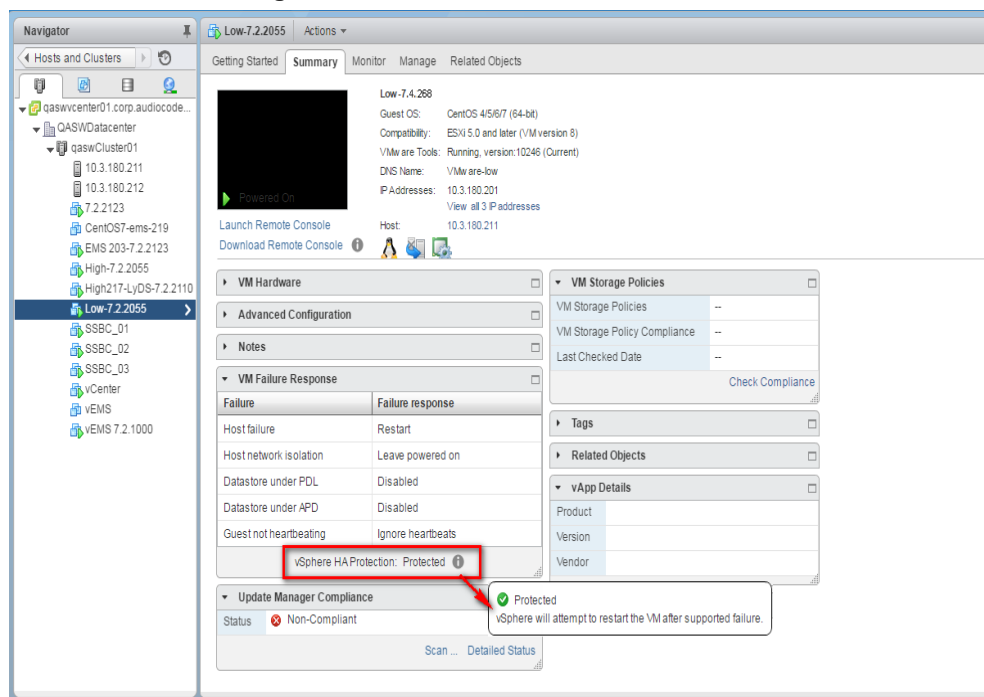
- Ensure that the networking configuration is identical on each cluster node:

**Figure 8-7: Networking**

- Ensure that the vMotion is enabled on each cluster node. The recommended method is to use a separate virtual switch for vMotion network (this should be defined in all cluster nodes and interconnected):

**Figure 8-8: Switch Properties**

- A VM will be movable and HA protected only when its hard disk is located on shared network storage on a cluster. You should choose an appropriate location for the VM hard disk when you deploy the OVOC VM. If your configuration is performed correctly, a VM should be marked as “protected” as is shown in the figure below:

**Figure 8-9: Protected VM**

If you wish to manually migrate the OVOC VMs to another cluster node, see [Managing Clusters](#) on page 184.

## Cluster Host Node Failure on VMware

In case a host node where the VM is running fails, the VM is restarted on the redundant cluster node automatically.



When one of the cluster nodes fail, the OVOC VM is automatically migrated to the redundant host node. During this process, the OVOC VM is restarted and consequently any active OVOC process is dropped. The migration process may take several minutes.

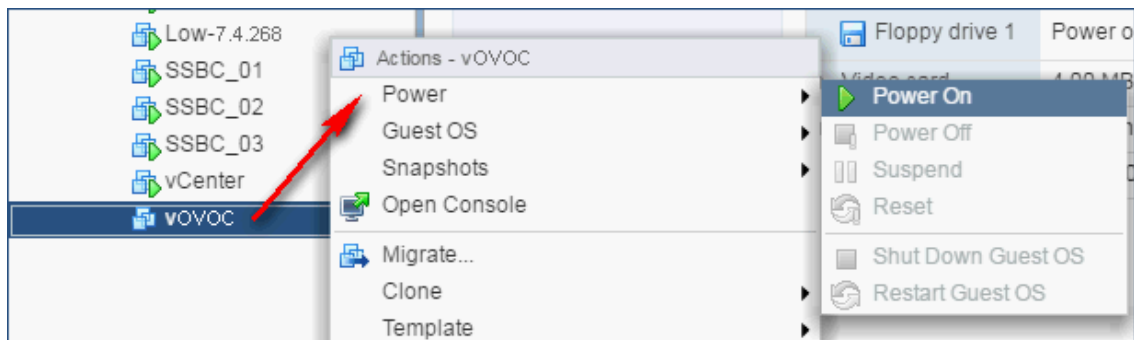
## Connecting OVOC Server to Network on VMware

After installation, the OVOC server is assigned a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network interface card connected to the 'trusted' virtual network switch during the OVOC server installation. You need to change this IP address to suit your IP addressing scheme.

### ➤ To assign OVOC server IP address to network:

1. Power on the machine; in the vCenter tree, right-click the AudioCodes One Voice Operations Center node (vOC) and in the drop-down menu, choose **Power > Power On**. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications ([Hardware and Software Specifications](#) on page 7).

Figure 8-10: Power On



2. Wait until the boot process has completed, and then connect the running server through the vSphere client console.
3. Login into the OVOC server by SSH, as 'acems' user and enter *acems* password.
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Proceed to the network configuration using the OVOC Server Manager. To run the manager type 'EmsServerManager', and then press Enter.
6. Set the OVOC server network IP address as described in [Server IP Address](#) on page 117.
7. Perform configuration actions as required using the OVOC Server Manager ([Getting Started](#) on page 101).



**This page is intentionally left blank.**

## 9 Installing OVOC Server on Dedicated Hardware

The OVOC server installation process supports the Linux platform. The installation includes four separate components, where each component is supplied on a separate DVD:

- **DVD1:** OS installation: OS installation DVD
- **DVD2:** Oracle Installation: Oracle installation DVD platform
- **DVD3:** OVOC application: OVOC server application installation DVD



- Ensure that the minimum platform requirements are met (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the installation.
- For obtaining the installation files, see [OVOC Software Deliverables](#) on page 14. Note that you should verify the installation files (see [Files Verification](#) on page 72

### DVD1: Linux CentOS 7.3

The procedure below describes how to install Linux CentOS 7.3. This procedure takes approximately 20 minutes.



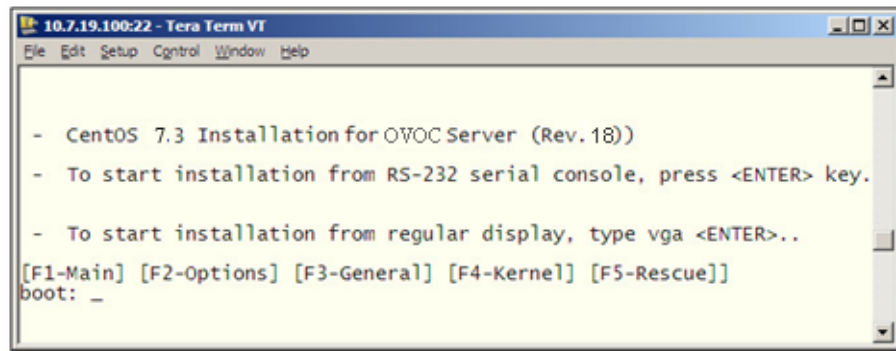
Before commencing the installation, you must configure RAID-0 (see [Appendix Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Servers](#) on page 177).

#### ➤ To perform DVD1 installation:

1. Insert the **DVD1-CentOS 7.3 Rev 18** into the DVD ROM.
2. Connect the OVOC server through the serial port with a terminal application and login with 'root' user. Default password is *root*.
3. Perform OVOC server machine reboot by specifying the following command:

```
reboot
```

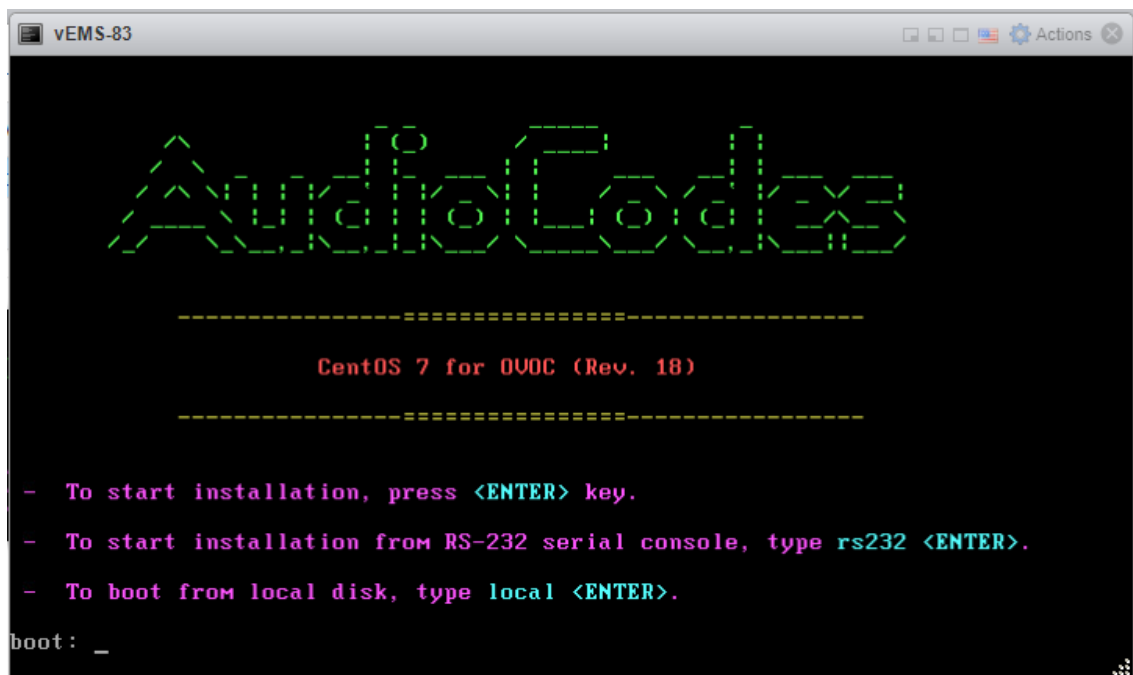
4. Press Enter; you are prompted whether you which to start the installation through the RS-232 console or through the regular display.
5. Press Enter to start the installation from the RS-232 serial console or type **vga**, and then press Enter to start the installation from a regular display.

**Figure 9-1: Linux CentOS Installation**

10.7.19.100:22 - Tera Term VT

File Edit Setup Control Window Help

```
- CentOS 7.3 Installation for OVOC Server (Rev.18))  
- To start installation from RS-232 serial console, press <ENTER> key.  
- To start installation from regular display, type vga <ENTER>..  
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]  
boot: _
```

**Figure 9-2: CentOS 7.3**

vEMS-83

AudioCodes

-----

CentOS 7 for OVOC (Rev. 18)

-----

```
- To start installation, press <ENTER> key.  
- To start installation from RS-232 serial console, type rs232 <ENTER>..  
- To boot from local disk, type local <ENTER>..  
boot: _
```

6. Wait for the installation to complete.

**Figure 9-3: CentOS Installation**

```
vEMS-83
Installing compat-libgfortran-41 (392/417)
Installing compat-libf2c-34 (393/417)
Installing iwl2000-firmware (394/417)
Installing iwl1000-firmware (395/417)
Installing roothfs (396/417)
Installing iwl2830-firmware (397/417)
Installing iwl5150-firmware (398/417)
Installing iwl6000-firmware (399/417)
Installing iwl3160-firmware (400/417)
Installing ivtv-firmware (401/417)
Installing iwl135-firmware (402/417)
Installing iwl7260-firmware (403/417)
Installing iwl3945-firmware (404/417)
Installing iwl6950-firmware (405/417)
Installing iwl100-firmware (406/417)
Installing iwl7265-firmware (407/417)
Installing iwl6000g2b-firmware (408/417)
Installing iwl6000g2a-firmware (409/417)
Installing iwl5000-firmware (410/417)
Installing iwl4965-firmware (411/417)
Installing iwl105-firmware (412/417)
Installing libgcc.i686 (413/417)
Installing nss-softhoken-freebl.i686 (414/417)
Installing glibc.i686 (415/417)
Installing libstdc++.i686 (416/417)
Installing compat-libstdc++-33.i686 (417/417)
Performing post-installation setup tasks
Installing boot loader

Performing post-installation setup tasks

Configuring installed system

Writing network configuration

Creating users

Configuring addons

Generating initramfs

Running post-installation scripts

Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA

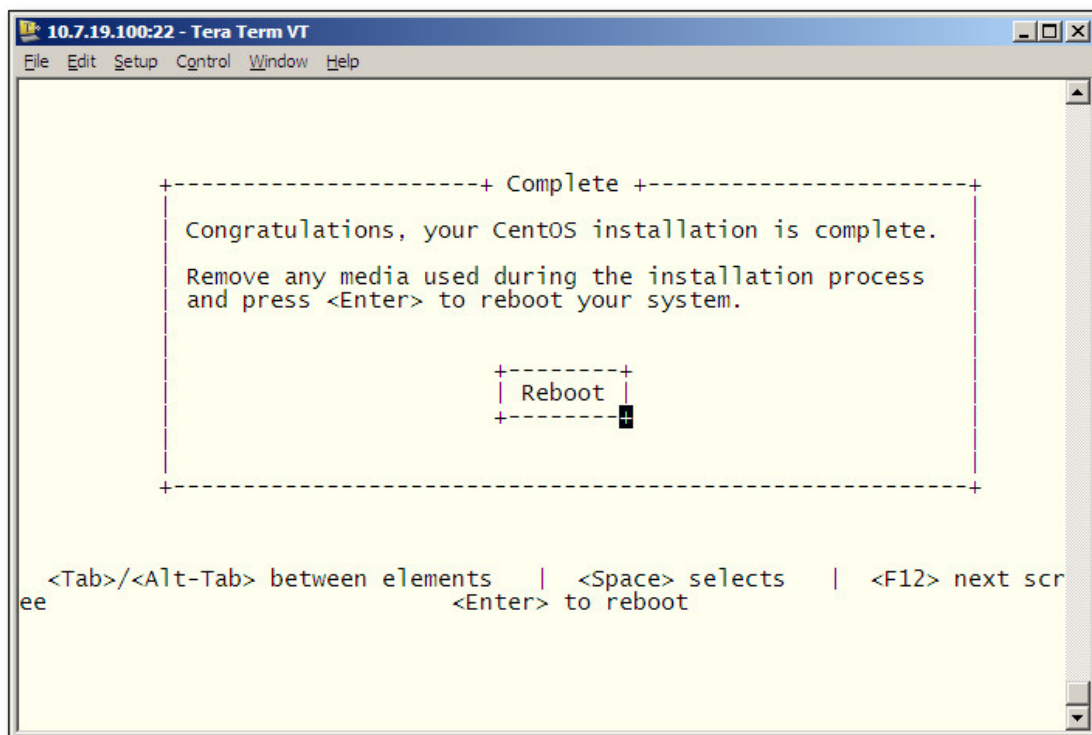
Installation complete. Press return to quit
```

7. Reboot your machine by pressing Enter.



Do not forget to remove the Linux installation DVD from the DVD-ROM before rebooting your machine.

**Figure 9-4: Linux CentOS Installation Complete**



8. Login as 'root' user with password *root*.

9. Type **network-config**, and then press Enter; the current configuration is displayed:

**Figure 9-5: Linux CentOS Network Configuration**

```
[acems@OVOC-7 ~]$ su -
Password:
Last login: Thu Dec 14 12:08:24 GMT 2017 on pts/0
[root@OVOC-7 ~]# TMOUT=0
[root@OVOC-7 ~]# network-config
-----
Current network configuration:
-----
Hostname           : OVOC-7
IP Address          : 10.3.180.7
Prefix              : 16
Default Gateway     : 10.3.0.1

Do you wish to change it? (y/[n]) : y

Hostname           : ovoc-server-7
IP Address          : 10.3.180.7
Prefix              : 16
Default Gateway     : 10.3.0.1

Apply new configuration? ([y]/n) : y

-----

Activate the network configuration.
```



This script can only be used during the server installation process. Any additional Network configuration should later be performed using the OVOC Server Manager.

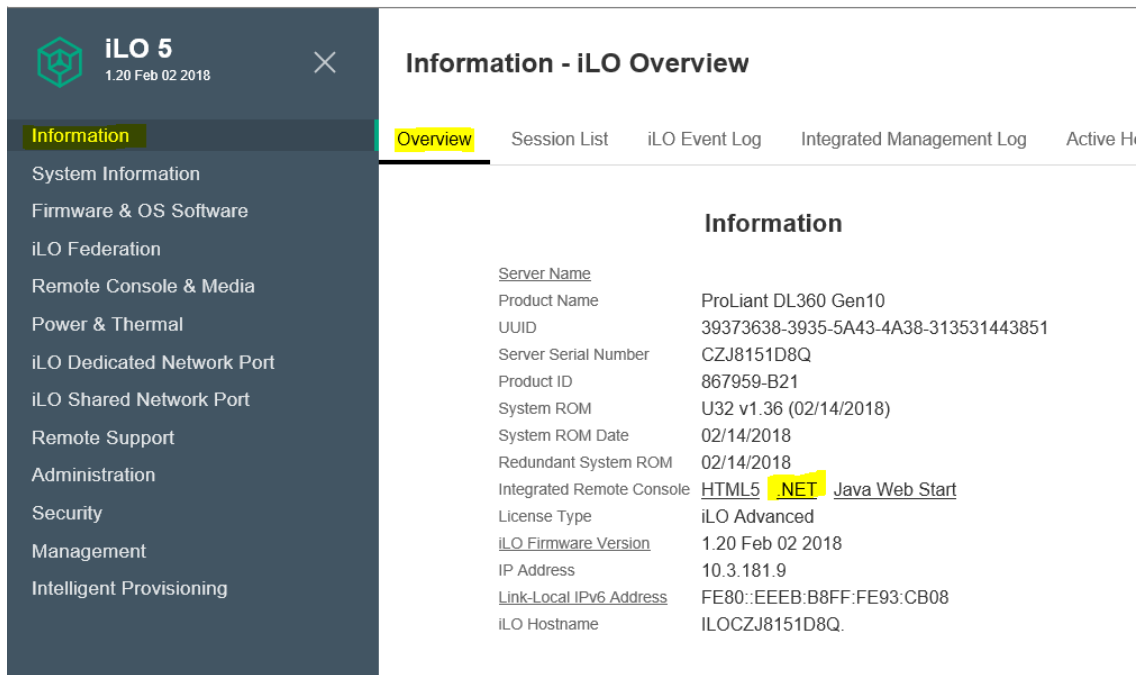
10. You are prompted to change the configuration; enter **y**.
11. Enter your Hostname, IP Address, Subnet Mask and Default Gateway.
12. Confirm the changes; enter **y**.
13. You are prompted to reboot; enter **y**.

## Installing DVD1 without a CD-ROM

This section describes how to install DVD1 without a CD-ROM.

### ➤ To install DVD1 without a CD-ROM:

1. Login to ILO 5 with “Administrator” privileges.
2. Launch the Integrated Remote Console.

**Figure 9-6: Information-iLO Overview**


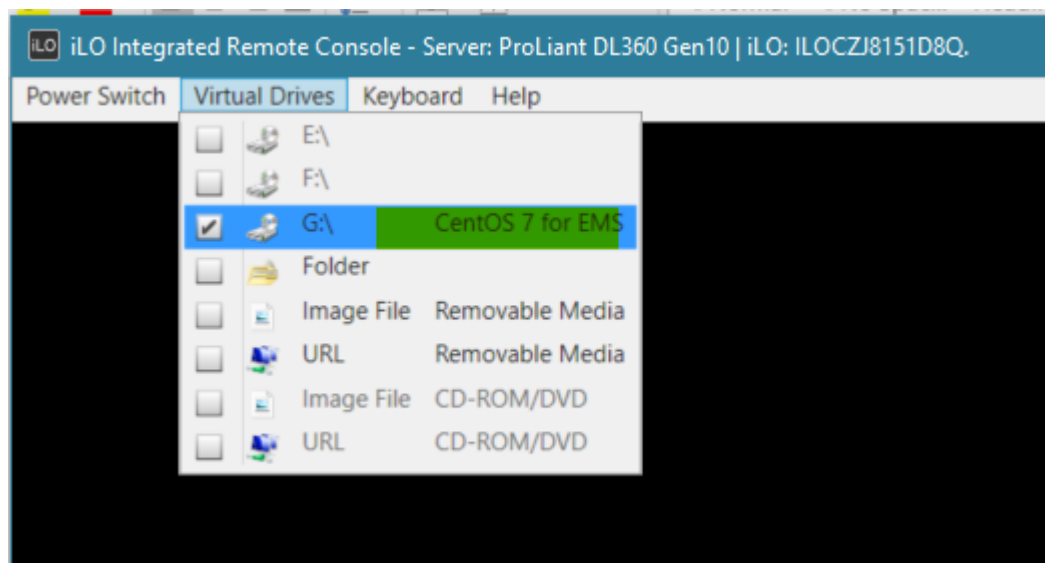
**iLO 5**  
1.20 Feb 02 2018

**Information - iLO Overview**

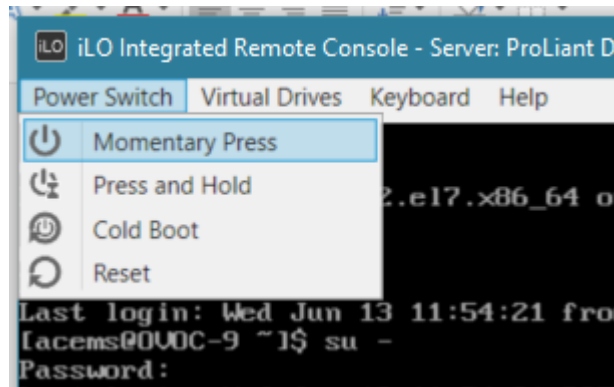
**Information**

Server Name	ProLiant DL360 Gen10
Product Name	ProLiant DL360 Gen10
UUID	39373638-3935-5A43-4A38-313531443851
Server Serial Number	CZJ8151D8Q
Product ID	867959-B21
System ROM	U32 v1.36 (02/14/2018)
System ROM Date	02/14/2018
Redundant System ROM	02/14/2018
Integrated Remote Console	<a href="#">HTML5</a> <a href="#">NET</a> <a href="#">Java Web Start</a>
License Type	iLO Advanced
iLO Firmware Version	1.20 Feb 02 2018
IP Address	10.3.181.9
Link-Local IPv6 Address	FE80::EEEE:B8FF:FE93:CB08
iLO Hostname	ILOCZJ8151D8Q

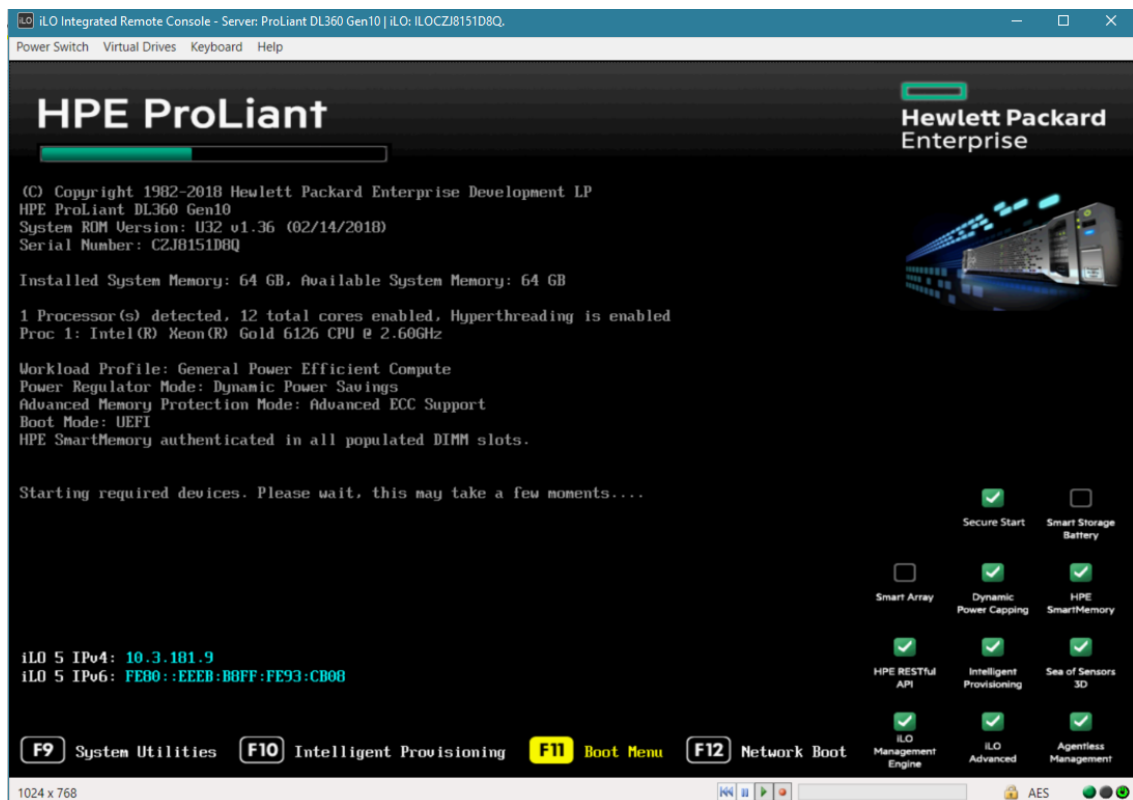
3. On your PC insert the OVOC DVD1 to the drive and note the drive letter.
4. From Integrated Remote Console, click Virtual Drives and select the appropriate drive letter.

**Figure 9-7: iLO Integrated Remote Console**

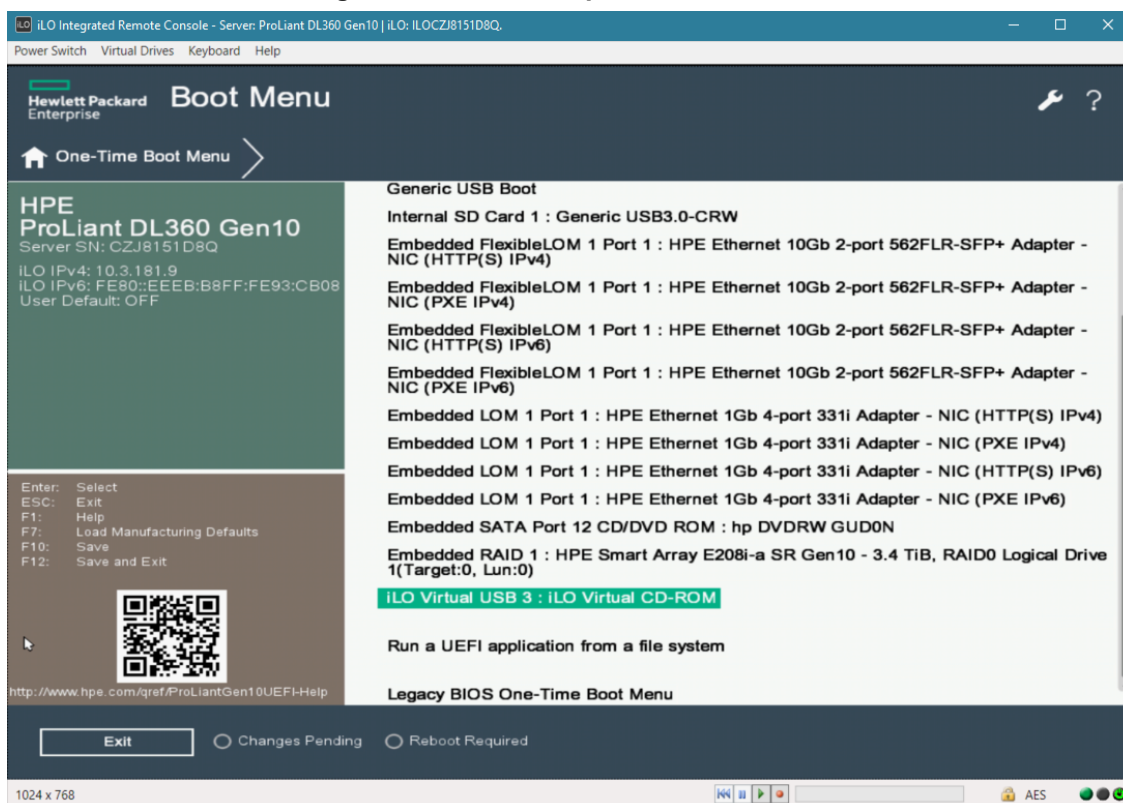
5. From Integrated Remote Console, click **Power Switch > Momentary Press**, the server is shutdown. Click **Momentary Press** to power the server back on.

**Figure 9-8: Momentary Press**

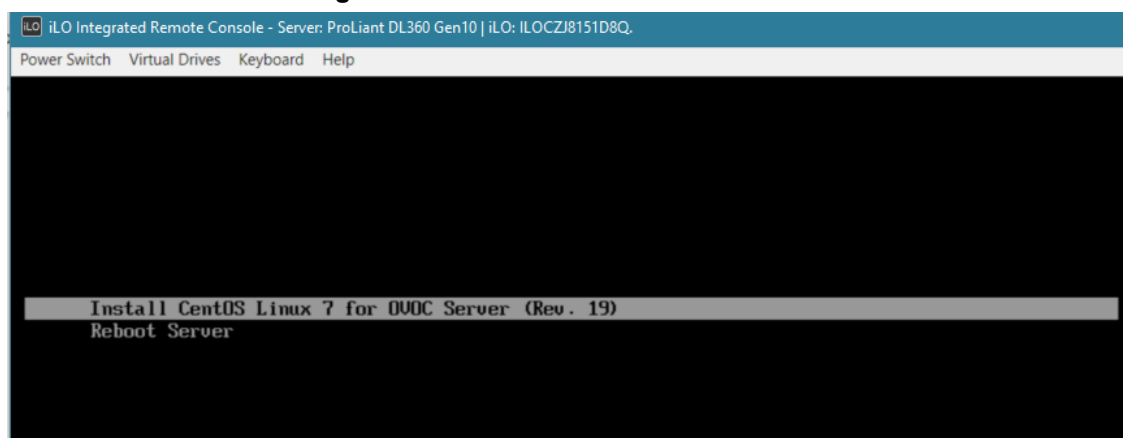
After server boot process has commenced, press F11 to enter the boot menu.

**Figure 9-9: Boot Menu**

6. On boot menu, scroll down by mouse or arrows keys and select the “iLO Virtual USB 3 : iLO Virtual CD-ROM” to start the boot sequence.

**Figure 9-10: Boot Sequence**

7. The following screen appears, select “Install CentOS ...” and press Enter.

**Figure 9-11: Install CentOS**

8. After a while the CentOS installation commences:

**Figure 9-12: Start CentOS**



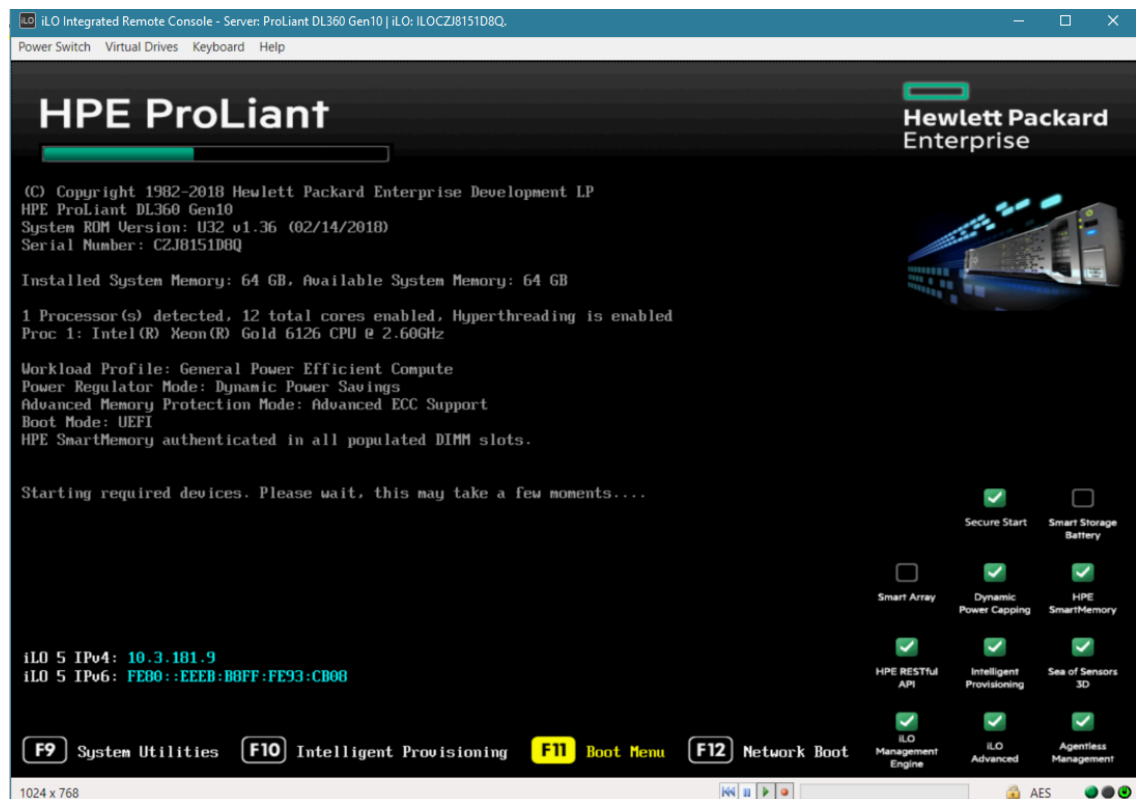
9. Wait for the installation to finish, from “Virtual Drives” menu deselect the selected drive and press Enter, the server is rebooted.

Figure 9-13: Server Rebooted

```
Installing glibc.i686 (420/422)
Installing libstdc++.i686 (421/422)
Installing compat-libstdc++-33.i686 (422/422)
Performing post-installation setup tasks
Installing boot loader
.
Performing post-installation setup tasks
.
Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
.
Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA
.
Installation complete. Press return to quit
anaconda1 i:main* 2:shell 3:log 4:storage-log 5:program-log- Switch tab
1024 x 768
```

10. After server has restarted, press F11 to enter boot menu.

Figure 9-14: Boot Menu



## DVD2: Oracle DB Installation

The procedure below describes how to install the Oracle database. This procedure takes approximately 30 minutes.



Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

## ➤ To perform DVD2 installation:

1. Insert **DVD2-Oracle DB installation** into the DVD ROM.
2. Login into the OVOC server by SSH, as 'acems' user, and enter password *acems*.
3. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

4. Mount the CDROM to make it available:

```
mount -t iso9660 /dev/sr0 /mnt
cd /mnt
```

5. Run the installation script from its location:

```
./install
```

Figure 9-15: Oracle DB Installation

```
[root@EMS-Linux145 /]#
[root@EMS-Linux145 /]# cd /misc/cd
[root@EMS-Linux145 cd]# ./install
Start installValues
Use of uninitialized value in concatenation (.) or string at installValues.pm line 279.
ls: /misc/cd/ac_ems_deploy/: No such file or directory
"my" variable $date masks earlier declaration in same scope at AllSystemChecks.pm line 1302.
Found = in conditional, should be == at ./FastOracleInstall.pl line 120.
Start executing User Login Check script at Sun Oct  3 12:00:19 BST 2010

Login Check Successfully Passed.

>>> Verifying OS version - Sun Oct  3 12:00:20 BST 2010

...
SOFTWARE EVALUATION LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS SOFTWARE
EVALUATION AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE
AGREEMENT FOR THE AUDIOCODES SOFTWARE (THE "PROGRAM") AND
THE ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE
```

6. Enter **y**, and then press Enter to accept the License agreement.

Figure 9-16: Oracle DB Installation - License Agreement

```
8. NO WAIVER. The failure of either party to enforce any rights granted
hereunder or to take action against the other party in the event of any
breach hereunder shall not be deemed a waiver by that party as to
subsequent enforcement of rights or subsequent actions in the event of
future breaches.

Do you accept this agreement? (y/n)y
```

7. Type the 'SYS' user password, type **sys** and then press Enter.

**Figure 9-17: Oracle DB Installation (cont)**

```
SQL> Connected to an idle instance.
SQL> ORACLE instance started.

Total System Global Area  321601536 bytes
Fixed Size                  2102168 bytes
Variable Size              251661416 bytes
Database Buffers           62914560 bytes
Redo Buffers                4923392 bytes
SQL>
File created.

SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - 64bit Production
>>> Restoring database File using RMAN...

...
RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN> RMAN>  >>>

Restore has finished successfully...

...
>>> Please enter a password for the SYS user: ...
sys
```

- Wait for the installation to complete; reboot is not required at this stage.

**Figure 9-18: Oracle DB Installation (cont)**

```
...
>>> Start executing Create_DB_Listener_Startup_Scripts at - Thu Sep 16 18:59:07 IST 2010
...
chown: /ACEMS/orahome/network/log/listener.log: No such file or directory
>>> >>> PASSED
...
>>> Remove Oracle demo directory: /ACEMS/orahome/xdk/demo/java ...
/ACEMS/orahome/xdk/demo/java: No such file or directory
>>> Remove Oracle demo directory: /ACEMS/orahome/rdbms/demo ...
>>> !!!!!!!!!!!!!!! ORACLE INSTALL SUCCESSFULLY FINISHED !!!!!!!!!!!!!!! ...
EMS-Server40#
```

## DVD3: OVOC server Application Installation

The procedure below describes how to install the OVOC server application. This procedure takes approximately 20 minutes.

➤ **To perform DVD3 installation:**

1. Insert **DVD3-OVOC Server Application Installation** into the DVD ROM.
2. Login into the OVOC server by SSH, as 'acems' user, and enter the password *acems*.
3. Switch to 'root' user and provide *root* password (default password is *root*):

su - root

4. Mount the CDRom to make it available:

```
mount -t iso9660 /dev/sr0 /mnt
cd /mnt/EmsServerInstall/
```

5. Run the installation script from its location:

```
./install
```

**Figure 9-19: OVOC server Application Installation**

```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/
[root@EMS-Linux2 EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
  >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...
Login Check Successfully Passed.

  >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013

...
  >>>  >>> PASSED
...
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013

...
SOFTWARE LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I
ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

6. Enter **y**, and then press Enter to accept the License agreement.

**Figure 9-20: OVOC server Application Installation – License Agreement**

```
based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement or any of Licensee's rights or obl
tten permission of Licensor and any attempt to do so shall be without effe
sferred to any person; (ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regu
, and may require a license to export such. Licensee is solely responsible
11.7. Relationship of Parties Nothing herein shall be deemed to create an
the parties. Neither party shall have the right to bind the other to any o
11.8. Integration This Agreement is the complete and exclusive agreement b
ated hereto. Any Licensee purchase order issue for the software, documenta
erms hereof.
11.9. Counterparts This Agreement may be executed in multiple original cou
ing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
```

7. When you are prompted to change the *acems* and *root* passwords, enter new passwords or enter existing passwords. You are then prompted to reboot the OVOC server machine; press Enter.

Figure 9-21: OVOC server Application Installation (cont)

```

udev.x86_64          095-14.20.el5_3      ems-local
wget.x86_64          1.11.4-2.el5_4.1      ems-local
wireshark.x86_64     1.0.11-1.el5_5.5      ems-local

Hardening Linux OS for DoD STIG compliancy

>>> Enter new password for user 'acems'
Changing password for user acems.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

>>> Enter new password for user 'root'
Changing password for user root.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
+++++
EMS Server must be rebooted to proceed with the installation.

After the reboot completes, re-login to the EMS Server and
re-run the installation script to complete the installation.
+++++

Press Enter to reboot...

```

8. The installation process verifies whether CentOS 7.3 that you installed from **DVD1** includes the latest OS patch updates; do one of the following:
  - If OS patches are installed, press Enter to reboot the server.
  - If there are no OS patches to install, proceed to step [Wait for the installation to complete and reboot the OVOC server by typing `reboot`](#). below



After the OVOC server has rebooted, repeat steps [Login into the OVOC server by SSH, as 'acems' user and enter password acems \(or customer defined password\)](#). on page 74 to [Enter y](#), and then press Enter to accept the License agreement. on page 75.

Figure 9-22: OVOC server Installation Complete

```

Done
>>> .....
>>> Installation Completed, Oracle is Now Secured ...
>>> .....
>>> Remove /tmp/EmsServerInstall ...
[root@EMS-Linux145 EmsServerInstall]#

```

9. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
10. When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
11. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

12. Type the following command:

```
# EmsServerManager
```

13. Verify that all processes are up and running ([Viewing Process Statuses](#) on page 104) and verify login to the OVOC Web client is successful.
14. Verify that the Date and Time are set correctly ([Date and Time Settings](#) on page 131) to set the date and time).
15. Configure other settings as required ([Getting Started](#) on page 101).

## 10 Files Verification

You need to verify the contents of the ISO file received from AudioCodes using an MD5 checksum. As an Internet standard (RFC 1321), MD5 has been used in a wide variety of security applications, and is also commonly used to check the integrity of file, and verify download. Perform the following verifications on the relevant platform:

- Windows (see [Windows](#) below)
- Linux ( [Linux](#) below)

### Windows

Use the WinMD5 tool to calculate md5 hash or checksum for the file:

- Verify the checksum with WinMD5 (see [www.WinMD5.com](http://www.WinMD5.com))

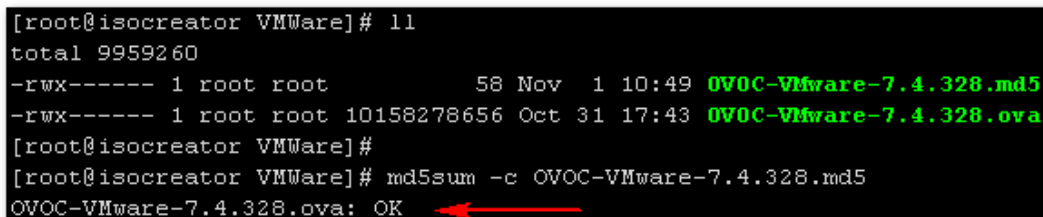
### Linux

Copy the checksum and the files to a Linux machine, and then run the following command:

```
md5sum -c filename.md5
```

The “OK” result should be displayed on the screen (see figure below).

**Figure 10-1: ISO File Integrity Verification**



```
[root@isocreator VMWare]# ll
total 9959260
-rwx----- 1 root root      58 Nov  1 10:49 OVOC-VMware-7.4.328.md5
-rwx----- 1 root root 10158278656 Oct 31 17:43 OVOC-VMware-7.4.328.ova
[root@isocreator VMWare]#
[root@isocreator VMWare]# md5sum -c OVOC-VMware-7.4.328.md5
OVOC-VMware-7.4.328.ova: OK
```

### OVOC Server Users

OVOC server OS user permissions vary according to the specific application task. This feature is designed to prevent security breaches and to ensure that a specific OS user is authorized to perform a subset of tasks on a subset of machine directories. The OVOC server includes the following OS user permissions:

- 'root' user: User permissions for installation, upgrade, maintenance using OVOC Server Manager and OVOC application execution.
- *acems* user: The **only available user** for login through SSH/SFTP tasks.
- *ovocadmin* user: User with permissions for mainly the OVOC Server Manager and OVOC application for data manipulation and database access.
- *oracle* user: User permissions for the Oracle database access for maintenance such as installation, patches upgrade, backups and other Oracle database tasks.
- *oralshr* user: User in charge of oracle listener startup.



# Part III

## OVOC Server Upgrade

This part describes the upgrade of the OVOC server on dedicated hardware and on virtual and cloud platforms.



# 11 Upgrading OVOC Server on Dedicated Hardware

This section describes the upgrade of the OVOC server on dedicated hardware. You can perform the upgrade using AudioCodes supplied **DVD3**.



- Prior to performing the upgrade, it is highly recommended to perform a complete backup of the OVOC server ([OVOC Server Backup](#) on page 98).
- If you are upgrading from Version 7.2.3000, you can optionally migrate topology to Version 7.4 and later (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center*).
- Ensure that the minimum platform requirements are met before proceeding with the upgrade (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the upgrade.
- For obtaining the installation files, see [OVOC Software Deliverables](#) on page 14. Note that you should verify the upgrade files (see [Files Verification](#) on page 72).

## Upgrading the OVOC Server-DVD

This section describes how to upgrade the OVOC server from the AudioCodes supplied installation DVD on the Linux platform.

To upgrade the OVOC server, only DVD3 is required. Verify in the EMS Manager 'General Info' screen that you have installed the latest Linux revision ([Hardware and Software Specifications](#) on page 7). If you have an older OS revision, a clean installation must be performed using all three DVDs (Installing the OVOC server on Dedicated Hardware).



Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

### ➤ To upgrade the OVOC server:

1. Insert **DVD3-OVOC Server Application Installation** into the DVD ROM.
2. Login into the OVOC server by SSH, as 'acems' user and enter password *acems* (or customer defined password).
3. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

4. Mount the CDROM to make it available (if required):

```
mount -t iso9660 /dev/sr0 /misc/cd/
```

5. Run the installation script from its location:

```
cd /misc/cd/EmsServerInstall/
```

```
./install
```

**Figure 11-1: OVOC server Upgrade (Linux)**

```
[root@EMS-Linux2 ~]# cd /misc/cd/EmsServerInstall/
[root@EMS-Linux2 EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
  >>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...
Login Check Successfully Passed.

  >>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013

...
  >>>  >>> PASSED
...
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013

...
SOFTWARE LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I
ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC
```

6. Enter **y**, and then press Enter to accept the License agreement.

**Figure 11-2: OVOC server Upgrade (Linux) – License Agreement**

```
Based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respec
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement or any of Licensee's rights or obl
tten permission of Licensor and any attempt to do so shall be without effe
sferred to any person; (ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regu
, and may require a license to export such. Licensee is solely responsible
11.7. Relationship of Parties Nothing herein shall be deemed to create an
the parties. Neither party shall have the right to bind the other to any of
11.8. Integration This Agreement is the complete and exclusive agreement b
ated hereto. Any Licensee purchase order issue for the software, documenta
erms hereof.
11.9. Counterparts This Agreement may be executed in multiple original cou
ing an authorized signature of Licensor and Licensee.

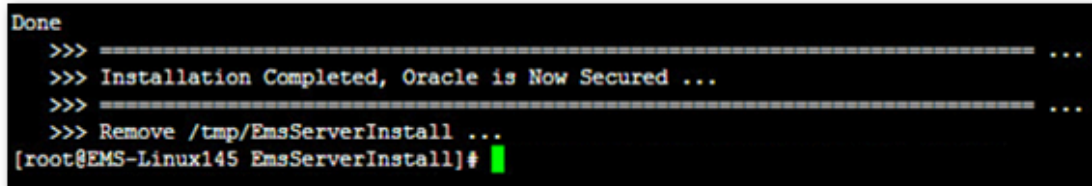
Do you accept this agreement? (y/n)y
```

7. The upgrade process verifies whether CentOS 7.3 that you installed from **DVD1** includes the latest OS patch updates; do one of the following:
  - If OS patches are installed, press Enter to reboot the server.



After the OVOC server has rebooted, repeat steps 2-7 (inclusive).

- If OS patches are not installed, proceed to step [Wait for the installation to complete and reboot the OVOC server by typing reboot.](#) on the next page

**Figure 11-3: OVOC server Installation Complete**


```

Done
>>> ===== ...
>>> Installation Completed, Oracle is Now Secured ...
>>> ===== ...
>>> Remove /tmp/EmsServerInstall ...
[root@EMS-Linux145 EmsServerInstall]#

```

8. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
9. When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
10. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

11. Type the following command:

```
# EmsServerManager
```

12. Verify that all processes are up and running ([Viewing Process Statuses](#) on page 104) and verify login to OVOC Web client is successful.
13. Verify that the Date and Time are set correctly (see [Date and Time](#) on page 133 to set the date and time).
14. Set the OVOC server network IP address as described in [Server IP Address](#) on page 117.
15. Configure other settings as required ([Getting Started](#) on page 101).



For Statistics Reports: each time the OVOC server version is upgraded, the operator should perform CTRL – F5 (refresh) action on the Statistics Report Page, and then re-login to the application.

## Upgrading the OVOC Server using an ISO File

This section describes how to upgrade the OVOC server using an ISO file. Before performing this procedure, you need to verify the ISO file contents ([Linux](#) on page 72).

### ➤ To upgrade using an ISO file:

1. Login into the OVOC server by SSH, as 'acems' user and enter password *acems* (or customer defined password).
2. Use SFTP or SCP to copy the ISO file to /home/acems in the server.
3. Replace "7.6.xxx" in the filename with the relevant version in two of the following commands.

```
mkdir /ins
cp ~/acems/DVD3_EMS_7.6.xxx.iso /ins
mkdir /tmp/cd
```

4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Specify the following commands:

```

umount -l /tmp/cd
mount -t iso9660 -o loop,ro /ins/DVD3_EMS_7.6.xxx.iso /tmp/cd
cd /tmp/cd/EmsServerInstall

```

6. Run the installation script from its location:

```
./install
```

Figure 11-4: OVOC server Upgrade (Linux)

```

[root@EMS-Linux2 EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
>>> Start executing User Login Check script at Wed Jun 12 12:24:42 BST 2013 ...
Login Check Successfully Passed.

>>> Check CD Sequence - Wed Jun 12 12:24:42 BST 2013

...
>>> >>> PASSED
...
>>> Verifying OS version - Wed Jun 12 12:24:42 BST 2013

...
SOFTWARE LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I
ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (N
CEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND
OF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AG
PRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF THIS LIC

```

7. Enter **y**, and then press Enter to accept the License agreement.

Figure 11-5: OVOC server Upgrade (Linux) – License Agreement

```

Based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement or any of Licensee's rights or obl
tten permission of Licensor and any attempt to do so shall be without effe
sferred to any person; (ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regu
, and may require a license to export such. Licensee is solely responsible
11.7. Relationship of Parties Nothing herein shall be deemed to create an
the parties. Neither party shall have the right to bind the other to any o
11.8. Integration This Agreement is the complete and exclusive agreement b
ated hereto. Any Licensee purchase order issue for the software, documenta
erms hereof.
11.9. Counterparts This Agreement may be executed in multiple original cou
ing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y

```

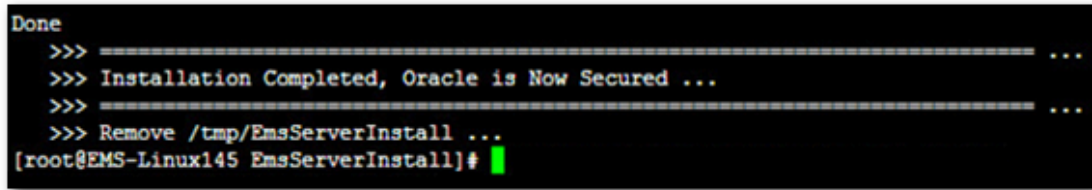
8. The upgrade process verifies whether CentOS 7.3 that you installed from **DVD1** includes the latest OS patch updates; do one of the following:
  - If OS patches are installed, press Enter to reboot the server.



After the OVOC server has rebooted, repeat steps 4-8 (inclusive).

- If OS patches are not installed, proceed to step [Wait for the installation to complete and reboot the OVOC server by typing reboot.](#) below.

**Figure 11-6: OVOC server Installation Complete**

A terminal window showing the completion of the OVOC server installation. The text displayed is: Done, followed by three lines of progress bars (each starting with >>> and ending with ...). The second line says "Installation Completed, Oracle is Now Secured ...". The third line says "Remove /tmp/EmsServerInstall ...". The prompt is [root@EMS-Linux145 EmsServerInstall]#.

```
Done
>>> .....
>>> Installation Completed, Oracle is Now Secured ...
>>> .....
>>> Remove /tmp/EmsServerInstall ...
[root@EMS-Linux145 EmsServerInstall]#
```

9. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
10. When the OVOC server has successfully restarted, login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
11. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

12. Type the following command:

```
# EmsServerManager
```

13. Verify that all processes are up and running ([Viewing Process Statuses](#) on page 104) and verify login to OVOC Web client is successful.
14. Verify that the Date and Time are set correctly (see [Date and Time](#) on page 133 to set the date and time).
15. Set the OVOC server network IP address as described in [Server IP Address](#) on page 117.
16. Configure other settings as required ([Getting Started](#) on page 101).



For Statistics Reports: each time the OVOC server version is upgraded, the operator should perform CTRL – F5 (refresh) action on the Statistics Report Page, and then re-login to the application.

## 12 Upgrading OVOC Server on a Virtual Platform

The upgrade of the OVOC server involves the following steps:

- **Step 1:** Setup the Virtual Machine ( [Step 1: Setup the Virtual Machine](#) below)
- **Step 2:** Run the upgrade script ( [Step 2: Run the Upgrade Script](#) on page 90)
- **Step 3:** Connect the OVOC server to the network ( [Step 3: Connect the OVOC Server to Network](#) on page 91)

You can perform the upgrade using AudioCodes supplied **DVD3**.



- Prior to performing the upgrade, it is highly recommended to perform a complete backup of the OVOC server ([OVOC Server Backup](#) on page 98).
- If you are upgrading from Version 7.2.3000, you can optionally migrate topology to Version 7.4 and later (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center*).
- Ensure that the minimum platform requirements are met (see [Hardware and Software Specifications](#) on page 7). Failure to meet these requirements will lead to the aborting of the upgrade.
- For obtaining the installation files, see [OVOC Software Deliverables](#) on page 14. Note that you should verify the upgrade files (see [Files Verification](#) on page 72).

### Step 1: Setup the Virtual Machine

This section describes how to setup the virtual machine before you run the upgrade script.

- [Setting up Using VMware Server Host for Upgrade](#) on page 85
- [Setting Up Microsoft Hyper-V Platform for Upgrade](#) on page 86

### Setting up VMware Platform for Upgrade

The upgrade on the VMware platform can be run using either the Upgrade media CD/DVD or ISO file using either the VMware Remote Console Application (VMRC) or the VMware Server Host.

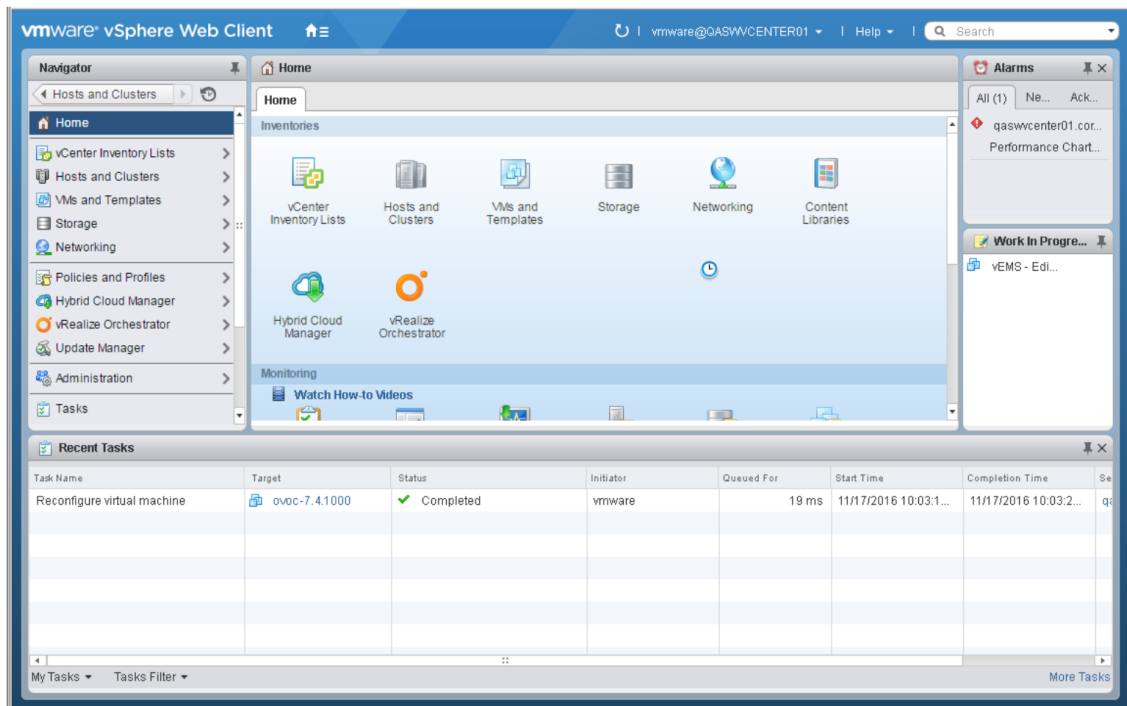


- A remote connection to the VMware host is established using the VMware Remote Console application (VMRC). You must download this application or use a pre-installed remote connection client to connect to the remote host.
- The procedures below show screen examples of the vSphere Web Client. However, refer to the VMware documentation for more information.

#### ➤ To setup the VMware machine:

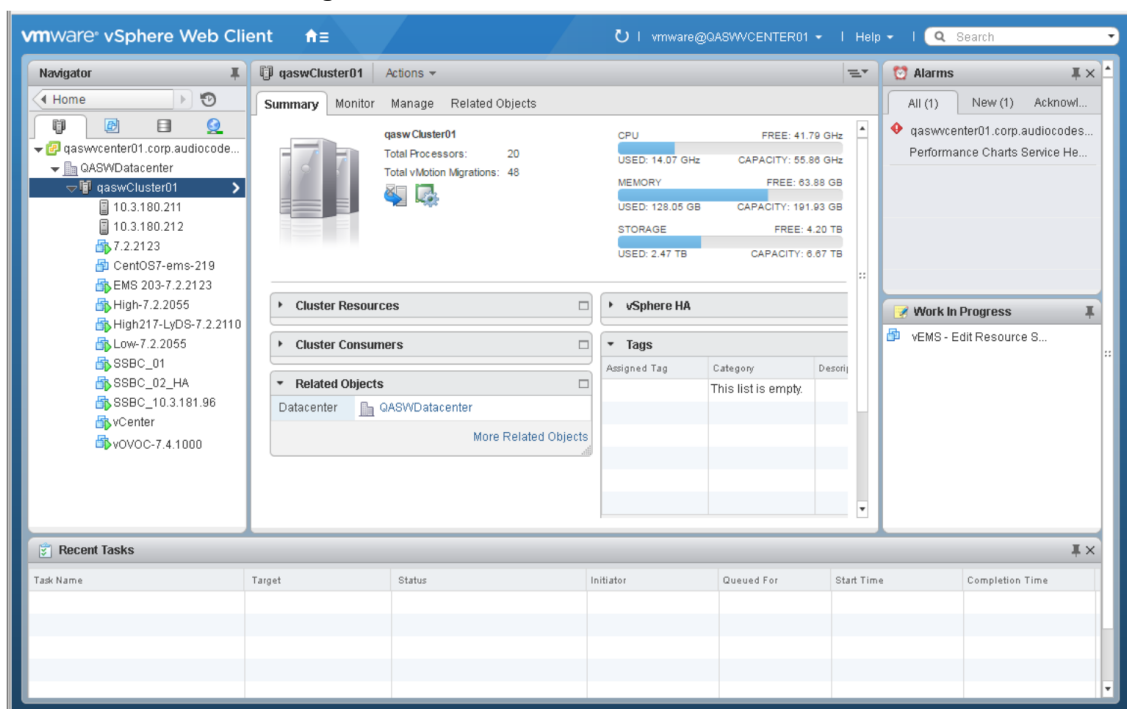
1. Transfer the OVA file containing the VMware Virtual Machine installation package from **DVD3-OVOC server Application Installation** to your PC (see Appendix [Transferring Files](#) on page 200 for instructions on how to transfer files).
2. Login to the VMware vSphere Web client.

Figure 12-1: VMware vSphere Web Client

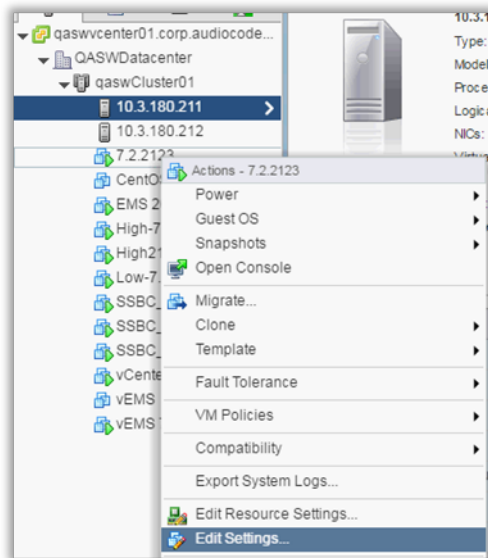


3. In the vCenter Navigator, select **Hosts and Clusters**. A list of Hosts and Clusters is displayed.

Figure 12-2: Hosts and Clusters

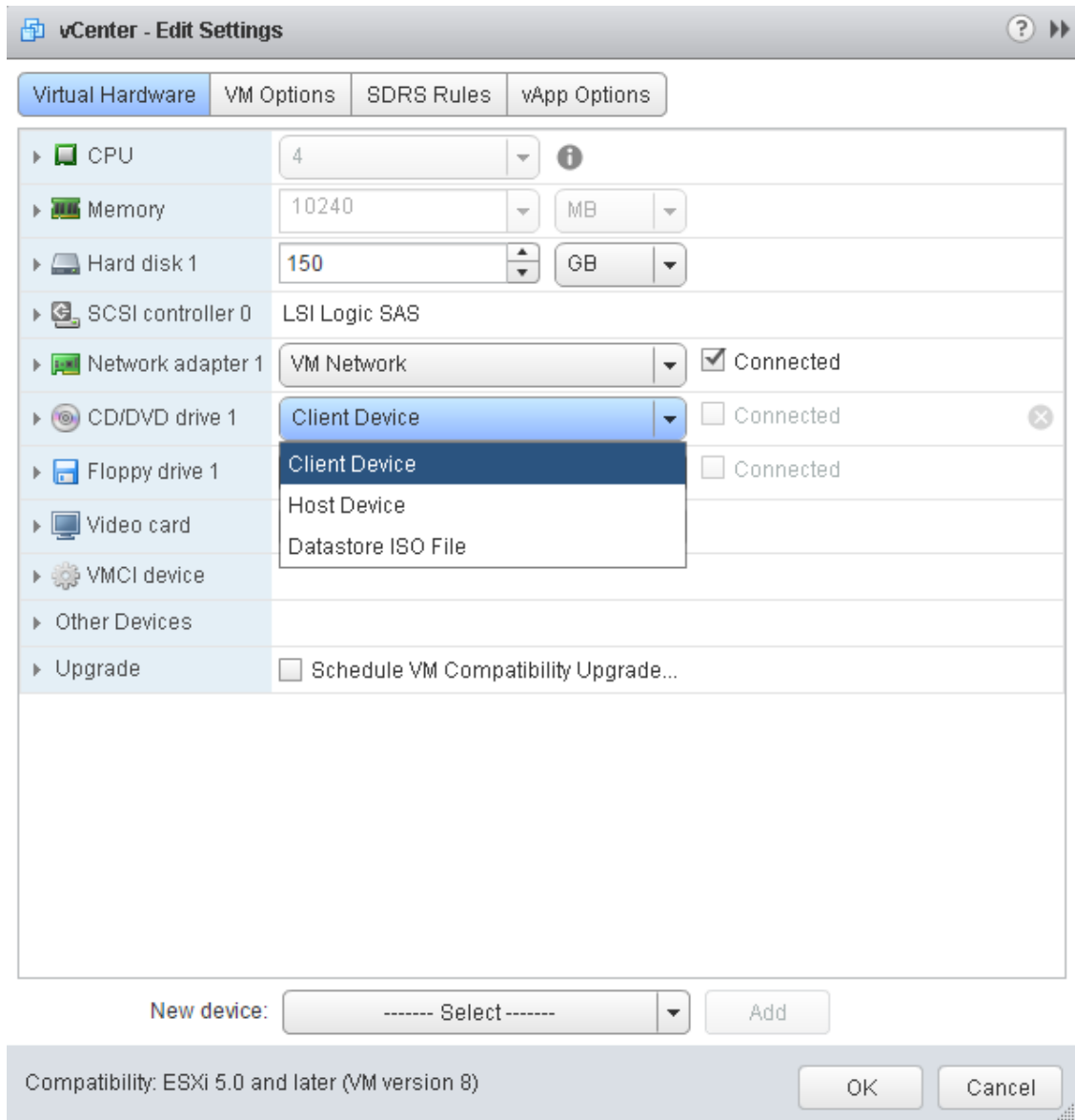


4. Right-click the AudioCodes OVOC node that you wish to upgrade and choose the **Edit Settings** option.

**Figure 12-3: Edit Settings Option**

The vCenter Edit Settings screen is displayed.



**Figure 12-4: Connection Options**

5. In the **Virtual Hardware** tab, select the CD/DVD drive item, and from the drop-down list, select the relevant option according to where you placed the Upgrade Media (CD/DVD or ISO image file):
  - **Client Device:** This option enables you to run the upgrade from the PC running the remote console ([Setting up Using VMware Remote Console Application \(VMRC\)](#) below).
  - **Host Device:** This option enables you to run the upgrade from the CD/DVD drive of the VMware server host ( 13.1.1.2 Setting up Using VMware Server Host).
  - **Datastore ISO file:** This option enables you to run the upgrade from the image file on the storage device of the VMware server host. When you choose this option, browse to the location of the ISO file on the VMware storage device ( 13.1.1.2 Setting up Using VMware Server Host).

### Setting up Using VMware Remote Console Application (VMRC)

This section describes how to run the upgrade from the VMware host. This procedure requires connecting to the VMware host using the VMware Remote Console application (VMRC).

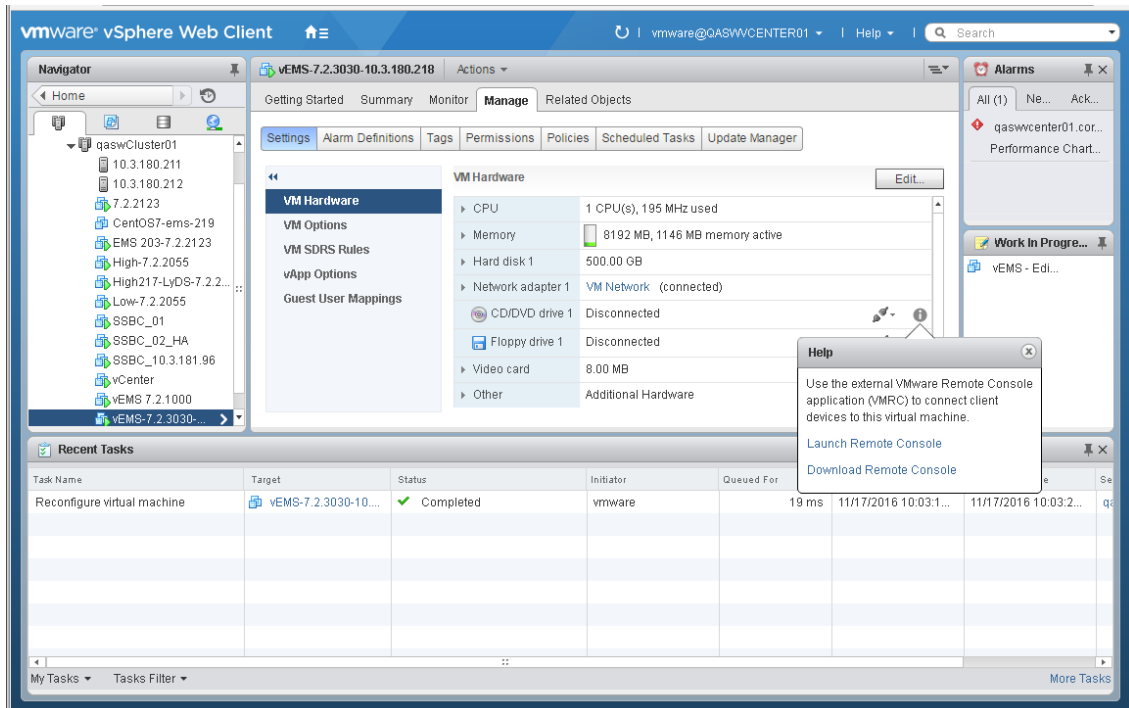
➤ **To run the upgrade using VMRC:**

1. In the **Manage** tab under **Settings> VM Hardware**, select the Help icon adjacent to the CD/DVD drive item and then from the pop-up, click the **Launch Remote Console** to launch the VMware Remote Console application (VMRC). If necessary, click the **Download Remote Console** link to download this application.

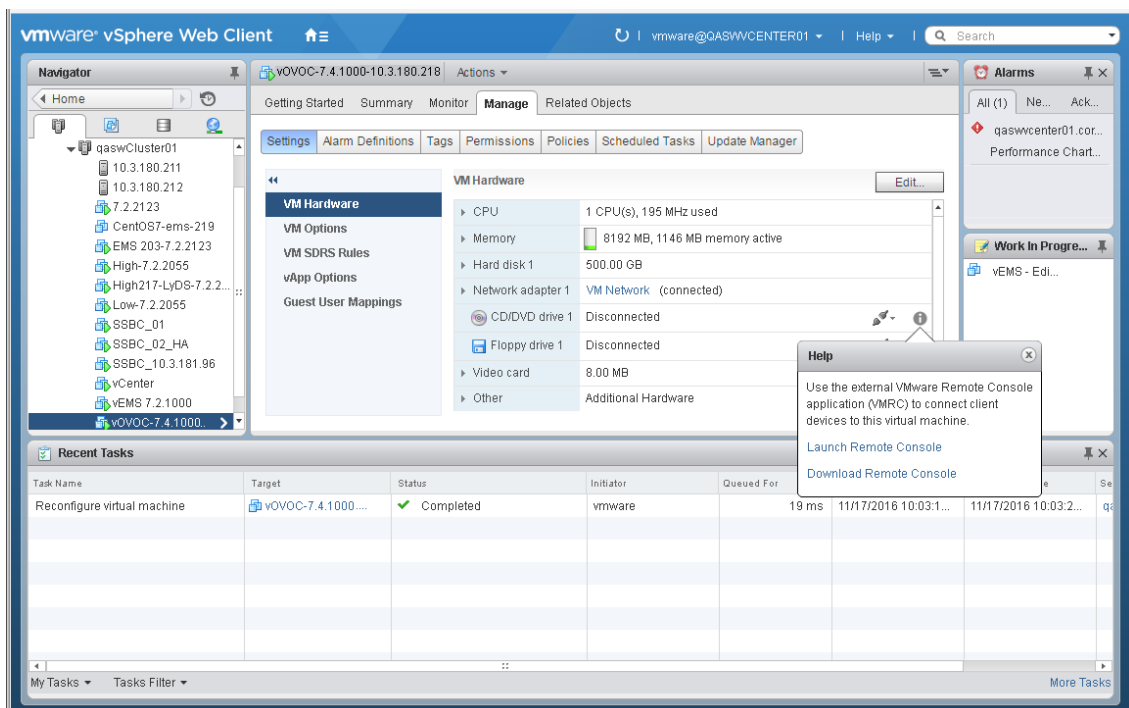


If you already have a remote console application installed on your machine, you can use your pre-installed application.

**Figure 12-5: Help Link to Launch Remote Console**

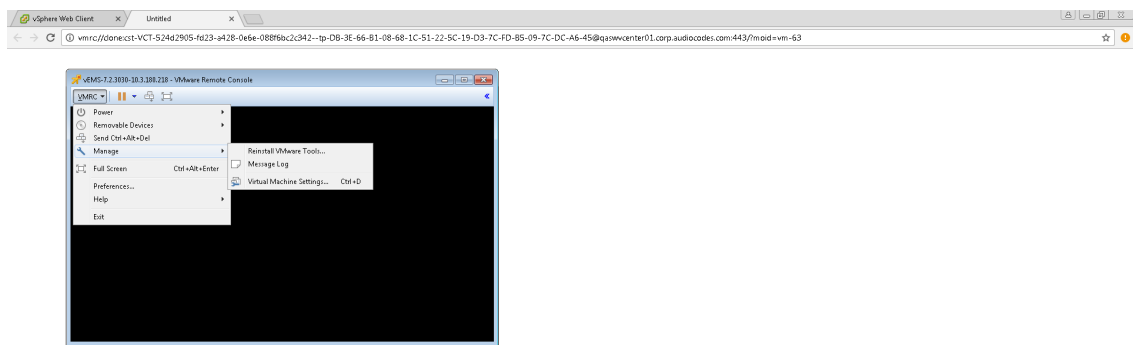


**Figure 12-6: VMware Web Client**



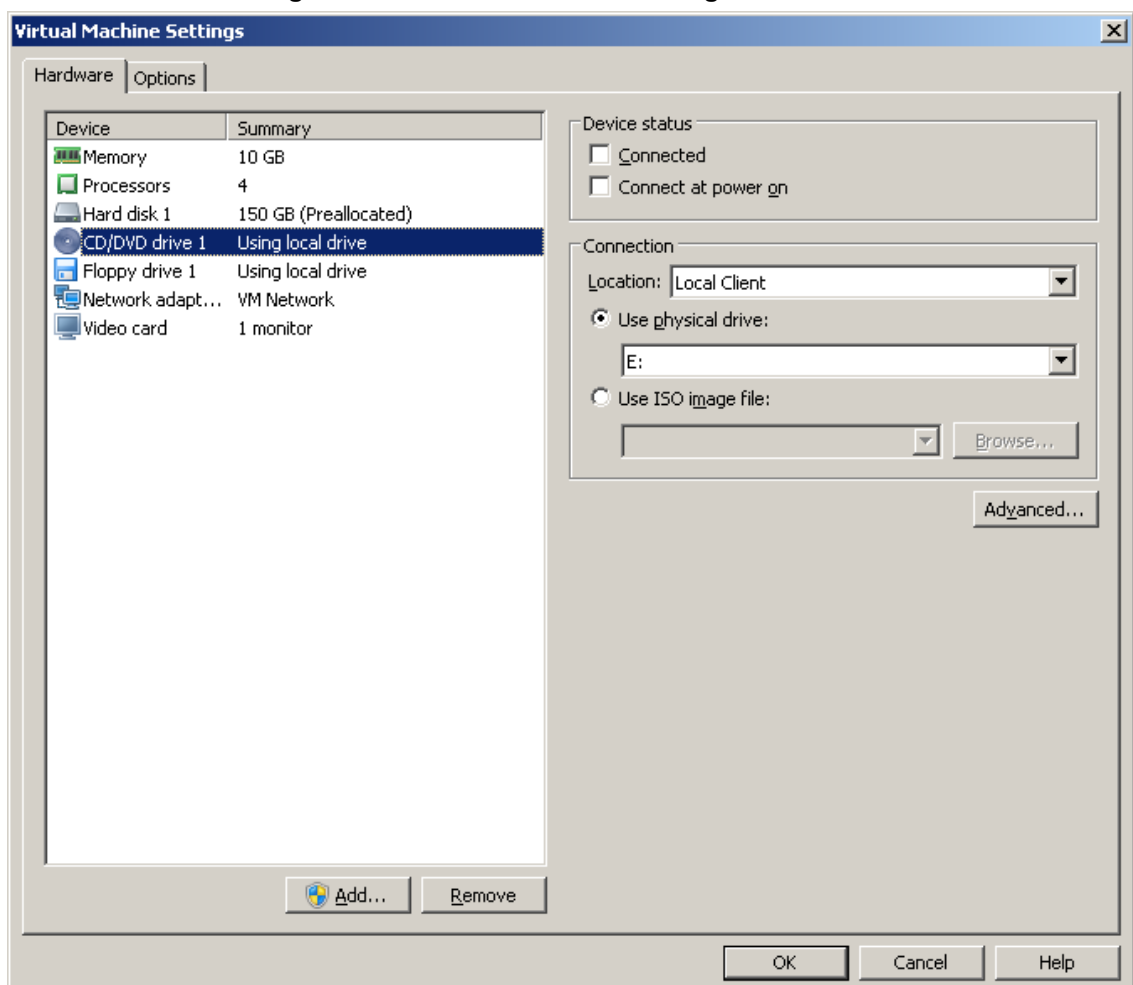
The remote console application is displayed.

**Figure 12-7: Remote Console Application**



- In the toolbar, from the VMRC drop-down list, choose **Manage > Virtual Machine Settings**. The Virtual Machine Settings screen is displayed:

**Figure 12-8: Virtual Machine Settings**



- From the Location drop-down list, select **Local Client**.

4. Select the CD/DVD drive item and then choose one of the following:
  - Use physical drive: from the drop-down list, select the CD/DVD drive where you placed the Upgrade media.
  - Use ISO image file: browse to the location of the ISO image file.
5. Click **OK**.

## Setting up Using VMware Server Host for Upgrade

This section describes how to run the upgrade using the VMware server host.

### ➤ To run the upgrade using the VMware Server host:

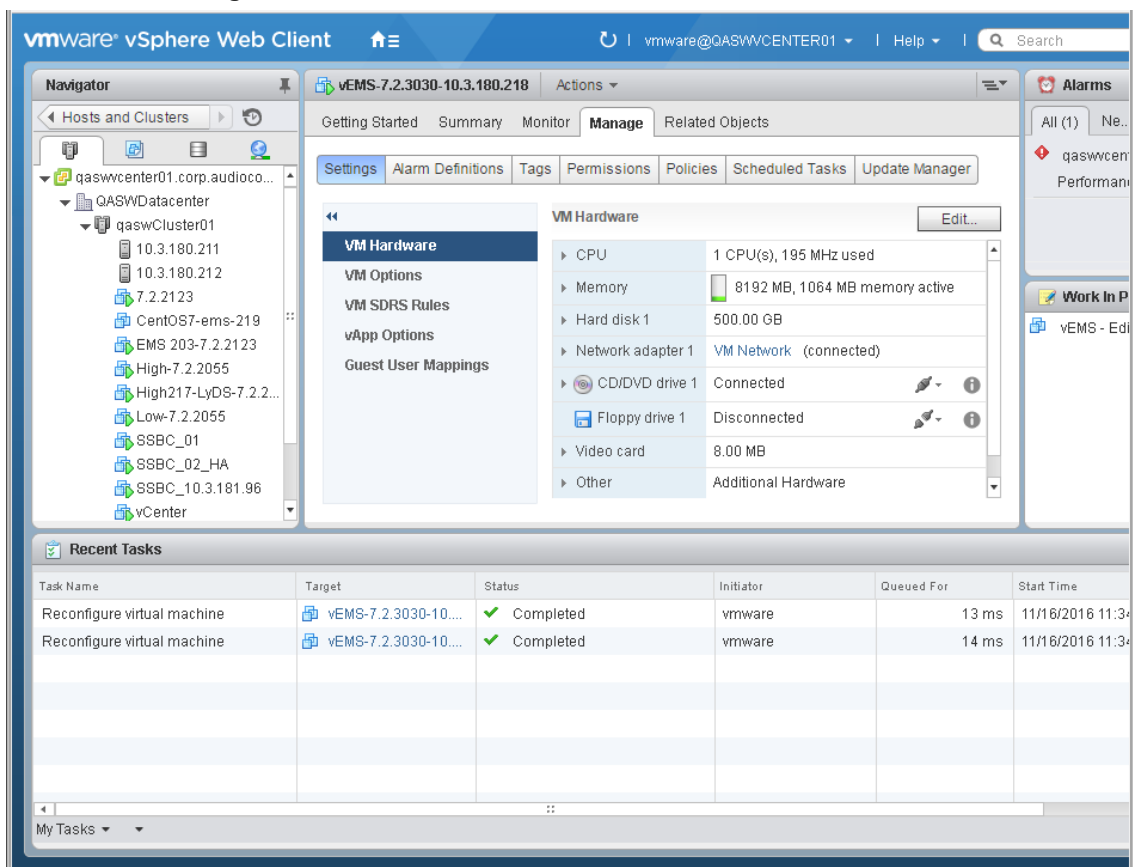
1. Select the **Manage** tab, right-click the Connect icon and select one of the following options:
  - Connect to host CD device
  - Connect to CD/DVD image on a datastore

**Figure 12-9: Connect to Host CD Device/ Datastore ISO file**



2. Wait until the machine reconfiguration has completed, and then verify that the 'Connected' status is displayed:

**Figure 12-10: CD/DVD Drive - Connected Status**



## Setting Up Microsoft Hyper-V Platform for Upgrade

This section describes how to upgrade the OVOC server on the Microsoft Hyper-V Server 2012 R2 platform. This procedure takes approximately 30 minutes and predominantly depends on the hardware machine where the Microsoft Hyper-V platform is installed.

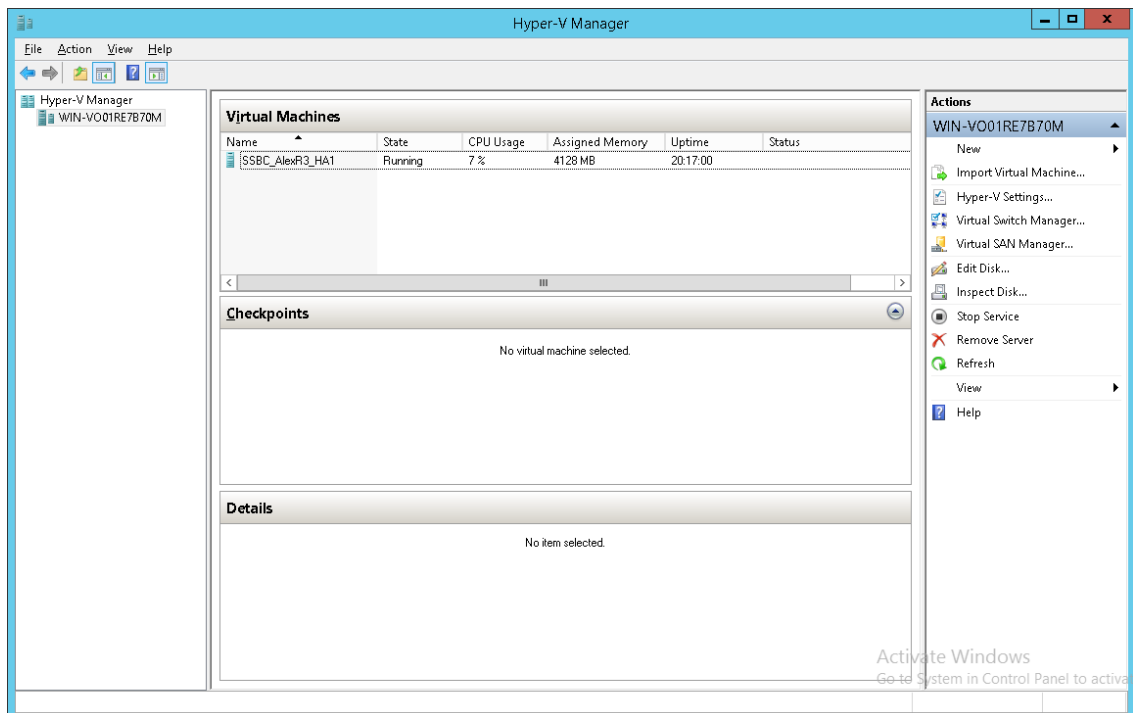
The upgrade of the OVOC server on Microsoft Hyper-V includes the following procedures:

- Upgrade the Virtual Machine (VM) (Installing the Microsoft Hyper-V Virtual Machine).
- Configure the Virtual machine hardware settings ([Configuring the Virtual Machine Hardware Settings](#) on page 39).
- Change MAC addresses from 'Dynamic' to 'Static' ([Changing MAC Addresses from 'Dynamic' to 'Static'](#) on page 45).

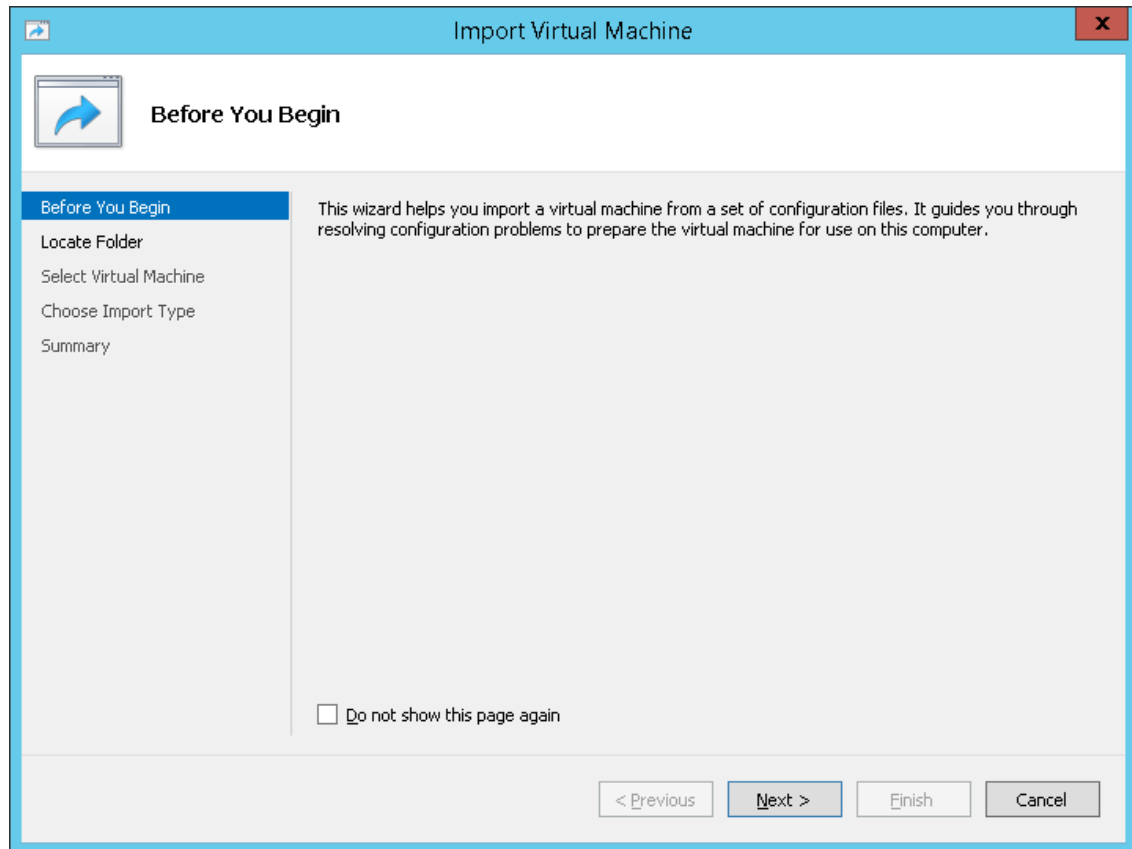
### ➤ To setup the Microsoft Hyper-V machine:

1. Transfer the ZIP file containing the Microsoft Hyper-V Virtual Machine installation package from the AudioCodes **DVD3-OVOC server Application Installation** to your PC (see [Appendix Transferring Files](#) on page 200 for instructions on how to transfer files).
2. Open Hyper-V Manager by clicking **Start > Administrative Tools > Hyper-V Manager**; the following screen opens:

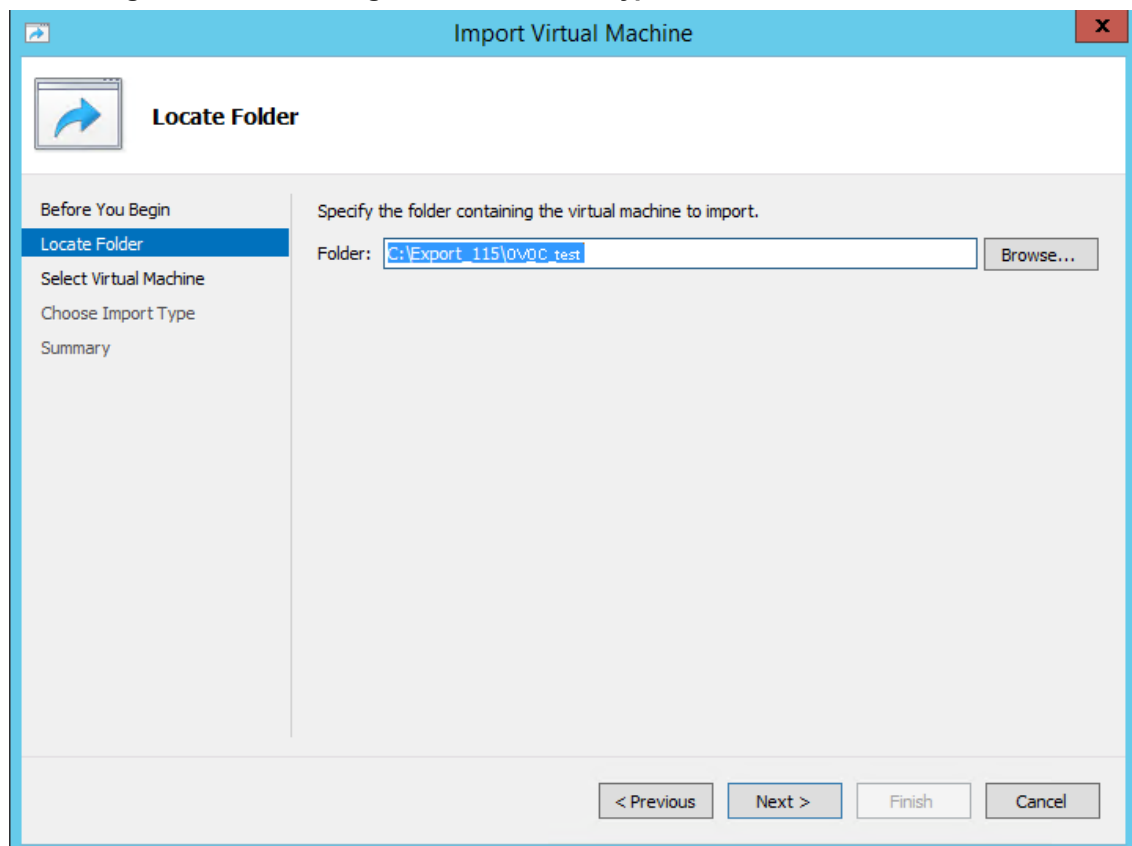
**Figure 12-11: Installing the OVOC server on Hyper-V – Hyper-V Manager**



3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

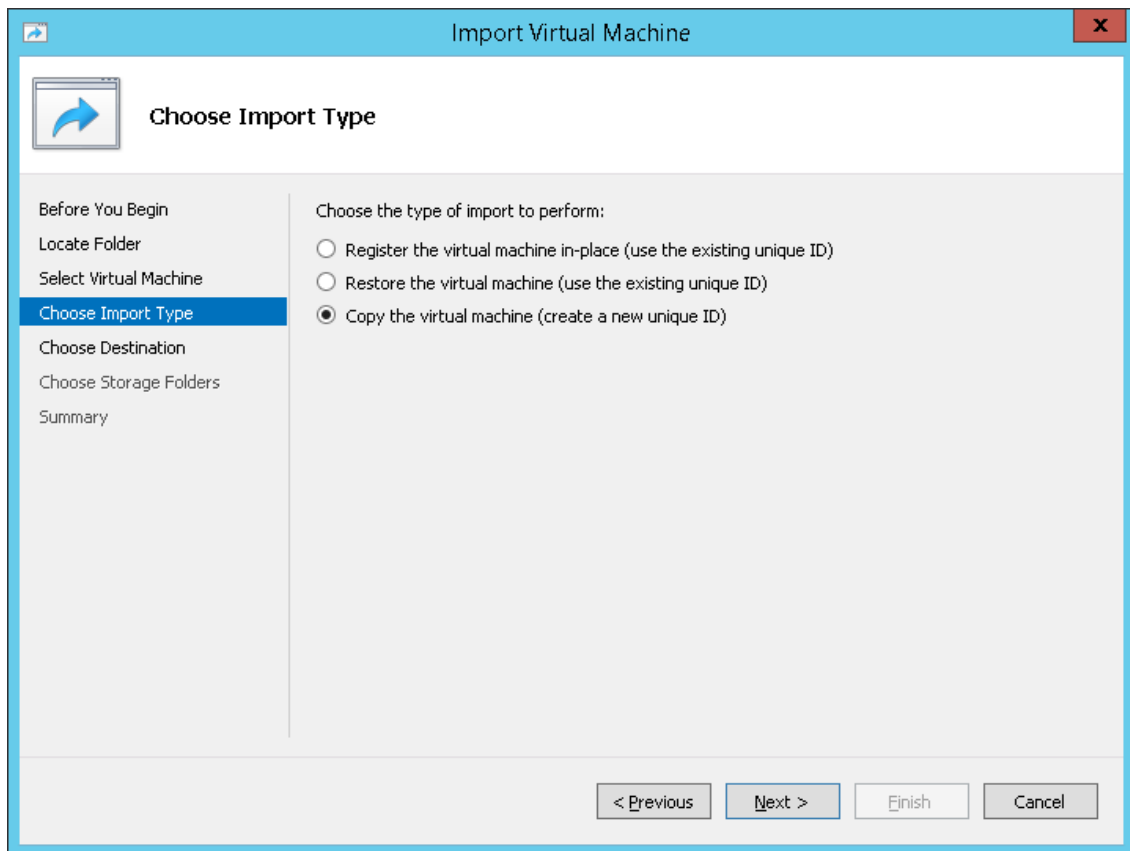
**Figure 12-12: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard**

4. Click **Next**; the Locate Folder screen opens:

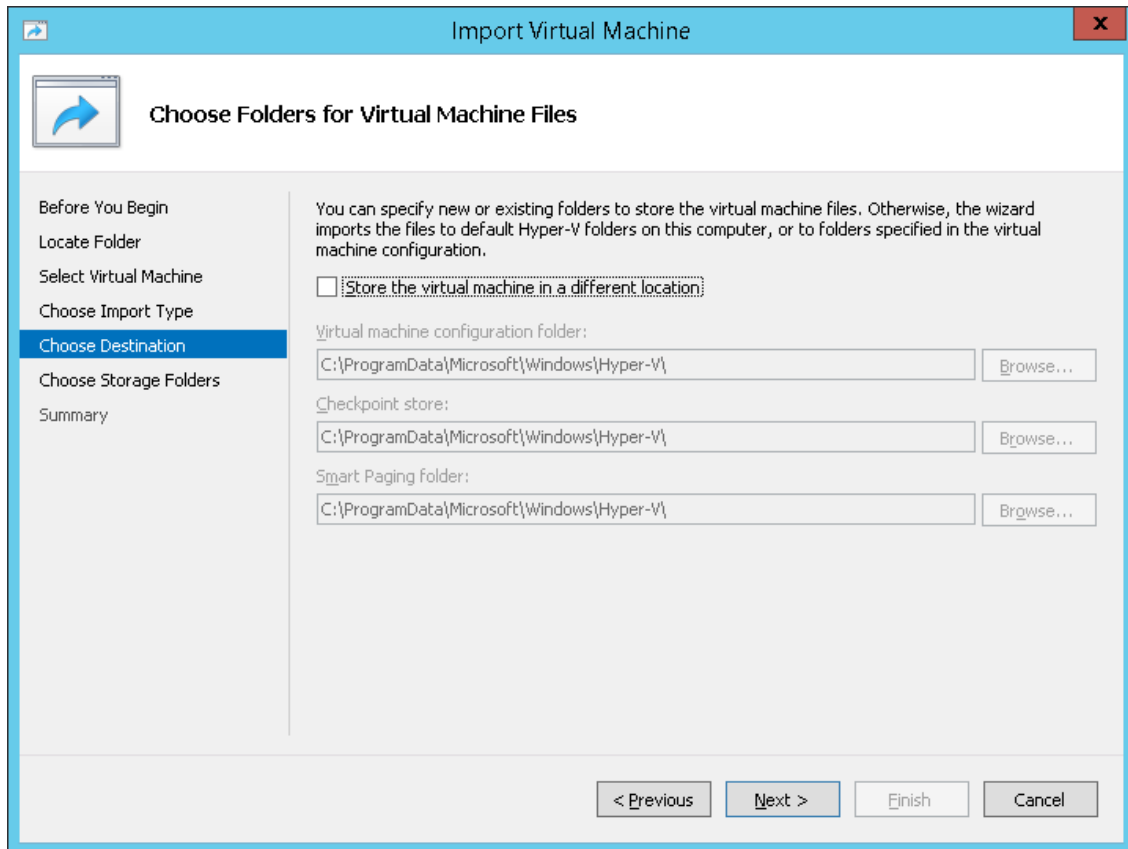
**Figure 12-13: Installing OVOC server on Hyper-V – Locate Folder**

5. Enter the location of the VM installation folder, which was previously extracted, from the zip file as shown in the figure above, and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

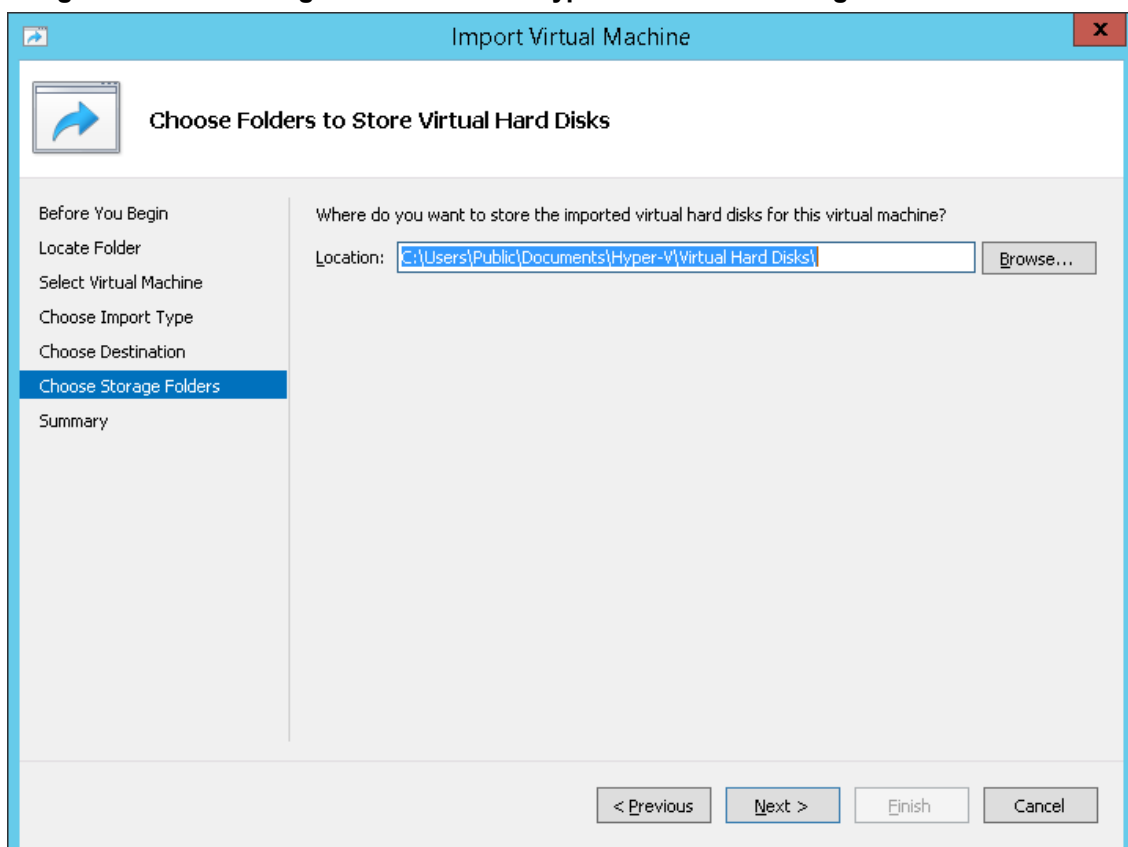
**Figure 12-14: Installing OVOC server on Hyper-V – Choose Import Type**



7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

**Figure 12-15: Installing OVOC server on Hyper-V – Choose Destination**

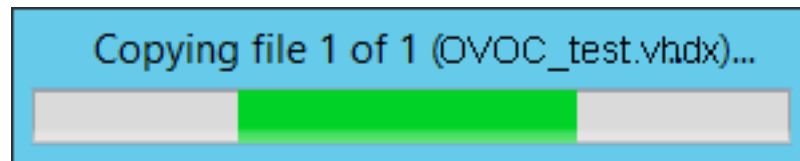
8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

**Figure 12-16: Installing OVOC server on Hyper-V – Choose Storage Folders**



9. Select the Storage Folder for the Virtual Hard Disk, and then click **Next**; the Summary screen opens.
10. Click **Finish** to start the creation of the VM; a similar installation progress indicator is shown:

Figure 12-17: File Copy Progress Bar



This step may take approximately 30 minutes to complete.

## Step 2: Run the Upgrade Script

Once you have setup the virtual machines, you can run the upgrade script.



Before starting the installation, it is highly recommended to configure the SSH client (e.g. Putty application) to save the session output into a log file.

### ➤ To run the upgrade:

1. Open an SSH connection or the VM console.
2. Login into the OVOC server as 'acems' user with password *acems* (or customer defined password).
3. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

4. Mount the CDROM to make it available:

```
mount -t iso9660 /dev/sr0 /mnt
cd /mnt/EmsServerInstall/
```

5. Run the installation script from its location:

```
./install
```

Figure 12-18: OVOC server Installation Script

```
[root@ems-server ~]#
[root@ems-server ~]# cd /misc/cd/EmsServerInstall/
[root@ems-server EmsServerInstall]#
[root@ems-server EmsServerInstall]# ./install
DIR Name /misc/cd/EmsServerInstall
Start installValues
>>> Start executing User Login Check script at Mon May 21 08:29:59 BST 2012 ...
Login Check Successfully Passed.

>>> Check CD Sequence - Mon May 21 08:29:59 BST 2012
...
>>> >>> PASSED
...
>>> Verifying OS version - Mon May 21 08:29:59 BST 2012
...
SOFTWARE EVALUATION LICENSE AGREEMENT
YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS SOFTWARE
EVALUATION AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE
AGREEMENT FOR THE AUDIOCODES SOFTWARE (THE "PROGRAM") AND
THE ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE
```

6. Enter **y**, and then press Enter to accept the License agreement.

**Figure 12-19: OVOC server Upgrade (Linux) – License Agreement**

```

Based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respect,
on shall be limited only so far as it is necessary to allow conformance to
shall be deleted from the Agreement, but the remaining provisions shall remain
11.5. Assignment Neither this Agreement or any of Licensee's rights or obligations
without permission of Licensor and any attempt to do so shall be without effect
transferred to any person; (ii) the Licensee being merged or consolidated with
11.6. Export Licensee understands that the Licensed Software may be a regulated
, and may require a license to export such. Licensee is solely responsible for
11.7. Relationship of Parties Nothing herein shall be deemed to create an agency
the parties. Neither party shall have the right to bind the other to any of its
11.8. Integration This Agreement is the complete and exclusive agreement between
ated hereto. Any Licensee purchase order issue for the software, documentation
terms hereof.
11.9. Counterparts This Agreement may be executed in multiple original copies
ing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y

```

7. The upgrade process verifies whether CentOS 7.3 that you installed from **DVD1** includes the latest OS patch updates; do one of the following:
  - If OS patches are installed, press Enter to reboot the server.
  - If OS patches are not installed, proceed to step [Wait for the installation to complete and reboot the OVOC server by typing \*\*reboot\*\*](#). below.



After the OVOC server has rebooted, repeat steps [Login into the OVOC server as 'acems' user with password acems \(or customer defined password\)](#). on the previous page to [Enter y](#), and then press Enter to accept the License agreement. on the previous page.

**Figure 12-20: OVOC server Installation Complete**

```

Done
>>> ===== ...
>>> Installation Completed, Oracle is Now Secured ...
>>> ===== ...
>>> Remove /tmp/EmsServerInstall ...
[root@EMS-Linux145 EmsServerInstall]#

```

8. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.

## Step 3: Connect the OVOC Server to Network

After installation, the OVOC server is assigned a default IP address that will most likely be inaccessible from the customer's network. This address is assigned to the first virtual network interface card connected to the 'trusted' virtual network switch during the OVOC server installation. You need to change this IP address to suit your IP addressing scheme.

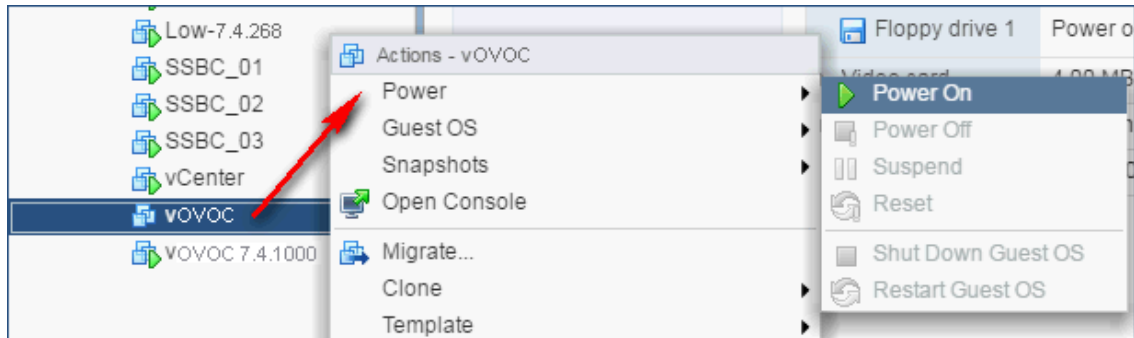
### VMware Platform

This section describes how to assign the OVOC server IP address to the network on the VMware platform.

➤ **To assign the OVOC server IP address:**

1. Power on the machine; in the vCenter tree, right-click the AudioCodes One Voice Operations Center node (vOC) and in the drop-down menu, choose **Power > Power On**. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications ([Hardware and Software Specifications](#) on page 7).

**Figure 12-21: Power On**



2. Wait until the boot process has completed, and then connect the running server through the vSphere client console.
3. Login into the OVOC server by SSH, as 'acems' user and enter *acems* password.
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Type the following command:

```
# EmsServerManager
```

6. Verify that all processes are up and running ([Viewing Process Statuses](#) on page 104) and verify login to OVOC Web client is successful.
7. Verify that the Date and Time are set correctly ([Date and Time](#) on page 133 to set the date and time).
8. Set the OVOC server network IP address as described in [Server IP Address](#) on page 117.
9. Configure other settings as required (see [Getting Started](#) on page 101).

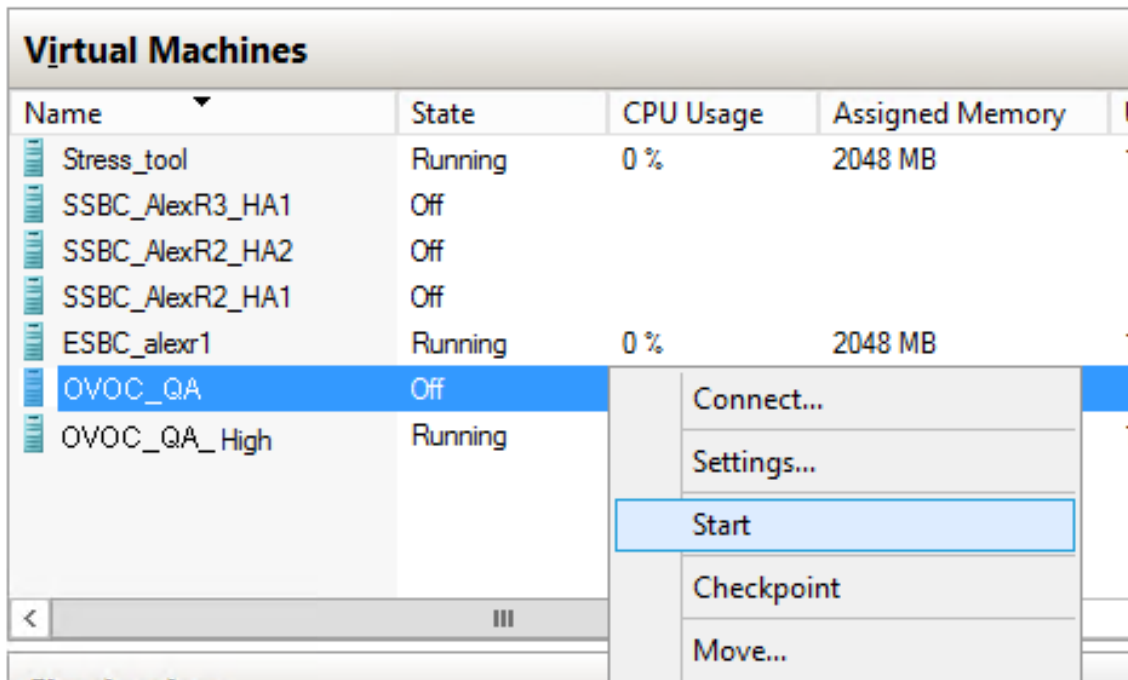
## Hyper-V Platform

This section describes how to assign the OVOC server IP address to the network on the Hyper-V platform.

➤ **To assign the OVOC server IP address:**

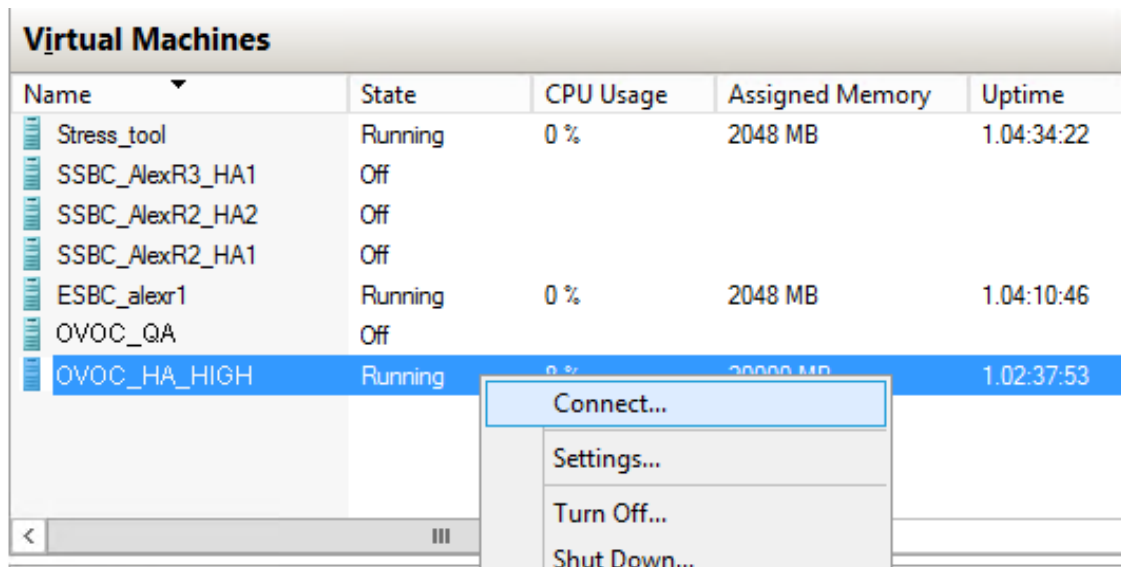
1. Start the OVOC server virtual machine, on the Hyper-V tree, right-click the OVOC server, and then in the drop-down menu, choose **Start**.

Figure 12-22: Power On Virtual Machine



2. Connect to the console of the running server by right-clicking the OVOC server virtual machine, and then in the drop-down menu, choose **Connect**.

Figure 12-23: Connect to OVOC server Console



3. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Type the following command:

```
# EmsServerManager
```

6. Verify that all processes are up and running ([Viewing Process Statuses](#) on page 104) and verify login to OVOC Web client is successful.

7. Verify that the Date and Time are set correctly (see [Date and Time](#) on page 133 to set the date and time).
8. Set the OVOC server network IP address as described in [Server IP Address](#) on page 117.
9. Configure other settings as required ([Getting Started](#) on page 101).

## 13 Installation and Upgrade Troubleshooting of the Operational Environment

This section describes the different scenarios for troubleshooting the operational environment.

- If you attempted to upgrade and your system did not meet the minimum hardware requirements, the following message is displayed:

**Figure 13-1: Minimum Hardware Requirements Upgrade**

```
>>> Checking the operational environment
...
>>> Checking hardware spec - Tue Feb  5 13:14:36 IST 2019
...
*****
ERROR: Your system does not meet the minimal requirements for VM
  Minimal requirements: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
  Actual setup:         CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB
*****
+++++
FATAL ERROR: Could not install the application - the system does not meet minimal hardware requirements
+++++
```

- If the OVOC server hardware configuration is changed and then the server is restarted, the following message is displayed in the /var/log/ems/nohup.out file.

**Figure 13-2: Minimum Hardware Requirements System Error**

```
05 Feb 2019 13:12:13 Checking the system spec...
*****
ERROR: Your system does not meet the minimal requirements for VM
  Minimal requirements: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
  Actual setup:         CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB
  Unable to start application
*****
█
```

- Whenever an upgrade or clean installation is performed and the user then later changes the hardware settings, which results in the minimum requirements not being met, the following message is displayed in the OVOC Server ManagerStatus screen :

**Figure 13-3: Status Screen Error**

```
-----Application-----|---Status---
| Watchdog                | DOWN
| OVOC Server              | DOWN
| SEM CPEs Server          | DOWN
| SEM MS Lync Server        | DOWN
| SEM Endpoints Server      | DOWN
| Floating License Server   | DOWN
| Pref Monitoring Server    | DOWN
| Tomcat Server            | DOWN
| Apache HTTP Server        | DOWN
| Oracle DB                | UP
| Oracle Listener          | UP
| Cassandra                | DOWN
| SNMP Agent               | DOWN
| NTP Daemon               | UP
|-----|-----
Your system does not meet the minimal requirements for VM
Minimal requirements: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
Actual setup:         CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB

Press 'Enter' key to go back to the main menu...█
```

- Whenever an upgrade or clean installation is performed and the user then later changes the hardware settings, which results in the minimum requirements not being met, the following is displayed in the OVOC Server Manager General Info screen:

Figure 13-4: General Info Minimum Requirements

```
Collecting information...

Machine information
|Environment: Virtual(Manufacturer: VMware, Inc.)
|Product Name: VMware Virtual Platform
|Spec: Minimal system requirements not met. See Status screen for more details.
|CPU: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz, total cores: 1
|Memory: 14877 MB
|Network:
  VMware VMXNET3 Ethernet Controller (rev 01)
|ACEMS Usage: 11G
|Disk:


| NAME       | MOUNTPOINT | SIZE  | FSTYPE      | TYPE | STATE   | VENDOR    |
|------------|------------|-------|-------------|------|---------|-----------|
| fd0        |            | 4K    |             | disk |         |           |
| sda        |            | 500G  |             | disk | running | VMware    |
| -sda1      |            | 2G    | xfs         | part |         |           |
| ~ -sda2    |            | 498G  | LVM2_member | part |         |           |
| -vg-root   | /          | 20G   | xfs         | lvm  | running |           |
| -vg-swap   | [SWAP]     | 7.8G  | swap        | lvm  | running |           |
| -vg-data   | /data      | 254G  | xfs         | lvm  | running |           |
| -vg-meta   | /meta      | 512M  | xfs         | lvm  | running |           |
| -vg-opt    | /opt       | 20G   | xfs         | lvm  | running |           |
| -vg-oracle | /oracle    | 25G   | xfs         | lvm  | running |           |
| -vg-var    | /var       | 20G   | xfs         | lvm  | running |           |
| ~ -vg-home | /home      | 150G  | xfs         | lvm  | running |           |
| sr0        |            | 1024M |             | rom  | running | NECVMMWar |
| loop0      | /misc/cd   | 2.1G  | iso9660     | loop |         |           |


|Data usage:
/dev/mapper/vg-data 254G 179G 76G 71% /data
10.3.180.50:/data1/7.6.1000/DVD3/7.6.1082 459G 281G 155G 65% /ins
-----
Versions
|OVOC Version : 7.6.1075
|OS Version : Linux 3.10.0-957.1.3.el7.x86_64 x86_64
|OS Revision : CentOS 7 for EMS Server (Rev. 18)
|Java Version : java full version "1.8.0_201-b09"
|Apache version : Apache/2.4.6 (CentOS) Server built: Nov 5 2018 01:47:09
|Cassandra version: 3.11.2
```

# Part IV

## OVOC Server Machine Backup and Restore

This part describes how to restore the OVOC server machine from a backup.



## 14 OVOC Server Backup

There are two main backup processes that run on the OVOC server:

- **Weekly backup:** runs once a week at a pre-configured date & time (default is Saturday 02:00). In this process, the whole database is backed up into several “RMAN” files that are located in /data/NBIF/EMSBackup/RmanBackup directory. In addition, many other configuration and software files are backed up to a TAR file in the /data/NBIF/EMSBackup/RmanBackup directory. In general, this TAR file contains the entire /data/NBIF directory’s content (except 'EMSBackup' directory), OVOC Software Manager content and server\_XXX directory’s content.

To change the weekly backup’s time and date, see Change Schedule Backup Time.

- **Daily backup:** runs daily except on the scheduled week day (see above). The daily backup process backs up the last 24 hours. There are no changes in the TAR file in this process.
- **Cassandra backup:** runs daily (runs prior to the above) and backs up the last 24 hours.

Daily and weekly backups run one hour after Cassandra. For example, if the backup time is 2:00, Cassandra runs at 2:00 and the Weekly/Daily backup runs at 3:00.



- The Backup process does not backup configurations performed using EMS Server Manager, such as networking and security.
- RmanBackup files are deleted during OVOC upgrade.

It is highly recommended to maintain all backup files on an external machine.

These files can be transferred outside the server directly from their default location by SCP or SFTP client using 'acems' user.

### ➤ Do the following:

1. Copy the backup tar files: /data/NBIF/EMSBackup/emsSServerBackup\_<time&date>\_<version>.tar file directory and /data/NBIF/EMSBackup/Cassandra<time&date>\_<version>.tar file to an external machine.

Where:

- <time&date> is only an example; replace this path with your filename.
  - <version> is the version number of the server release
2. Copy all files in /data/NBIF/EMSBackup/RmanBackup directory (including control.ctl and init.ora files) to an external machine.

## Change Schedule Backup Time

This step describes how to reschedule the backup time.

### ➤ To schedule backup time:

1. From the Application Maintenance menu, choose **Change Schedule Backup Time**.
2. Choose the day of the week that you wish to perform the backup.

## 15 OVOC Server Restore

This section describes how to restore the OVOC server. This can be done on the original machine that the backup files were created from or on any other machine.



- If you're running the restore process on a different machine, its disk size should be the same as the original machine from which the backup files were taken.
- Restore actions can be performed only with backup files which were previously created in the same OVOC version.
- If you are restoring to a new machine, make sure that you have purchased a new license file machine ID. AudioCodes customer support will assist you to obtain a new license prior to the restore process.

➤ **To restore the OVOC server:**

1. Install (or upgrade) OVOC to the same version from which the backup files were created. The Linux version must also be identical between the source and target machines.
2. Use the OVOC server Management utility to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.
3. For more details, see [Getting Started](#) on page 101.
4. Make sure all server processes are up in EMS Server Manager / Status menu and the server functions properly.
5. Copy all the files you backed up in Chapter [OVOC Server Backup](#) on page 98 to /data/NBIF directory by SCP or SFTP client using the 'acems' user. Overwrite existing files if required.
6. In OVOC Server Manager, from the Application Maintenance menu, select the **Restore** option.
7. Follow the instructions during the process; you might need to press Enter a few times.
8. After the restore operation has completed, you are prompted to reboot the OVOC server.
9. If you installed custom certificates prior to the restore, you must reinstall these certificates (see Appendix [Supplementary Security Procedures](#) on page 189).

# Part V

## OVOC Server Manager

This part describes the OVOC server machine maintenance using the OVOC server Management utility. The OVOC server Management utility is a CLI interface that is used to configure networking parameters and security settings and to perform various maintenance actions on the OVOC server.

**Warning:** Do not perform OVOC Server Manager actions directly through the Linux OS shell. If you perform such actions, OVOC application functionality may be harmed.

**Note:** To exit the OVOC Server Manager to Linux OS shell level, press q.

## 16 Getting Started

This section describes how to get started using the OVOC Server Manager.

### Connecting to the OVOC Server Manager

You can either run the OVOC Server Manager utility locally or remotely:

- If you wish to run it remotely, then connect to the OVOC server using Secure Shell (SSH).
- If you wish to run it locally, then connect using the management serial port or keyboard and monitor.

➤ **Do the following:**

1. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
2. Switch to 'root' user and provide root password (default password is root):

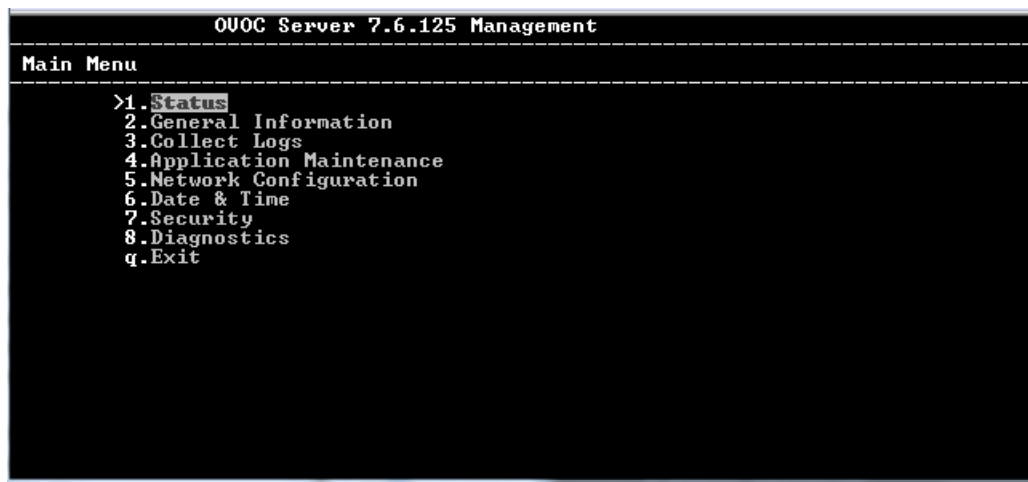
```
su - root
```

3. Type the following command:

```
# EmsServerManager
```

The OVOC Server Manager menu is displayed:

**Figure 16-1: OVOC Server Manager Menu**



- Whenever prompted to enter Host Name, provide letters or numbers.
- Ensure IP addresses contain all correct digits.
- For menu options where reboot is required, the OVOC server automatically reboots after changes confirmation.
- For some of the configuration options, you are prompted to authorize the changes. There are three options: Yes, No, Quit (y,n,q). Yes implements the changes, No cancels the changes and returns you to the initial prompt for the selected menu option and Quit returns you to the previous menu.

The following describes the full menu options for the OVOC Management utility:

- **Status** – Shows the status of current OVOC processes ([Viewing Process Statuses](#) on page 104)

- **General Information** – Provides the general OVOC server current information from the Linux operating system, including OVOC Version, OVOC server Process Status, Oracle Server Status, Apache Server Status, Java Version, Memory size and Time Zone ( [Viewing General Information](#) on page 106).
- **Collect Logs** – Collates all important logs into a single compressed file ( [Collecting Logs](#) on page 108):
  - General Info
  - Collect Logs
- **Application Maintenance** – Manages system maintenance actions ( [Application Maintenance](#) on page 110):
  - Start / Restart the Application
  - Stop Application
  - Web Servers
  - Change Schedule Backup Time
  - Restore
  - License
  - Shutdown the machine
  - Reboot the machine
- **Network Configuration** – Provides all basic, advanced network management and interface updates ( [Network Configuration](#) on page 117):
  - Server IP Address (The server will be rebooted)
  - Ethernet Interfaces (The server will be rebooted)
  - Ethernet Redundancy (The server will be rebooted)
  - DNS Client
  - NAT
  - Static Routes
  - SNMP Agent
  - SNMPv3 Engine ID
- **Date & Time** – Configures time and date settings ( [Date and Time Settings](#) on page 131):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations ( [Security](#) on page 134):
  - Add OVOC user
  - SSH
  - Oracle DB Password (OVOC server will be stopped)
  - Cassandra DB Password (OVOC server will be stopped)
  - OS Users Passwords
  - **HTTP** Security Settings:
    - ◆ TLS Version 1.0
    - ◆ TLS Version 1.1
    - ◆ Show Allowed SSL Cipher Suites
    - ◆ Edit SSL Cipher Suites Configuration String
    - ◆ Restore SSL Cipher Suites Configuration Default
    - ◆ Manage HTTP Service (Port 80)
    - ◆ Manage IPP Files Service (Port 8080)

- ◆ Manage IPPs HTTP (Port 8081)
- ◆ Manage IPPs HTTPS (Port 8082)
- ◆ OVOC REST (Port 911)
- ◆ Floating License REST (Port 912)
- ◆ OVOC WebSocket (Port 915)
- ◆ SBC HTTPS Authentication
- ◆ Enable Device Manager client secured communication (Apache will be restarted)
- ◆ Change HTTP/S Authentication Password for NBIF Directory
- File Integrity Checker
- Software Integrity Checker (AIDE) and Prelinking
- USB Storage
- Network Options
- Audit Agent Options (the server will be rebooted)
- Enable Statistics Report Web Page Secured Connection (OVOC application will be restarted).
- Server Certificates Update
- SEM-AudioCodes devices communication
- **Diagnostics** – Manages system debugging and troubleshooting ([Diagnostics](#) on page 160):
  - Server Syslog
  - Devices Syslog
  - Devices Debug
  - Server Logger Levels
  - Network Traffic Capture

## Using the EMS Server Manager

The following describes basic user hints for using the EMS Server Manager:

- The screens displaying the Main menu options in the procedures described in this section are based on a Linux installation with 'root' user permissions.
- The current navigation command path is displayed at the top of the screen to indicate your current submenu location in the CLI menu. For example, **Main Menu > Network Configuration > Ethernet Redundancy**.
- You can easily navigate between menu options using the keyboard arrow keys or by typing the menu option number.
- Each of the menu options includes an option to return to the main Menu "Back to Main Menu" and in some cases there is an option to go back to the previous menu level by specifying either "Back" or "Quit".

## 17 Viewing Process Statuses

You can view the statuses of the currently running OVOC applications.

➤ **To view the statuses of the current OVOC applications:**

1. From the OVOC server Management root menu, choose **Status**, and then press Enter; the following is displayed:

**Figure 17-1: Application Status**

```

-----Application-----|-----Status-----
Watchdog                 |UP
OVOC Server              |UP
SEM CPEs Server          |UP
SEM MS Lync Server       |UP
SEM Endpoints Server     |UP
Floating License Server  |UP
Perf Monitoring Server   |UP
Websocket Server         |UP
Tomcat Server            |UP
Apache HTTP Server       |UP
Oracle DB                |UP
Oracle Listener          |UP
Cassandra                |UP
SNMP Agent               |DOWN
NTP Daemon               |DOWN
-----|-----

Press 'Enter' key to go back to the main menu...
  
```

The following table describes the application statuses.

**Table 17-1: Application Statuses**

Application	Status
Watchdog	Indicates the status of the OVOC Watchdog process.
OVOC server	Indicates the status of the OVOC server process.
SEM CPEs Server	Indicates the status of the XML based SEM communication between the devices and the SEM CPEs Server.
SEM MS Lync Server	Indicates the status of the Skype for Business Server MS-SQL Server HTTP/S connection.
SEM Endpoints Server	Indicates the status of the Endpoint Server, which manages the UDP connection with the Endpoints (IP Phones) for SIP Publish RFC 6035 messages.
Floating License Server	Indicates the status of the connection between the OVOC server and the Floating License service.
Performance Monitoring Server	Indicates the status of the internal SNMP connection used by the OVOC server for polling managed devices.
WebSocket Server	Indicates the status of the internal connection between the WebSocket client and the OVOC server. This connection is used for managing the alarm and

Application	Status
	task notification mechanism in the OVOC Web.
Tomcat Server	Indicates the status of the Tomcat server, which manages the connection to the browser's statistics page.
Apache Server	Indicates the status of the Apache server, which manages the following connections: HTTP/S connection with the AudioCodes device, The OVOC server-Client connection. The HTTP connection that is used by Endpoints for downloading firmware and configuration files from the OVOC server.
Oracle DB	Indicates the status of the Oracle Database process.
Oracle Listener	Indicates the status of the Oracle Listener process.
Cassandra	Indicates the status of the Cassandra database that manages Call Details and SIP Ladder messages.
SNMP Agent	Indicates the status of the Linux SNMP Agent process. This agent is not responsible for the SNMPv2/SNMPv3 connection with the AudioCodes devices.
NTP Daemon	Indicates the status of the NTP Daemon process.



## 18 Viewing General Information

This section describes the General Information and Logs collection options. The General Information option provides detailed information about the OVOC server configuration and current status variables. The following information is provided:

- Components versions: OVOC, Linux, Java, Apache
- Components Statuses: OVOC server process and security, Watchdog, Apache, Oracle, SNMP agent, Tomcat and SEM.
- Memory size and disk usage
- Network configuration
- Time Zone and NTP configuration
- User logged in and session type

### ➤ To view General Information:

1. From the OVOC Server Managerroot menu, choose **General Information**, and then press Enter; the following is displayed:

Figure 18-1: General Information

```
sda          550G          disk running VMware
├─sda1       2G xfs      part
├─sda2       548G LVM2_member part
│   ├─vg-root /         20G xfs      lvm running
│   ├─vg-swap [SWAP]    7.8G swap    lvm running
│   ├─vg-data /data     304G xfs      lvm running
│   ├─vg-meta /meta     512M xfs      lvm running
│   ├─vg-opt  /opt       20G xfs      lvm running
│   ├─vg-oracle /oracle  25G xfs      lvm running
│   ├─vg-var  /var       20G xfs      lvm running
│   └─vg-home /home     150G xfs      lvm running
sr0          1024M        rom    running NECUMWar
!Data usage:
/dev/mapper/vg-data 304G 40G 265G 13% /data
-----
Versions
!OVOC Version      : 7.6.1075
!OS Version        : Linux 3.10.0-957.1.3.el7.x86_64 x86_64
!OS Revision       : CentOS 7 for EMS Server (Rev. 18)
!Java Version      : java full version "1.8.0_201-b09"
!Apache version    : Apache/2.4.6 (CentOS) Server built: Nov 5 2018 01:47:09
!Cassandra version : 3.11.2
<more>
```

2. Press **<more>** to view more information; the following is displayed:

Figure 18-2: General Information

```
Server's Network:
Interface      : ens160
Host Name      : vEMS-84
IP Address     : 172.17.140.84
Subnet Mask    : 255.255.255.0
Network Address : 172.17.140.0

Date & Time Information
!Date & Time    : [13/02/2019 10:13:16]
!Time Zone     : Israel (IST, +0200)

Network Time Protocol
Server #1
Peer:          : +aclads05.corp.a
Sync source    : 52.166.120.77
Stratum:       : 3
Type           : Unicast
Last response  : 853 seconds ago
Polling interval: 1024 seconds
Reach : 377 (all attempts successful)
Delay : 13.842 ms.
Offset : 5.534 ms.
Jitter : 48.481 ms.
<more>
```

```
Sync source      : 52.166.120.77
Stratum:         : 3
Type            : Unicast
Last response    : 853 seconds ago
Polling interval: 1024 seconds
Reach : 377 (all attempts successful)
Delay : 13.842 ms.
Offset : 5.534 ms.
Jitter : 48.481 ms.
<more>

Server #2
Peer:           : *aclads01.corp.a
Sync source     : 10.1.1.10
Stratum:        : 4
Type           : Unicast
Last response    : 895 seconds ago
Polling interval: 1024 seconds
Reach : 377 (all attempts successful)
Delay : 4.396 ms.
Offset : -7.824 ms.
Jitter : 16.422 ms.

Press 'Enter' key to back to main menu...□
```

Figure 18-3:

## 19 Collecting Logs

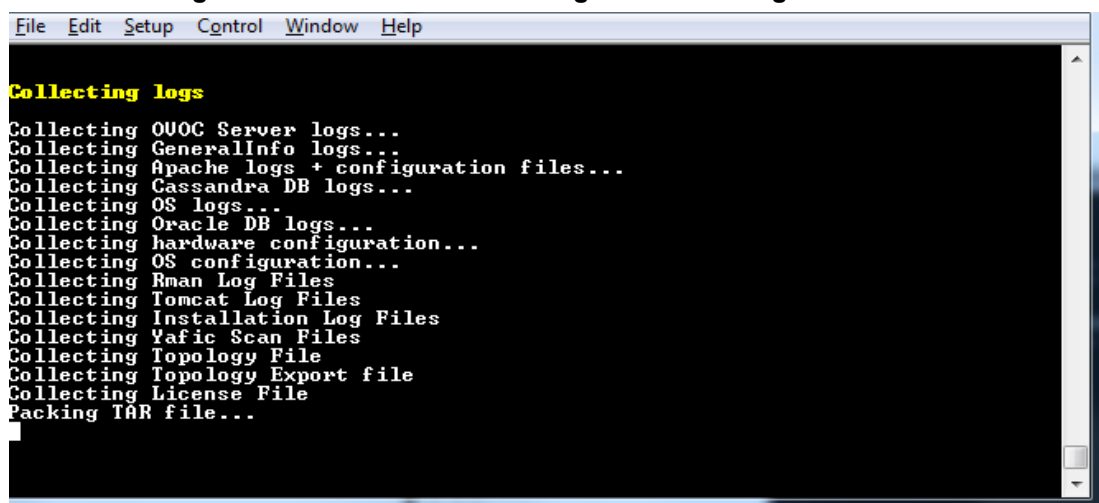
This option enables you to collect important log files. All log files are collected in a single file `log.tar` that is created under the user home directory. The following log files are collected:

- OVOC server Application logs
- General Info logs
- Apache logs and configuration files
- Cassandra DB logs
- OS logs
- Oracle DB logs
- Hardware information (including disk)
- OS Configuration
- Rman logs
- Tomcat logs
- Installation logs
- Oracle Database logs
- Server's Syslog Messages
- Yafic scan files
- Topology file
- Topology export file
- License file
- Relevant network configuration files (including static routes)

➤ **To collect logs:**

- From the OVOC server Management root menu, choose **Collect Logs**, and then press Enter; the OVOC server commences the log collection process:

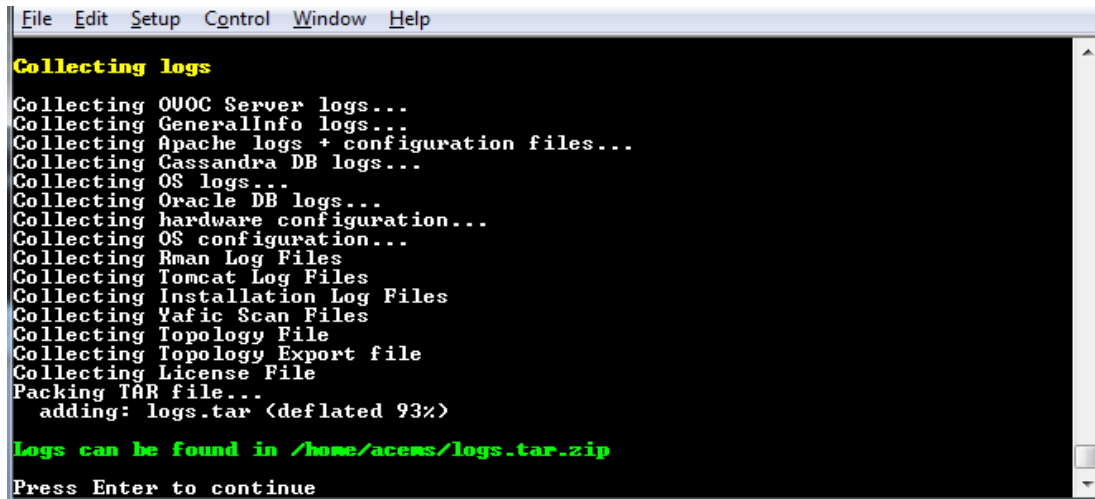
**Figure 19-1: OVOC Server Manager – Collect Logs**



```
File Edit Setup Control Window Help
Collecting logs
Collecting OVOC Server logs...
Collecting GeneralInfo logs...
Collecting Apache logs + configuration files...
Collecting Cassandra DB logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting Rman Log Files
Collecting Tomcat Log Files
Collecting Installation Log Files
Collecting Yafic Scan Files
Collecting Topology File
Collecting Topology Export file
Collecting License File
Packing TAR file...
```

This process can take a few minutes. Once the file generation has completed, a message is displayed on the screen informing you that a Diagnostic tar file has been created and the location of the tar file:

Figure 19-2: TAR File Location



```
File Edit Setup Control Window Help
Collecting logs
Collecting OVOC Server logs...
Collecting GeneralInfo logs...
Collecting Apache logs + configuration files...
Collecting Cassandra DB logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting Rman Log Files
Collecting Tomcat Log Files
Collecting Installation Log Files
Collecting Yafic Scan Files
Collecting Topology File
Collecting Topology Export file
Collecting License File
Packing TAR file...
  adding: logs.tar (deflated 93%)
Logs can be found in /home/acems/logs.tar.zip
Press Enter to continue
```

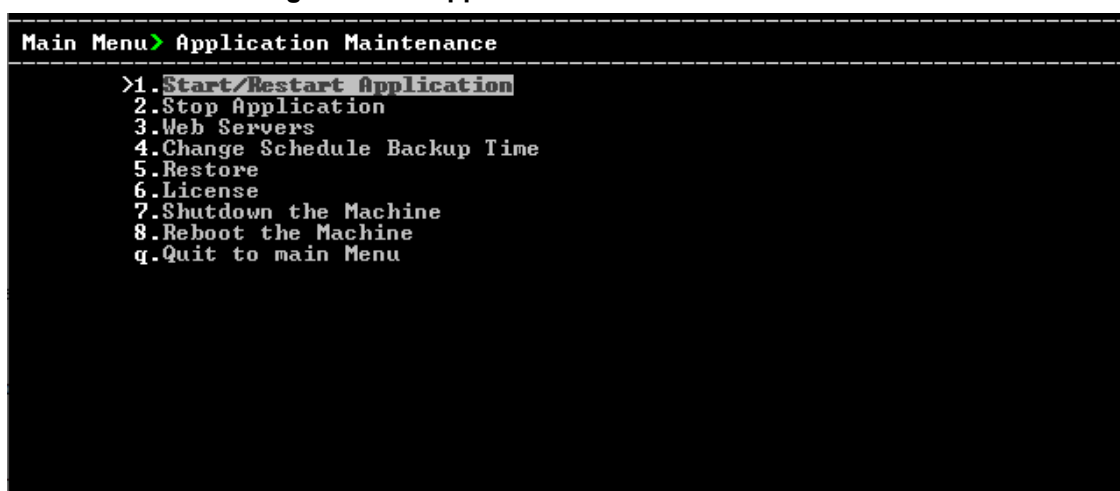
## 20 Application Maintenance

This section describes the application maintenance.

➤ **To configure application maintenance:**

- From the OVOC Server Manager root menu, choose **Application Maintenance**; the following is displayed:

**Figure 20-1: Application Maintenance**



This menu includes the following options:

- Start/Restart Application .([Start or Restart the Application](#) below)
- Stop Application ([Stop the Application](#) on the next page)
- Web Servers ([Web Servers](#) on the next page)
- Change Schedule Backup Time (Change Schedule Backup Time)
- Restore ([Restore](#) on page 112)
- License ([License](#) on page 112)
- Shutdown the Machine ( [Shutdown the OVOC Server Machine](#) on page 115)
- Reboot the Machine ([Reboot the OVOC Server Machine](#) on page 116)

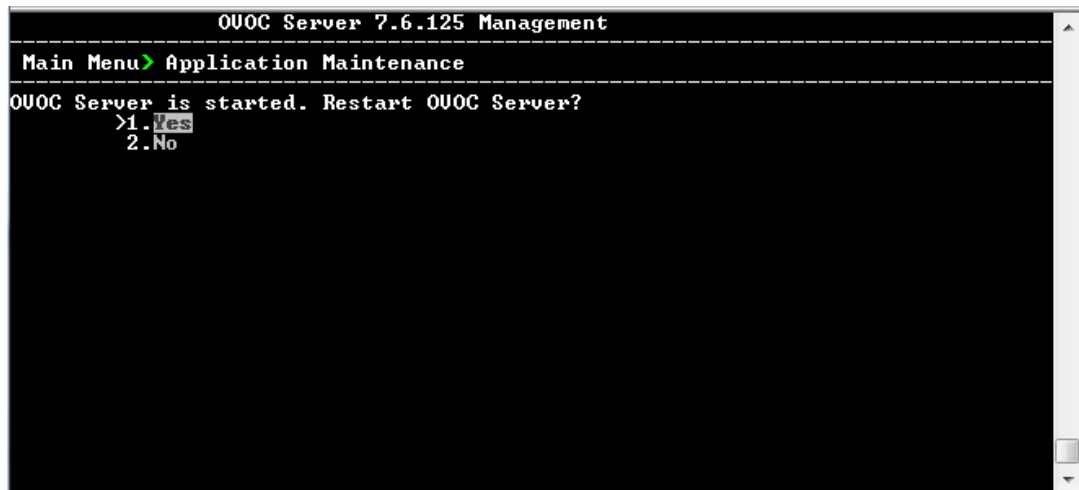
### Start or Restart the Application

This section describes how to start or restart the application.

➤ **To start/restart the application:**

1. From the Application Maintenance menu, choose **Start/Restart the Application**, and then press Enter; the following is displayed:

Figure 20-2: Start or Restart the OVOC server



2. Do one of the following:
  - Select **Yes** to start/restart the OVOC server
  - Select **No** to start/restart the OVOC server

## Stop the Application

1. In the Application menu, choose option **Stop Application**.
2. You are prompted whether you wish to stop the OVOC server.

Figure 20-3: Stop OVOC server



## Web Servers

- From the Application maintenance menu, choose **Web Servers**, and then press Enter; the following is displayed:

Figure 20-4: Web Servers

```

Main Menu> Application Maintenance> Web Servers
-----
!The Apache Server Process is: UP
!The Tomcat Server's Processes are: UP
!Port 80 <HTTP>: OPEN
!Port 8080 <IPPs FILES>: OPEN
!Port 8081 <IPPs HTTP>: OPEN
!Port 8082 <IPPs HTTPS>: OPEN

>1.Stop the Apache Server
2.Stop the Tomcat Server
3.Close HTTP Service <Port 80>
4.Close IPP Files service <Port 8080>
5.Close IPPs HTTP <Port 8081>
6.Close IPPs HTTPS <Port 8082>
b.Back
q.Quit to main Menu

```

## Apache and Tomcat Server Processes

This section describes how to open and close the Apache and Tomcat Web server connections.

### ➤ To stop the Apache server:

- In the Web Servers menu, choose option **Stop/Start Apache Server**, and then press Enter.

### ➤ To stop the Tomcat server:

- In the Web Servers menu, choose option **Stop/Start Tomcat Server**, and then press Enter.

## Change Schedule Backup Time

This option enables you to reschedule the time that you wish to back up the OVOC server ([OVOC Server Backup](#) on page 98).

## Restore

This option enables you to restore the OVOC server to the latest backed up version ([OVOC Server Restore](#) on page 99).

## License

The License menu enables you to view the details of the existing license or upload a new license.

The OVOC server License (SBC License pool, IP Phones and Voice Quality) should have a valid license loaded to the server in order for it to be fully operational.

To obtain a valid license for your OVOC server License you should activate your product through License Activation tool at <http://www.AudioCodes.com/swactivation>.

You will need your Product Key (see below) and the Server Machine ID (see below) for this activation process:

- **ProductKey:** the Product Key string is used in the customer order for upgrading the OVOC product. For more information, contact your AudioCodes partner.
- **Machine ID:** indicates the OVOC Machine ID that should be taken from the server as shown in the screen below (enter this ID in the Fingerprint field in the Activation form). This ID is also used in the customer order process when the product key is not known (for more information contact your AudioCodes representative).
- **License Status:** indicates whether the OVOC license is enabled ([OVOC Time License](#) on the next page below).

- **OVOC Advanced:** indicates whether the SEM license is enabled (default-no). When this parameter is set to default, the following licenses are available for the SEM:

- Devices Number = 2
- IP Phones Number = 10
- SEM Sessions = 10
- SEM Users = 10

When set to Yes, the above parameters can be configured according to the number of purchased licenses

- **Expiration Date:** indicates the expiration date of the OVOC time license. By default, this field displays 'Unlimited' ( below).

The time zone is determined by the configured date and time in the Date & Time menu ([Timezone Settings](#) on page 132).



- When you order AudioCodes devices (MediantSBC and MediantGateway AudioCodes products), ensure that a valid feature key is enabled with the "OVOC" parameter for those devices that you wish to manage. Note that this feature key is a separate license to the OVOC server license.
- Licenses can be allocated to Tenants in the OVOC Web according to the license parameters displayed in the License screen (see example in [OVOC Time License](#) below).

## OVOC Time License

The OVOC time license sets the time period for product use. When the time license is enabled and the configured license time expires, the connection to the OVOC server is denied. The time based license affects all the features in the OVOC including the SBC License Pool, Devices (entities managed by the Device Manager) and Voice Quality Management. When the OVOC server time license approaches or reaches its expiration date, the 'License alarm' is raised (Refer to the *One Voice Operations Center Alarms Guide*).

### ➤ To view the license details or upload a new license:

1. Copy the license file that you have obtained from AudioCodes to the following path on the OVOC server machine:  
/home/acems/<License\_File>
2. From the Application Maintenance menu, choose **License** option, and then press Enter; the current License details are displayed:



Figure 20-5: License Manager

```

Main Menu> Application Maintenance> License

License Configuration Manager:
Server Machine ID: B9C8B237B0DF
Product Key: B9C8B237B0DF
License Status: ENABLED
OVOC Advanced: Yes
Expiration Date: 02-06-2022

Floating License
Status: ENABLED
SBC Sessions:
SBC Registrations:
SBC Transcoding:
SBC Signaling:
-----

Fixed License Pool
SBC Managed Devices: 1,000,000
SBC Sessions: 100,000,000
SBC Registrations: 10,000,000
SBC Transcoding: 1,000,000
SBC Signaling: 10,000,000
CB Users: 1,000,000
CB PBX Users: 1,000,000
CB Analog Devices: 100,000
CB Voicemail Accounts: 100,000
-----

Endpoints
Managed Endpoints: 10,000,000
-----


Voice Quality
Total Devices: 10,000,000
Total Endpoints: 100,000,000
Total Sessions: 2,000,000,000
Total Users: 100,000,000
-----

>1. Load License
b. Back
q. Quit to main Menu

```

Table 20-1: License Pool Parameters

License Type	License Parameter
<b>Floating License</b>	
SBC Sessions	The number of concurrent floating license call sessions supported by the SBCs in your deployment
SBC Registrations	The number of floating license SIP endpoints that can register with the SBCs allowed by your license.
SBC Transcoding	The number of floating license transcoding sessions supported by the SBCs in your deployment.
SBC Signaling	The number of floating license signaling sessions supported by the SBCs in your deployment.
<b>Fixed License Pool</b>	
SBC Managed Devices	The total number of devices (SBCs, gateways and MSBRs) that can be managed by the License Pool.

License Type	License Parameter
SBC Registrations	The number of SIP endpoints that can register with the SBCs allowed by your license.
SBC Sessions	The number of concurrent call sessions supported by the SBCs in your deployment.
SBC Signaling	The number of SBC signaling sessions supported by the SBCs in your deployment.
SBC Transcoding	The number of SBC transcoding sessions supported by the SBCs in your deployment.
CB Analog Devices	Currently not supported.
CB PBX Users	Currently not supported.
CB Users	The supported number of CloudBond 365 users
CB Voicemail Accounts	Currently not supported.
<b>Endpoints</b>	
Devices	The number of endpoints supported by the Device Manager Pro application.
<b>Voice Quality</b>	
OVOC Managed Devices	The number of Voice Quality monitored devices (SBCs, gateways and MSBRs).
Devices	The number of Voice Quality monitored endpoints.
Sessions	The number of concurrent Voice Quality monitored call SBC sessions.
Users	<p>The number of Voice Quality monitored users supported by the SBC.</p> <div>  <p>The minimum number of Voice Quality user licenses is 10. If less than 10 user licenses are purchased, then Skype for Business devices cannot be added in the OVOC Web interface.</p> </div>

3. To load a new license, choose option **1**.
4. Enter the license file path and name.
5. Restart the OVOC server.

## Shutdown the OVOC Server Machine

This section describes how to shut down the OVOC server machine.

### ➤ To shut down the OVOC server machine:

1. From the Application Maintenance menu, choose **Shutdown the Machine**, and then press Enter.
2. Type **y** to confirm the shutdown; the OVOC server machine is shutdown.

## Reboot the OVOC Server Machine

This section describes how to reboot the OVOC server machine.

➤ **To reboot the OVOC server machine:**

1. From the Application Maintenance menu, choose **Reboot the Machine**, and then press Enter.
2. Type **y** to confirm the reboot; the OVOC server machine is rebooted.

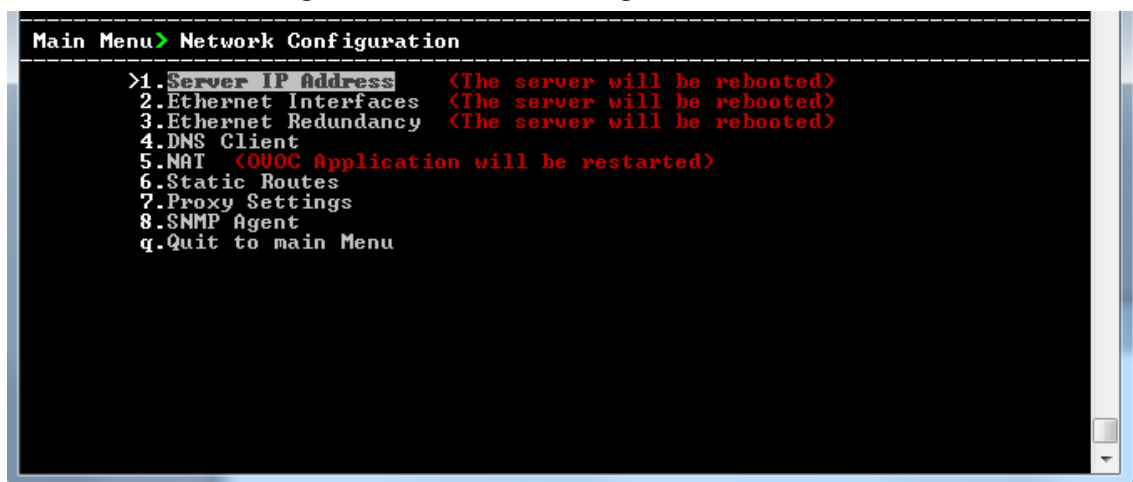
## 21 Network Configuration

This section describes the networking options in the EMS Server Manager.

➤ **To run the network configuration:**

- From the OVOC Server Managerroot menu, choose **Network Configuration**; the following is displayed:

**Figure 21-1: Network Configuration**



This menu includes the following options:

- Server IP Address (the server will be rebooted) ( [Server IP Address](#) below).
- Ethernet Interfaces (the server will be rebooted) ([Ethernet Interfaces](#) on the next page).
- Ethernet Redundancy (the server will be rebooted) ([Ethernet Redundancy](#) on page 121).
- DNS Client ([DNS Client](#) on page 125).
- NAT ([NAT](#) on page 126).
- Static Routes ([Static Routes](#) on page 126).
- OVOC Proxy Settings ([Proxy Settings](#) on page 127)
- SNMP Agent ([SNMP Agent](#) on page 128).

### Server IP Address

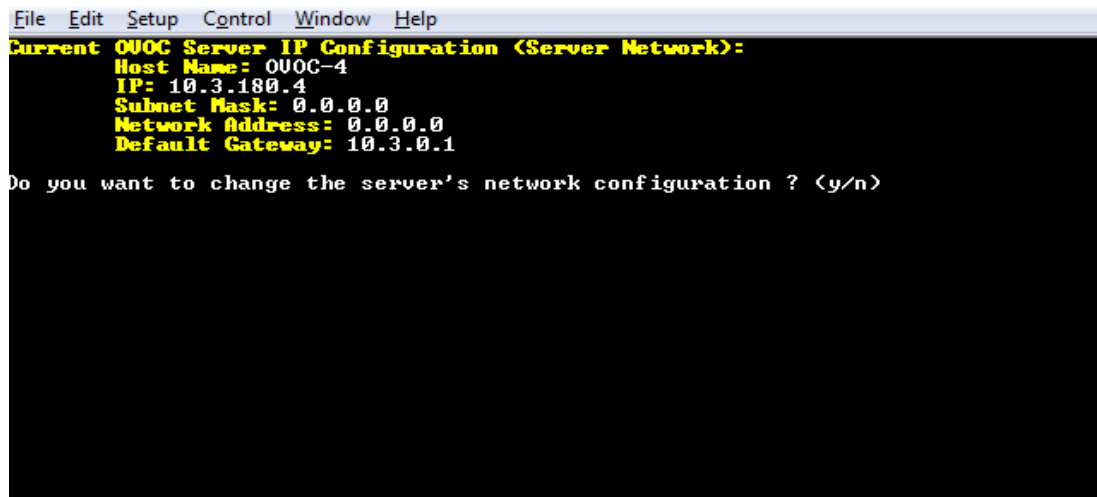
This option enables you to update the OVOC server's IP address. This option also enables you to modify the OVOC server host name.



When this operation has completed, the OVOC automatically reboots for the changes to take effect.

➤ **To change Server's IP address:**

1. From the Network Configuration menu, choose Server IP Address, and then press Enter; the following is displayed:

**Figure 21-2: EMS Server Manager – Change Server's IP Address**


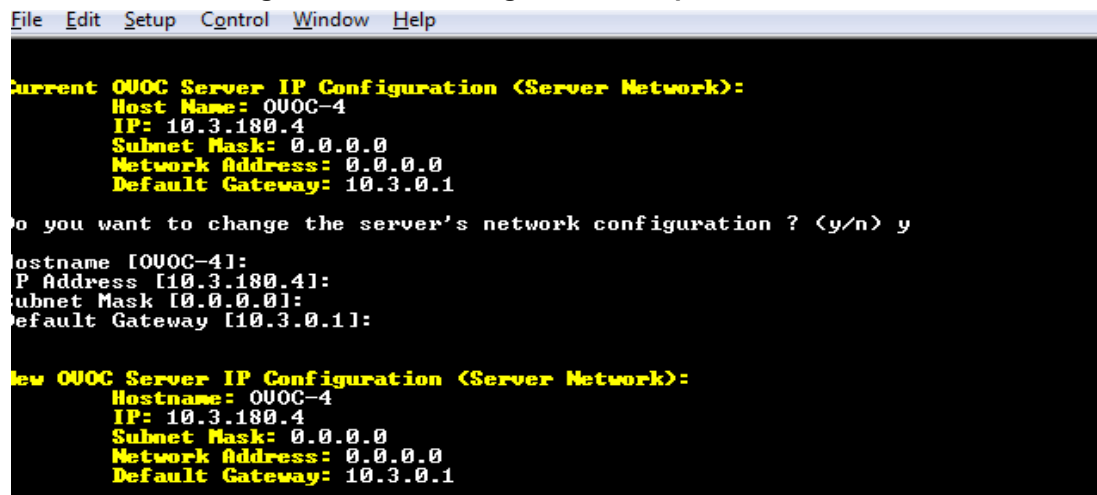
```

File Edit Setup Control Window Help
Current OVOC Server IP Configuration (Server Network):
Host Name: OVOC-4
IP: 10.3.180.4
Subnet Mask: 0.0.0.0
Network Address: 0.0.0.0
Default Gateway: 10.3.0.1

Do you want to change the server's network configuration ? <y/n>

```

2. Configure IP configuration parameters as desired.  
Each time you press Enter, the different IP configuration parameters of the OVOC server are displayed. These parameters include the Server Host Name, IP address, Subnet Mask, Network Address and Default Gateway.
3. Type **y** to confirm the changes, and then press Enter.

**Figure 21-3: IP Configuration Complete**


```

File Edit Setup Control Window Help

Current OVOC Server IP Configuration (Server Network):
Host Name: OVOC-4
IP: 10.3.180.4
Subnet Mask: 0.0.0.0
Network Address: 0.0.0.0
Default Gateway: 10.3.0.1

Do you want to change the server's network configuration ? <y/n> y

Hostname [OVOC-4]:
IP Address [10.3.180.4]:
Subnet Mask [0.0.0.0]:
Default Gateway [10.3.0.1]:

New OVOC Server IP Configuration (Server Network):
Hostname: OVOC-4
IP: 10.3.180.4
Subnet Mask: 0.0.0.0
Network Address: 0.0.0.0
Default Gateway: 10.3.0.1

```

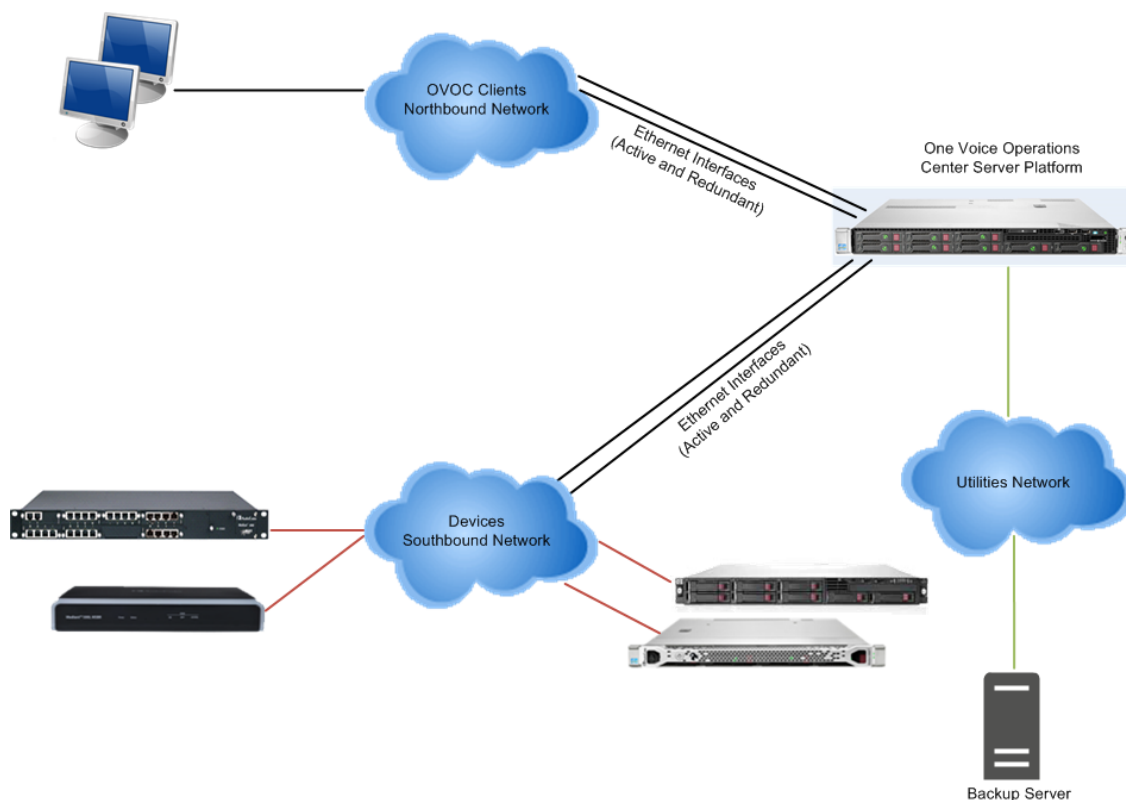
Upon confirmation, the OVOC automatically reboots for the changes to take effect.

## Ethernet Interfaces

This section describes how to configure Ethernet interfaces.

### OVOC Client Login on all OVOC Server Network Interfaces

The OVOC server can be configured with up to four network interfaces (connected to different subnets) as described above. You can connect to any one of the above interfaces directly from the OVOC client login dialog. The “Server IP” field in OVOC client login dialog is set to the desired OVOC server network interface IP address.

**Figure 21-4: OVOC server: Triple Ethernet Interfaces**

In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound Network' to each one of the subnets. For Static Routes configuration, [Static Routes](#) on page 126.

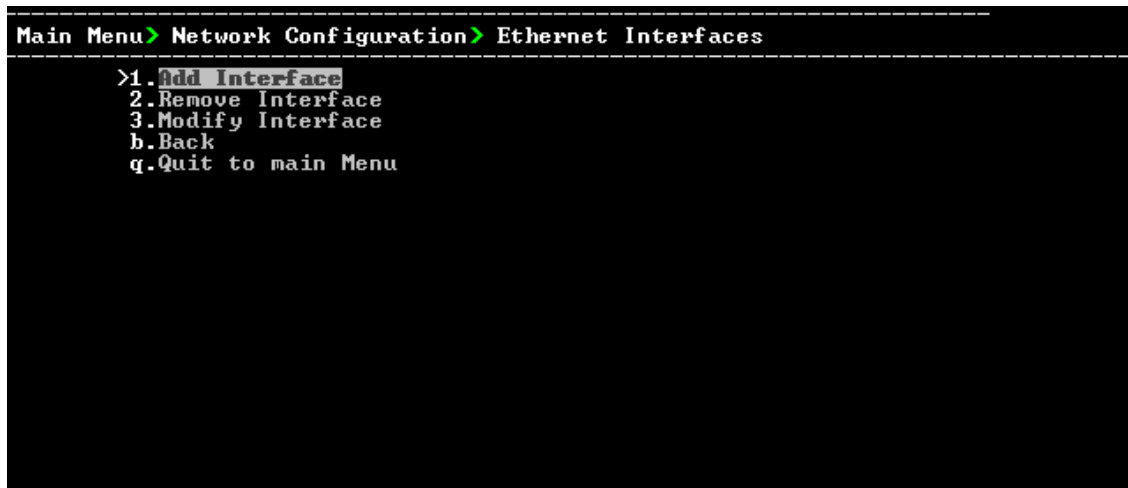
To ensure that the network configuration is performed successfully, test that the OVOC is successfully connected to each one of the gateways by running the following basic tests:

- Adding the gateway to the OVOC application
- Reviewing its status screen
- Performing basic configuration action (set of 'MG Location' in Media Gateways Provisioning Frame / General Setting tab)
- Ensuring that the OVOC receives traps from the gateway by adding TP boards in one of the empty slots and ensuring that the 'Operational Info' Event is received.

➤ **To configure Ethernet Interfaces:**

1. From the Network Configuration menu, choose Ethernet Interfaces, and then press Enter; the following is displayed:

Figure 21-5: EMS Server Manager – Configure Ethernet Interfaces



2. Choose from one of the following options:
  - **Add Interface** – Adds a new interface to the OVOC server ( [Add Interface](#) below).
  - **Remove Interface** – Removes an existing interface from the OVOC server ( [Remove Interface](#) on the next page).
  - **Modify Interface** – Modifies an existing interface from the OVOC server ( [Type y to confirm the changes; the OVOC server automatically reboots for the changes to take effect.](#) on the next page).

## Add Interface

This section describes how to add a new interface.

### ➤ To add a New Interface:

1. From the Ethernet Interfaces menu, choose option **1**; a list of currently available interfaces (not yet configured) is displayed.
2. Choose an interface (on HP machines the interfaces are called 'eno1', 'eno2', etc).
3. Choose the Network Type.
4. Enter values for the following interface parameters and confirm:
  - IP Address
  - Hostname
  - Subnet Mask

The new interface parameters are displayed.

5. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Figure 21-6: Add Interface Parameters

```

Add Interface:

Choose Interface:
1) eth1
2) eth2
3) eth3
q) Quit
: 1

Choose Network Type:
1) Network 1 (MG's Network)
2) Network 2
3) Network 3
4 ) Quit
: 1

New Interface Parameters:

IP Address : 10.4.100.55
Hostname : GWs
Subnet Mask : 255.255.0.0

Note: Reboot will be performed immediately at the end of configuration process.

Are you sure that you want to continue? (y/n/q) █

```

## Remove Interface

This section describes how to remove an interface.

### ➤ To remove an existing interface:

1. From the Ethernet Interfaces menu, choose option **2**; the following is displayed:
2. Choose the interface to remove.
3. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

## Modify Interface

This section describes how to modify an existing interface.

### ➤ To modify an existing interface:

1. From the Ethernet Interfaces menu, choose option **3**.
2. Choose the interface to modify; the following is displayed:
3. Change the interface parameters.
4. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

## Ethernet Redundancy

This section describes how to configure Ethernet Redundancy. Physical Ethernet Interfaces Redundancy provides failover when you have multiple network interface cards that are connected

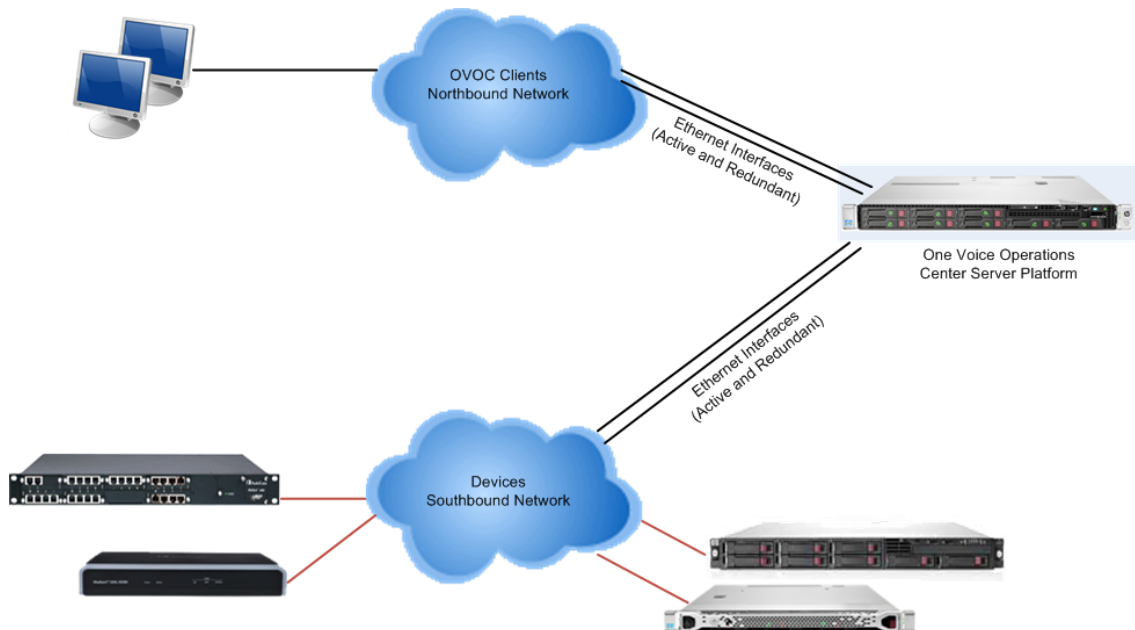


to the same IP link. The OVOC server supports up to four Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them. For example, OVOC Clients [Northbound] and Gateways [Southbound]. This option enables you to configure Ethernet ports redundancy.



When the operation is finished, the OVOC server automatically reboots for the changes to take effect.

**Figure 21-7: Physical Ethernet Interfaces Redundancy**



➤ **To configure Ethernet Redundancy:**

1. From the Network Configuration menu, choose **Ethernet Redundancy** option, and then press Enter; the following is displayed:

**Figure 21-8: Ethernet Redundancy Configuration**

```

Main Menu> Network Configuration> Ethernet Redundancy
-----
Interface: eth0
Network: Server's Network
IP Address: 10.3.180.7
Interface: eth1
Not configured
Interface: eth2
Not configured
Interface: eth3
Not configured
>1. Add Redundant Interface
2. Remove Redundant Interface
3. Modify Redundant Interface
b. Back
q. Quit to main Menu
  
```

2. This menu includes the following options:
  - Add Redundant Interface ([Add Redundant Interface](#) on the next page ).
  - Remove Redundant Interface ([Remove Ethernet Redundancy](#) on the next page).
  - Modify Redundant Interface ([Modify Redundant Interface](#) on page 124 ).

## Add Redundant Interface

Remove a redundant interface under the following circumstances:

- You have configured an Ethernet interface ([Add Redundant Interface](#) above).
- Your default router can respond to a 'ping' command, due to a heartbeat procedure between interfaces and the default router (to verify activity).

### ➤ To add a redundant interface:

1. From the Ethernet Redundancy menu, choose option 1.
2. Choose the network type for which to create a new redundant interface (for example, 'OVOC Client-Server Network').
3. Choose the interface in the selected network that you wish to make redundant (for example, 'eno', 'eno1', 'eno2').
4. Choose the redundancy mode (for example, 'balance-rr', 'active-backup').
5. Type **y** to confirm the changes; the OVOC server automatically reboots for changes to take effect.

**Figure 21-9: Add Redundant Interface**

```

Ethernet Redundancy Configuration

Interface: eth0
    Network: Server's Network
    IP Address: 10.7.14.141
Interface: eth1
    Not configured

1) Add Redundant Interface
2) Remove Redundant Interface
3) Modify Redundant Interface
4) Back to Main Menu
: 1

Add Redundant Interface:

Choose Network Type:
1) Server Network
2) Quit
: 1

Choose Redundant Interface:
1) eth1
q) Quit
: 1

Ethernet Redundancy Settings:

Ethernet Redundancy Mode:
0) balance-rr (round-robin load balancing)
1) active-backup - recommended
2) balance-xor (XOR-policy load balancing)
3) broadcast
4) 802.3ad (IEEE 802.3ad dynamic link aggregation)
5) balance-tlb (transmit load balancing)
6) balance-alb (adaptive load balancing)
: 1

Are you sure that you want to continue? (y/n/q) █

```

## Remove Ethernet Redundancy

This section describes how to remove an Ethernet redundancy interface.

➤ **To remove the Ethernet Redundancy interface:**

1. From the Ethernet Redundancy menu, choose option **2**.
2. Choose the network redundancy to remove.

The current Ethernet redundancy configuration is displayed.

3. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

**Figure 21-10: Ethernet Redundancy Interface to Disable**

```
Ethernet Redundancy Configuration

Interface: eth0
  Network: Server's Network
  IP Address: 10.7.14.141
Interface: eth1
  Network: Server's Network (redundant interface)

1) Add Redundant Interface
2) Remove Redundant Interface
3) Modify Redundant Interface
4) Back to Main Menu
: 2

Remove Redundant Interface:

Choose Redundant Network
1) Server's Network (eth0, eth1)
q) Quit
: 1

Are you sure that you want to continue? (y/n/q) y
```

## Modify Redundant Interface

This section describes how to modify a redundant interface.

➤ **To modify redundant interface and change redundancy settings:**

1. From the Ethernet Redundancy, choose option **3**.
2. Choose the Ethernet redundancy interface to modify.
3. Change the redundancy settings.
4. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Figure 21-11: Modify Redundant Interface

```

Ethernet Redundancy Configuration

Interface: eth0
    Network: Server's Network
    IP Address: 10.7.14.141
Interface: eth1
    Network: Server's Network (redundant interface)

1) Add Redundant Interface
2) Remove Redundant Interface
3) Modify Redundant Interface
4) Back to Main Menu
: 3

Modify Redundant Interface:

Choose Redundant Network
1) Server's Network (eth0, eth1)
q) Quit
: 1

Ethernet Redundancy Settings:

Ethernet Redundancy Mode:
0) balance-rr (round-robin load balancing)
1) active-backup - recommended
2) balance-xor (XOR-policy load balancing)
3) broadcast
4) 802.3ad (IEEE 802.3ad dynamic link aggregation)
5) balance-tlb (transmit load balancing)
6) balance-alb (adaptive load balancing)
[1]: 0

Are you sure that you want to continue? (y/n/q) y

```

## DNS Client

Domain Name System (DNS) is a [database](#) system that translates a computer's [fully qualified domain name](#) into an [IP address](#). If a DNS server cannot fulfill your request, it refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

This option enables you to configure the client side (Resolver). If there is no existing DNS configuration, the option **Configure DNS** is displayed. If already configured, the option **Modify DNS** is displayed.

### ➤ To Configure the DNS Client:

1. From the Network Configuration menu, choose DNS Client, press Enter, and then in the sub-menu, choose Configure DNS; the following is displayed:

Figure 21-12: DNS Setup

```

Do you want to specify the local domain name ? <y/n>y
Local Domain Name: Brad
Do you want to specify a search list ? <y/n>y
Search List (use "," between domains names): Brad

DNS IP Address 1: 10.1.1.10
DNS IP Address 2: 10.1.1.11
DNS IP Address 3: 10.1.1.12

New DNS Configuration:
  Domain Name: Brad
  Search List: Brad
  DNS IP 1: 10.1.1.10
  DNS IP 2: 10.1.1.11
  DNS IP 3: 10.1.1.12

Are you sure that you want to continue? <y/n/q> █

```

2. Specify the location domain. Type **y** to specify the local domain name or type **n**, and then press Enter.
3. Specify a search list; type **y** to specify a list of domains (use a comma delimiter to separate search entries in the list) or type **n**, and then press Enter.
4. Specify DNS IP addresses **1**, **2** and **3**.
5. Type **y** to confirm your configuration; the new configuration is displayed.

## NAT

NAT is the process of modifying network address information in datagram packet headers traversing a traffic routing device for the purpose of remapping a given address space to another.

### ➤ To configure NAT:

1. From the Network Configuration menu, choose **NAT**, and then press Enter.
2. Enable the OVOC Server's NAT address.
3. Type **y** to confirm the changes.
4. Stop and start the OVOC server for the changes to take effect.

### ➤ To remove NAT configuration:

1. Enter the value **-1**.
2. Type **y** to confirm the changes.
3. Stop and start the OVOC server for the changes to take effect.

## Static Routes

This option enables you to add or remove static route rules. Static routes are usually only used in conjunction with `/etc/defaultrouter`. Static routes may be required for network topology, where you don't want to traverse your default Gateway/Router. In this case, you will probably wish to make the routes permanent by adding the static routing rules.

### ➤ To configure static routes:

1. From the Network Configuration menu, choose Static Routes, and then press Enter; the Static Routes Configuration is displayed:

Figure 21-13: Routing Table and Menu

```

Main Menu> Network Configuration> Static Routes
-----
Static Routes Configuration

Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS  Window  irtt  Iface
10.3.0.0         0.0.0.0         255.255.0.0     U        0    0        0     eth0
11.200.0.0       10.3.180.20     255.255.0.0     UG        0    0        0     eth0
169.254.0.0      0.0.0.0         255.255.0.0     U        0    0        0     eth0
0.0.0.0          10.3.0.1        0.0.0.0         UG        0    0        0     eth0
>1. Add Static Route
  2. Remove Static Route
  b. Back
  q. Quit to main Menu

```

2. From the Static Routes configuration screen, choose one of the following options:

- Add a Static Route
- Remove a Static Route

➤ **To add a static route:**

1. From the Static Routes menu, choose option **1**.
2. Enter the Destination Network Address.
3. Enter the router's IP address.
4. Type **y** to confirm the changes.

➤ **To remove a static route:**

1. From the Static Routes menu, choose option **2**.
2. Enter the Destination Network Address for the static route you wish to remove.
3. Enter the router's IP address.
4. Type **y** to confirm the changes.

## Proxy Settings

This option enables the configuration of a proxy server connection that is used to connect to between OVOC and a remote platform such as AudioCodes Floating License. The connection is configured over HTTP/HTTPS/FTP .

➤ **To configure proxy settings:**

1. From the Network Configuration menu, choose **Proxy Settings**.
2. Select **Configure Proxy**, and confirm that you wish to configure the HTTP/HTTPS/FTP Proxy server.
3. Enter the IP address and port of the proxy server.
4. Enter the Proxy username and password.
5. Enter "No Proxy" addresses (a list of IP addresses for connecting directly from OVOC and not through a proxy server).

Figure 21-14: Proxy Settings

```

Current HTTP/HTTPS/FTP Proxy configuration:
URL: http://165.72.196.27:8080
No password
No proxy for URLs: 127.0.0.1,localhost
Would you like to change Proxy Settings? (y/n)
Would you like to change Proxy Settings? (y/n) y
Enter Proxy server address (incl. port number), blank to disable Proxy:
http://165.72.196.27:8080
Enter Proxy username (leave blank if no username and password authentication needed):
Enter addresses to access directly, comma-separated (NO PROXY):
127.0.0.1,localhost

```



HTTPS Proxy server is currently not supported.

## SNMP Agent

The SNMP Management agent enables access to system inventory and monitoring and provides support for alarms using the industry standard management protocol: Simple Network Management Protocol (SNMP). This agent serves OVOC, NMS, or higher level management system synchronization. This menu includes the following options:

- Stop and start the SNMP agent
- Configure the SNMP agent including:
  - Configure the SNMP agent listening port ([SNMP Agent Listening Port](#) on the next page)
  - Configure the northbound destination for linux system traps forwarding ([Linux Trap Forwarding Configuration](#) on the next page).
  - Configure the SNMPv3 Engine ID ([Server SNMPv3 Engine ID](#) on page 130)

### ➤ To configure SNMP Agent:

1. From the Network Configuration menu, choose **SNMP** Agent, and then press Enter.

Figure 21-15: SNMP Agent

```

Main Menu> Network Configuration> SNMP Agent
-----
SNMP Agent Status: DOWN
>1. Configure SNMP Agent
  2. Start SNMP Agent
   b. Back
   q. Quit to main Menu

```

The SNMP Agent status is displayed.

### ➤ To start the SNMP Agent:

- Choose option 2.

➤ **To configure SNMP Agent:**

1. Choose option 1.

Figure 21-16: Configure SNMP Agent

```
Main Menu> Network Configuration> SNMP Agent> Configure SNMP Agent
>1. SNMP Agent Listening Port
2. Linux System Traps Forwarding Configuration
3. SNMPv3 Engine ID
b.Back
q.Quit to main Menu
```

## SNMP Agent Listening Port

The SNMP Agent Listening port is a bi-directional UDP port used by the SNMP agent for listening for traps from managed devices. You can change this listening port according to your network traffic management setup.

➤ **To configure SNMP Agent Listening port**

1. Choose option 1.

Figure 21-17: SNMP Agent Listening Port

```
Main Menu> Network Configuration> SNMP Agent> Configure SNMP Agent
>1. SNMP Agent Listening Port
2. Linux System Traps Forwarding Configuration
3. SNMPv3 Engine ID
b.Back
q.Quit to main Menu
```

2. Configure the desired listening port (default 161).

## Linux Trap Forwarding Configuration

This option enables you to configure the northbound interface for forwarding Linux system traps.

➤ **To configure the Linux System Traps Forwarding Configuration:**

1. Choose option 2.
2. Configure the NMS IP address.



3. Enter the Community string; the new configuration is applied.

## Server SNMPv3 Engine ID

The OVOC server Engine ID is used by the SNMPv3 protocol when alarms are forwarded from the OVOC to an NMS. By default, the OVOC server SNMPv3 Engine ID is automatically created from the OVOC server IP address. This option enables the user to customize the OVOC server Engine ID according to their NMS configuration.

### ➤ To configure the SNMPv3 Engine ID:

1. From the Network Configuration menu, choose **SNMPv3 Engine ID**, and then press Enter; the following is displayed:

**Figure 21-18: EMS Server Manager – Configure SNMPv3 Engine ID**

```
SNMPv3 Engine ID Configuration

Server's SNMPv3 Engine ID (0 in all values return to default configuration)
Byte[0] (valid range -128 .. 127):
```

2. Enter '12' separate bytes ranges of the Engine ID (each valid range from between -128 to 127). In each case, press Enter to confirm the current value insertion and then proceed to the next one.
3. When all Engine ID bytes are provided, type **y** to confirm the configuration. To return to the root menu of the EMS Server Manager, press **q**.

**Figure 21-19: SNMPv3 Engine ID Configuration – Complete Configuration**

```
SNMPv3 Engine ID Configuration

Server's SNMPv3 Engine ID (0 in all values return to default configuration)
Byte[0] (valid range -128 .. 127):21
Byte[1] (valid range -128 .. 127):23
Byte[2] (valid range -128 .. 127):2
Byte[3] (valid range -128 .. 127):5
Byte[4] (valid range -128 .. 127):3
Byte[5] (valid range -128 .. 127):78
Byte[6] (valid range -128 .. 127):-17
Byte[7] (valid range -128 .. 127):-56
Byte[8] (valid range -128 .. 127):121
Byte[9] (valid range -128 .. 127):117
Byte[10] (valid range -128 .. 127):-111
Byte[11] (valid range -128 .. 127):127

Engine ID: 21.23.2.5.3.78.-17.-56.121.117.-111.127
Are you sure that you want to continue? (y/n/q)
```

## 22 Date and Time Settings

This option enables you to change the system time and date.

### ➤ To change system time and date:

- From the OVOC server Management root menu, choose Date & Time, and then press Enter; the following is displayed:

**Figure 22-1: EMS Server Manager - Change System Time & Date**

```

Main Menu> Date & Time
-----
>1.NTP
  2.Timezone Settings      (Apache Server will be restarted)
  3.Date & Time Settings
  q.Quit to main Menu
  
```

This menu includes the following options:

- NTP [NTP](#) below
- Timezone Settings [Timezone Settings](#) on the next page
- Date & Time Settings [Date and Time Settings](#) above

## NTP

Network Time Protocol (NTP) is used to synchronize the time and date of the OVOC server (and all its components) with other devices in the IP network.

This option enables you to configure the OVOC server to obtain its clock from an external NTP clock source and other devices that are connected to the OVOC server in the IP network can synchronize with this clock source. These devices can be any device containing an NTP server or client.

Alternatively, you can configure the NTP server to allow other devices in the IP network to synchronize their clocks according to the OVOC server clock.



- It is recommended to configure the OVOC server to synchronize with an external clock source because the OVOC server clock is less precise than other NTP devices.
- Configure the same NTP server on both the OVOC server and the AudioCodes device.
- When connecting the Skype for Business Front-End server, ensure that the same NTP server clock is used on both the OVOC server and Skype for Business server.
- If you configure NTP server on the device, it is recommended to configure the same NTP server settings on the device and the OVOC server.

### ➤ To configure NTP:

1. From the Date & Time menu, choose **NTP**, and then press Enter; the following is displayed:

Figure 22-2: EMS Server Manager - Configure NTP

```

Main Menu> Date & Time> NTP
-----
Current NTP status: ON
Allow/Restrict access to NTP clients: Allow

remote      refid      st t when poll reach  delay  offset  jitter
=====
60-56-214-78f2. .INIT.      16 u   -   64    0    0.000   0.000   0.000
106.247.248.106 .INIT.      16 u   -   64    0    0.000   0.000   0.000
>1. Configure NTP
  2. Stop NTP
  3. Restrict access to NTP clients
  4. Activate DDoS protection
  5. Add authorized subnet to sync by NTP
  6. Remove authorized subnet from NTP rules
  b. Back
  q. Quit to main Menu

```

2. From the NTP menu, choose option **1** to configure NTP.
3. At the prompt, do one of the following:
  - Type **y** for the OVOC server to act as both the NTP server and NTP client. Enter the IP addresses of the NTP servers to serve as the clock reference source for the NTP client (Up to four NTP servers can be configured).
  - Type **n** for the OVOC server to act as the NTP server only. The OVOC server is configured as a Stand-alone NTP server. The NTP process daemon starts and the NTP status information is displayed on the screen.

## Stopping and Starting the NTP Server

This section describes how to stop and start the NTP server.

### ➤ To start NTP services:

- From the NTP menu, choose option **2**, and then choose one of the following options:
  - If NTP Service is on: **Stop NTP**
  - If NTP Service is off: **Start NTP**

The NTP daemon process starts; when the process completes, you return to the NTP menu.

## Restrict Access to NTP Clients

This section describes how to restrict access to NTP clients.

### ➤ To allow access to NTP clients:

- From the NTP menu, choose option **3** to allow or restrict access to NTP clients; the screen is updated accordingly.

## Timezone Settings

This option enables you to change the timezone of the OVOC server.



The Apache server is automatically restarted after the timezone changes are confirmed.

➤ **To change the system timezone:**

1. From the Date & Time menu, choose Time Zone Settings, and then press Enter.
2. Enter the required time zone.
3. Type y to confirm the changes; the OVOC server restarts the Apache server for the changes to take effect.

## Date and Time

This option enables you to set the date and time.

➤ **To set the date and time:**

1. From the Date & Time menu, choose **Date & Time Settings**, and then press Enter; the current server time is displayed:

**Figure 22-3: Change System Time and Date Prompt**

```
Server's Time Is: [23/10/2013 09:56:38]  
New Time <mmddHHMMyyyy.SS> [1: ]
```

2. Enter the new time as shown in the following example:

```
mmddHHMMyyyy.SS : month(08),day(16),Hour(16),Minute(08),year(2007),". " Second.
```

## 23 Security

The OVOC Management security options enable you to perform security actions, such as configuring the SSH Server Configuration Manager, and user's administration.

➤ **To configure security settings:**

- From the OVOC Server Managerroot menu, choose **Security**, and then press Enter, the following is displayed:

**Figure 23-1: Security Settings**

```

Main Menu> Security
-----
>1.Add OVOC User
2.SSH
3.Oracle DB Password (OVOC Server will be stopped)
4.Cassandra DB Password (OVOC Server will be stopped)
5.OS Users Passwords
6.Apache Security Settings
7.File Integrity Checker
8.Software Integrity Checker (AIDE) and Prelinking
9.USB Storage
10.Network options
11.Audit Agent Options
12.Disable Statistics Report Web page Secured Communication (OVOC Server will be restarted)
13.Server Certificates Update
14.SEM - AudioCodes devices communication
q.Quit to main Menu
  
```

This menu includes the following options:

- Add OVOC User ([OVOC User](#) below)
- SSH ([SSH](#) on the next page)
- Oracle DB Password (EMS and SEM applications will be stopped) ([Oracle DB Password](#) on page 141)
- OS Users Password ([OS Users Passwords](#) on page 142)
- File Integrity Checker ([File Integrity Checker](#) on page 145)
- HTTP Security Settings ( [HTTP Security Settings](#) on page 154
- Software Integrity Checker (AIDE) and Pre-linking ([Software Integrity Checker \(AIDE\) and Pre-linking](#) on page 145)
- USB Storage ([USB Storage](#) on page 145)
- Network options ([Network Options](#) on page 146)
- Audit Agent Options ([Auditd Options](#) on page 147)
- HTTPS/SSL/TLS ([HTTPS/SSL/TLS Security](#) on page 147)

### OVOC User

This option enables you to add a new administrator user to the OVOC server database. This user can then log into the OVOC client. This option is advised to use for the operator's definition only in cases where all the OVOC application users are blocked and there is no way to perform an application login.

➤ **To add an OVOC user:**

1. From the Security menu, choose Add OVOC User, and then press Enter.
2. Enter the name of the user you wish to add.
3. Enter a password for the user.
4. Type **y** to confirm your changes.



Note and retain these passwords for future access.

## SSH

This section describes how to configure the OVOC server SSH connection properties using the SSH Server Configuration Manager.

➤ **To configure SSH:**

1. From the Security menu, choose **SSH**; the following is displayed:

**Figure 23-2: SSH Configuration**

```

Main Menu> Security> SSH
-----
>1. Configure SSH Log Level
2. Configure SSH Banner
3. Configure SSH on Ethernet Interfaces
4. Disable SSH Password Authentication
5. Enable SSH IgnoreUserKnownHosts parameter
6. Configure SSH Allowed Hosts
b. Back
q. Quit to main Menu
  
```

This menu includes the following options:

- Configure SSH Log Level ([SSH Log Level](#) below).
- Configure SSH Banner ([SSH Banner](#) on the next page).
- Configure SSH on Ethernet Interfaces ([SSH on Ethernet Interfaces](#) on the next page).
- Disable SSH Password Authentication ([Enable/Disable SSH Password Authentication](#) on page 138).
- Enable SSH Ignore User Known Hosts Parameter ([Enable SSH IgnoreUserKnownHosts Parameter](#) on page 138).
- Configure SSH Allowed Hosts ([SSH Allowed Hosts](#) on page 139).

## SSH Log Level

You can configure the log level of the SSH daemon server. The log files are found at the location `/var/log/secure` (older records are stored in `secure.1`, `secure.2` etc.).

➤ **To configure the SSH Log Level:**

1. From the SSH menu, choose option **1**, and then press Enter; the following is displayed.

Figure 23-3: SSH Log Level Manager

```

Main Menu> Security> SSH> Configure SSH Log Level
-----
LogLevel DEFAULT
Note: Changing LogLevel will restart SSH
>1. 1
2. FATAL
3. ERROR
4. INFO
5. VERBOSE
6. DEBUG
7. DEBUG1
8. DEBUG2
9. DEBUG3
10. DEFAULT
b. Back
q. Quit to main Menu

```

2. To configure the desired log level, choose the number corresponding to the desired level from the list, and then press Enter.

The SSH daemon restarts automatically.

The Log Level status is updated on the screen to the configured value.

## SSH Banner

The SSH Banner displays a pre-defined text message each time the user connects to the OVOC server using an SSH connection. You can customize this message. By default this option is disabled.

### ➤ To configure the SSH banner:

1. From the SSH menu, choose option 2, and then press Enter; the following is displayed:

Figure 23-4: SSH Banner Manager

```

Main Menu> Security> SSH> Configure SSH Banner
-----
Current Banner State: DISABLED
To change SSH Banner, please, change /etc/issue file.
Note: Changing Banner state will restart SSH
>1. 1
b. Back
q. Quit to main Menu

```

2. Edit a '/etc/issue' file with the desired text.
  3. Choose option 1 to enable or disable the SSH banner.
- Whenever you change the banner state, SSH is restarted.
- The 'Current Banner State' is displayed in the screen.

## SSH on Ethernet Interfaces

You can allow or deny SSH access separately for each network interface enabled on the OVOC server.

➤ **To configure SSH on Ethernet interfaces:**

- From the SSH menu, choose option **3**, and then press Enter; the following is displayed:

**Figure 23-5: Configure SSH on Ethernet Interfaces**

```

Main Menu> Security> SSH> Configure SSH on Ethernet Interfaces
-----
Ethernet Interfaces - SSH Manager:
SSH Listener Statuses:
    ALL - SSH enabled on all the Interfaces
    Yes - SSH enabled on specific Interface
    No  - SSH disabled on specific Interface

Interface : SSH Listener Status : IP Address      : Host Name
eth0       : ALL                : 10.3.180.7    : G8-Linux?
>1.Add SSH to All Ethernet Interfaces
2.Add SSH to Ethernet Interface
3.Remove SSH from Ethernet Interface
h.Back
q.Quit to main Menu
  
```

This menu includes the following options:

- Add SSH to All Ethernet Interfaces ([Add SSH to All Ethernet Interfaces](#) below).
- Add SSH to Ethernet Interface ([Add SSH to Ethernet Interface](#) below).
- Remove SSH from Ethernet Interface ([Remove SSH from Ethernet Interface](#) below).

## Add SSH to All Ethernet Interfaces

This option enables SSH access for all network interfaces currently enabled on the OVOC server.

➤ **To add SSH to All Ethernet Interfaces:**

- From the Configure SSH on Ethernet Interfaces menu, choose option **1**, and then press Enter.  
The SSH daemon restarts automatically to update this configuration action.  
The column 'SSH Listener Status' displays ALL for all interfaces.

## Add SSH to Ethernet Interface

This option enables you to allow SSH access separately for each network interface.

➤ **To add SSH to Ethernet Interfaces:**

1. From the Configure SSH on Ethernet Interfaces menu, choose option **2**, and then press Enter.  
After entering the appropriate sub-menu, all the interfaces upon which SSH access is currently disabled are displayed.
2. Enter the appropriate interface number, and then press Enter.  
The SSH daemon restarts automatically to update this configuration action.  
The column 'SSH Listener Status' displays 'YES' for the configured interface.

## Remove SSH from Ethernet Interface

This option enables you to deny SSH access separately for each network interface.

➤ **To deny SSH from a specific Ethernet Interface:**

1. From the Configure SSH on Ethernet Interfaces menu, choose option **3**, and then press Enter.  
All the interfaces to which SSH access is currently enabled are displayed.
2. Enter the desired interface number, and then press Enter.



The SSH daemon restarts automatically to update this configuration action.

The column 'SSH Listener Status' displays 'No' for the denied interface.



If you attempt to deny SSH access for the only enabled interface, a message is displayed informing you that such an action is not allowed.

## Enable/Disable SSH Password Authentication

This option enables you to disable the username/password authentication method for all network interfaces enabled on the OVOC server.

### ➤ To disable SSH Password Authentication:

1. From the SSH menu, choose option **4**, and then press Enter; the following is displayed:

**Figure 23-6: Disable Password Authentication**

```
Disable SSH Password Authentication:

Current SSH Password Authentication is ENABLED.

Note: Changing Password Authentication mode will restart SSH
Are you sure you want to Disable SSH Password Authentication?(y/n) █
```

2. Type **y** to disable SSH password authentication or **n** to enable, and then press Enter. The SSH daemon restarts automatically to update this configuration action.



Once you perform this action, you cannot reconnect to the OVOC server using User/Password authentication. Therefore, before you disable this authentication method, ensure that you provision an alternative SSH connection method. For example, using an RSA keys pair. For detailed instructions on how to perform such an action, see [www.junauza.com](http://www.junauza.com) or search the internet for an alternative method.

## Enable SSH IgnoreUserKnownHosts Parameter

This option enables you to disable the use of the '\$HOME/.ssh/known\_host' file with stored remote servers fingerprints.

### ➤ To enable SSH IgnoreUserKnownHosts parameter:

1. From the SSH menu, choose option **5**, and then press Enter; the following is displayed:

**Figure 23-7: SSH IgnoreUserKnownHosts Parameter - Confirm**

```
Enable SSH IgnoreUserKnownHosts parameter:

Current SSH IgnoreUserKnownHosts parameter value is NO.

Are you sure you want to Change SSH IgnoreUserKnownHosts value to YES?(y/n) y █
```

2. Type **y** to change this parameter value to either 'YES' or 'NO' or type **n** to leave as is, and then press Enter.

## SSH Allowed Hosts

This option enables you to define which hosts are allowed to connect to the OVOC server through SSH.

### ➤ To Configure SSH Allowed Hosts:

- From the SSH menu, choose option **6**, and then press Enter; the following is displayed:

**Figure 23-8: Configure SSH Allowed Hosts**

```

Main Menu> Security> SSH> Configure SSH Allowed Hosts
-----
SSH Allowed for ALL Hosts.
>1.Deny ALL Hosts
  2.Add Host/Subnet to Allowed Hosts
  b.Back
  q.Quit to main Menu
  
```

This menu includes the following options:

- Allow ALL Hosts ([Allow ALL Hosts](#) below).
- Deny ALL Hosts ([Deny ALL Hosts](#) below).
- Add Host/Subnet to Allowed Hosts ( [Add Hosts to Allowed Hosts](#) on the next page).
- Remove Host/Subnet from Allowed Hosts ([Remove Host/Subnet from Allowed Hosts](#) on page 141).

### Allow ALL Hosts

This option enables all remote hosts to access this OVOC server through the SSH connection (default).

### ➤ To allow ALL Hosts:

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter.
2. Type **y** to confirm, and then press Enter.

The appropriate status is displayed in the screen.

### Deny ALL Hosts

This option enables you to deny all remote hosts access to this OVOC server through the SSH connection.

### ➤ To deny all remote hosts access:

1. From the Configure SSH Allowed Hosts menu, choose option **2**, and then press Enter.
2. Type **y** to confirm, and then press Enter.

The appropriate status is displayed in the screen.



When this action is performed, the OVOC server is disconnected and you cannot reconnect to the OVOC server through SSH. Before you disable SSH access, ensure that you have provisioned alternative connection methods, for example, serial management connection or KVM connection.

## Add Hosts to Allowed Hosts

This option enables you to allow different SSH access methods to different remote hosts. You can provide the desired remote host IP, subnet or host name in order to connect to the OVOC server through SSH.

### ➤ To add Hosts to Allowed Hosts:

1. From the Configure SSH Allowed Hosts menu, choose option **3**, and then press Enter; the following is displayed:

**Figure 23-9: Add Host/Subnet to Allowed Hosts**

```

Main Menu> Security> SSH> Configure SSH Allowed Hosts> Add Host/Subnet to Allowed Hosts
-----
>1. Add IP Address (x.x.x.x)
2. Add Subnet (n.n.n.n/m.m.m.m - network/netmask)
3. Add Host Name (without "/" or "," characters)
b. Back
q. Quit to main Menu
  
```

2. Choose the desired option, and then press Enter.
3. Enter the desired IP address, subnet or host name, and then press Enter.



When adding a Host Name, ensure the following:

- Verify your remote host name appears in the DNS server database and your OVOC server has an access to the DNS server.
- Provide the host name of the desired network interface defined in “/etc/hosts” file.

4. Type **y** to confirm the entry, and then press Enter again.

If the entry is already included in the list of allowed hosts, an appropriate notification is displayed.

When the allowed hosts entry has been successfully added, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:

**Figure 23-10: Add Host/Subnet to Allowed Hosts-Configured Host**

```

Main Menu> Security> SSH> Configure SSH Allowed Hosts
-----
Current Allowed Hosts/Subnets:

IP Addresses:
10.13.22.3

1.Allow ALL Hosts
2.Deny ALL Hosts
>3.Add Host/Subnet to Allowed Hosts
4.Remove Host/Subnet from Allowed Hosts
b.Back
q.Quit to main Menu

```

## Remove Host/Subnet from Allowed Hosts

If you have already configured a list of allowed hosts IP addresses, you can then remove one or more of these host addresses from the list.

### ➤ To remove an existing allowed host's IP address:

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter; the following is displayed:
2. Choose the desired entry to remove from the Allowed Hosts list, i.e. to deny access to the OVOC server through SSH connection, and then press Enter again.
3. Type **y** to confirm the entry, and then press Enter again.

When the allowed hosts entry has been successfully removed, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:



When you remove either the only existing IP address, Subnet or Host Name in the Allowed Hosts in the Allowed Hosts list, the configuration is automatically set to the default state "Allow All Hosts".

## Oracle DB Password

This option enables you to change the default Oracle Database password "pass\_1234". The OVOC server shuts down automatically before changing the Oracle Database password.

### ➤ To change the DB Password:

1. From the Security menu, choose DB Password, and then press Enter; the OVOC server is rebooted.
2. Press Enter until the New Password prompt is displayed.

Figure 23-11: EMS Server Manager – Change DB Password

```

Do you really want to change DB password? Press Esc to quit or any key to continue...

*****
Oracle Change password Script start
*****
User name:
EMSADMIN
Current Password:
*****
The password should be at least 15 characters long, contain at least two digits, two lowercase
and two uppercase characters, two punctuation characters and should differ by more than
4 characters from the previous passwords.
New Password:

```

- a. Enter the new password, which should be at least 15 characters long, contain at least two digits, two lowercase and two uppercase characters, two punctuation characters and should differ by more than one character from the previous passwords.



- The OVOC server is rebooted when you change the Oracle Database password.
- Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the OVOC Oracle Database without them.

3. After validation, a message is displayed indicating that the password was changed successfully.

## OS Users Passwords

This section describes how to change the OS password settings.

### ➤ To change OS passwords:

1. From the Security menu, choose **OS Users Passwords**, and then press Enter.
2. Do one of the following:
  - Change General Password Settings ([General Password Settings](#) below).
  - Change User Password: at the prompt, enter the user name whose password you wish to change and follow the prompts

## General Password Settings

This option enables you to change the OS general password settings, such as 'Minimum Acceptable Password Length' and 'Enable User Block on Failed Login'. This feature also enables you to modify settings for a specific user, such as 'User's Password' and 'Password Validity Max Period'.

### ➤ To modify general password settings:

1. The Change General Password Settings prompt is displayed; type **y**, and then press Enter.
2. Do you want to change general password settings? (y/n)y
3. The Minimum Acceptable Password Length prompt is displayed; type 10, and then press Enter.

Minimum Acceptable Password Length [10]: 10

4. The Enable User Block on Failed Login prompt is displayed; type **y**, and then press Enter.

Enable User Block on Failed Login (y/n) [y] y

5. The Maximum Login Retries prompt is displayed; type **3**, and then press Enter.

Maximum Login Retries [3]: 3

6. The Failed Login Locking Timeout prompt is displayed; type **900**, and then press Enter.

Failed Login Locking Timeout [900]:900

7. You are prompted if you wish to continue; type **y**, and then press Enter.

Are you sure that you want to continue? (y/n/q) y

## Operating System User Security Extensions

This feature enables the administrator to configure the following additional user security extensions:

- Maximum allowed numbers of simultaneous open sessions.
- Inactivity time period (days) before the OS user is locked.

To configure these parameters, in the OS Passwords Settings menu, configure parameters according to the procedure below (see also green arrows indicating the relevant parameters to configure ).

### ➤ To configure operating system users security extensions:

1. The Change General Password Settings prompt is displayed; type **n**, and then press Enter.

Do you want to change general password settings ? (y/n) n

2. The Change password for a specific user prompt is displayed; type **y**, and then press Enter.

Do you want to change password for specific user ? (y/n) y

3. Enter the Username upon which you wish to configure, and then press Enter.

Enter Username [acems]:

4. The change User Password prompt is displayed; type **n**, and then press Enter.

Do you want to change its password ? (y/n) n

5. An additional Password prompt is displayed, type **y**, and then press Enter.

Do you want to change its login and password properties? (y/n) y

6. The Password Validity prompt is displayed; press Enter.

Password Validity Max Period (days) [90]:

7. The Password Update prompt is displayed; press Enter.

Password Update Min Period (days) [1]:

8. The Password Warning prompt is displayed; press Enter.

Password Warning Max Period (days) [7]:

9. The Maximum number of Simultaneous Open Sessions prompt is displayed; enter the number of simultaneous open SSH connections you wish to allow for this user.

Maximum allowed number of simultaneous open sessions [0]:

10. The Inactivity Days prompt is displayed; enter the number of inactivity days before the user is locked. For example, if you'd like to suspend a specific user if they have not connected to the OVOC server for a week, enter 7 days.

Days of inactivity before user is locked (days) [0]:

**Figure 23-12: OS Passwords Settings with Security Extensions**

```
OS Passwords Settings

Do you want to change general password settings? (y/n) n

Do you want to change password for specific user? (y/n) y
Enter Username [acems]: testuser

Do you want to change its password ? (y/n) n

Do you want to change its login and password properties? (y/n) y
Password Validity Max Period (days) [90]:
Password Update Min Period (days) [1]:
Password Warning Max Period (days) [7]:
Maximum allowed number of simultaneous open sessions [0]: 3
Days of inactivity before user is locked (days) [0]: 3

Are you sure that you want to continue? (y/n/q) y

Adjusting aging data for user testuser.
passwd: Success
Done.
```

If the user attempts to open more than three SSH sessions simultaneously, they are prompted and immediately disconnected from the fourth session as displayed in the figure below.

**Figure 23-13: Maximum Active SSH Sessions**

```
Connecting to 10.7.14.142:22...
Connection established.
Escape character is '^@]'.

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Jul 11 15:15:13 2011 from 10.7.2.31
Too many active sessions (4) for user acems

Connection closed by foreign host.
```



By default you can connect through SSH to the OVOC server with user *acems* only. If you configure an inactivity days limitation on this user, the situation may arise, for example, where a user is away for an extended period and has no active user to access the OVOC server. Therefore, we strongly recommend to use this limitation very carefully and preferably to configure this option for each user to connect to the OVOC server through SSH other than with the *acems* user.

## File Integrity Checker

The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported through OVOC Security Events. The File Integrity checker tool runs on the OVOC server machine.

- From the Security menu, choose **File Integrity Checker**, and then press Enter; the File Integrity Checker is started or stopped.

## Software Integrity Checker (AIDE) and Pre-linking

AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

Pre-linking is designed to decrease process startup time by loading each shared library into an address for which the linking of needed symbols has already been performed. After a binary has been pre-linked, the address where the shared libraries are loaded will no longer be random on a per-process basis. This is undesirable because it provides a stable address for an attacker to use during an exploitation attempt.

### ➤ To start AIDE and disable pre-linking:

1. From the Security menu, choose **Software Integrity Checker (AIDE) and Pre-linking**; the current status of these two processes is displayed:

**Figure 23-14: Software Integrity Checker (AIDE) and Pre-linking**

```
Software Integrity Checker <AIDE> and Prelinking:

Software integrity checker <AIDE> is disabled and Prelinking is enabled.
Enable integrity checker, and disable prelinking? <y/n>■
```

2. Do one of the following:
  - Type **y** to enable AIDE and disable pre-linking
  - Type **n** to disable AIDE and enable pre-linking.

## USB Storage

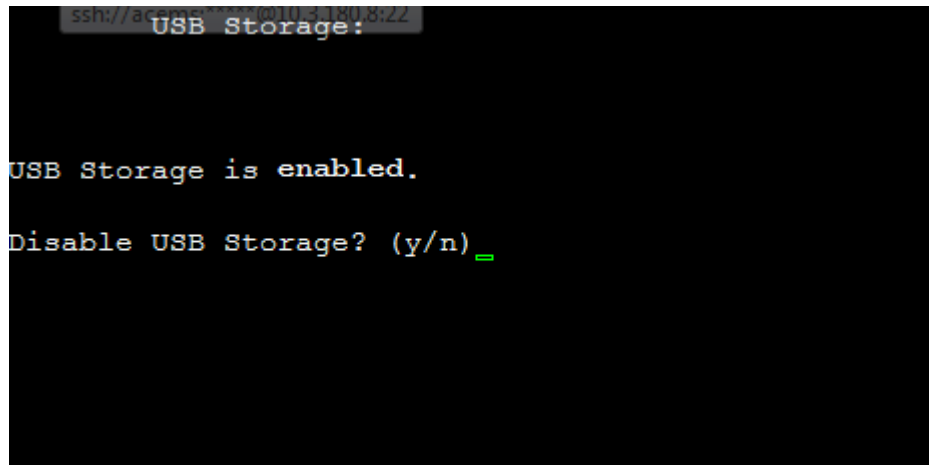
This menu option allows enabling or disabling the OVOC server's USB storage access as required.

### ➤ To enable USB storage:

1. From the Security menu, choose **USB Storage**; the following prompt is displayed:



Figure 23-15: USB Storage



2. Enable or disable USB storage as required.

## Network Options

This menu option provides the following options to enhance network security:

- Ignore Internet Control Message Protocol (ICMP) Echo requests:  
This option ensures that the OVOC server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.
- Ignore ICMP Echo and Timestamp requests:  
This option ensures that the OVOC server does not respond to an ICMP timestamp request to query for the current time. This reduces exposure to spoofing of the system time.
- Send ICMP Redirect Messages:  
This option disables the sending of ICMP Redirect Messages, which are generally sent only by routers.
- Ignore ICMP Redirect Messages:  
This option ensures that the OVOC server does not respond to ICMP Redirect broadcasts, and therefore such replies are always discarded.

This prevents an intruder from attempting to redirect traffic from the OVOC server to a different gateway or a non-existent gateway.

### ➤ To enable network options:

1. From the Security menu, choose **Network Options**; the following screen is displayed:

Figure 23-16: Network Options

```

-----
Main Menu> Security> Network options
-----
|Log packets with impossible addresses to kernel log: DISABLED
|Ignore all ICMP ECHO requests: DISABLED
|Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED
|Send ICMP redirect messages: DISABLED
|Accept ICMP redirect messages: DISABLED
>1.Enable log packets with impossible addresses to kernel log
2.Enable ignore all ICMP ECHO requests
3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
4.Enable send ICMP redirect messages
5.Enable accept ICMP redirect messages
b.Back
q.Quit to main Menu

```

1. Set the required network options.

## Auditd Options

Auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk. Using the Auditd option, you can change the auditd tool settings to comply with the Security Technical Information Guidelines (STIG) recommendations.

### ➤ To set Auditd options according to STIG:

1. From the Security menu, choose **Auditd Options**; the following screen is displayed:

Figure 23-17: Auditd Options

```

Auditd Options:

Not using STIG recommendations for auditd

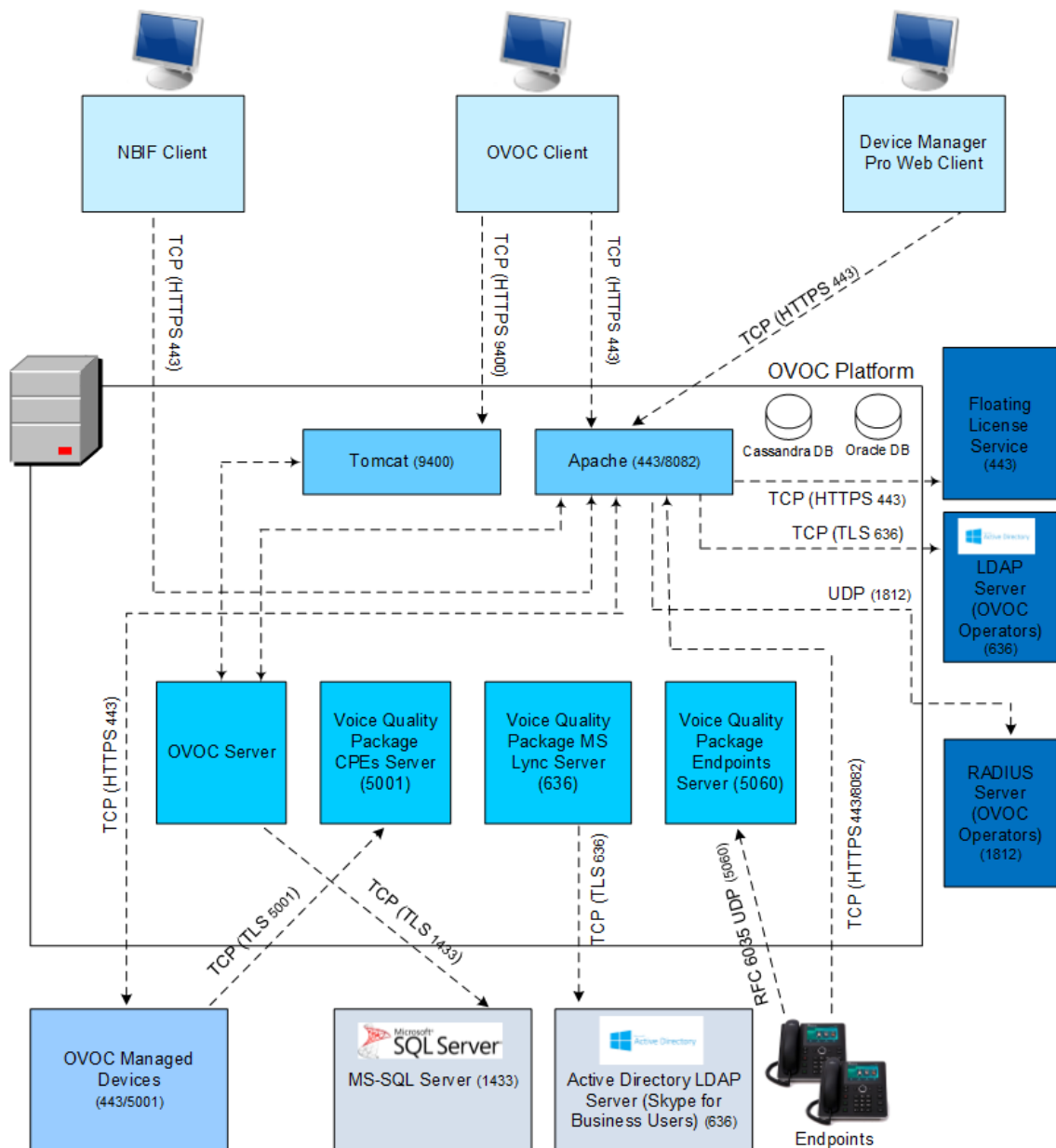
Change auditd settings according to STIG recommendations? (y/n) _

```

1. Enable or disable Auditd options as required.  
Audit records are saved in the following `/var/log/audit/` directory.

## HTTPS/SSL/TLS Security

This section describes the configuration settings for the HTTPS/SSL/TLS connections. The figure below shows the maximum security that can be implemented in the OVOC environment.

**Figure 23-18: OVOC Maximum Security Implementation**

- The above figure shows all the HTTPS/SSL/TLS connections in the OVOC network. Use this figure as an overview to the procedures described below. Note that not all of the connections shown in the above figure have corresponding procedures. For more information, refer to the OVOC Security Guidelines document.
- This version supports TLS versions 1.0, 1.1, and 1.2.

## Enable Statistics Report Web Page Secured Connection

This menu option enables you to secure the connection between the Statistics Report Web pages and the Tomcat server over HTTPS. When this option is enabled, the connection is secured through HTTPS port 9400 (instead of port 8400-HTTP).

➤ **To enable Statistics Report web pages over HTTPS:**

- From the Security menu, choose **Statistics Report Web page Secured Communication**; the connection is secured.

## Server Certificates Update

This menu option enables you to automatically generate custom SSL server certificates for securing connections between OVOC server and client processes. See . for an illustration of these connections.



If you are using self-generated certificates and private key, you can skip to step 4.

The procedure for server certificates update consists of the following steps:

1. **Step 1:** Generate Server Private Key.
2. **Step 2:** Generate Server Certificate Signing Request (CSR).
3. **Step 3:** Transfer the generated CSR file to your PC and send to CA.
4. **Step 4:** Transfer certificates files received from CA back to OVOC server.
5. **Step 5:** Import new certificates on OVOC server.
6. **Step 6:** Verify the installed Server certificate.
7. **Step 7:** Verify the installed Root certificate.
8. **Step 8:** Perform Supplementary procedures to complete certificate update process (refer to Appendix [Supplementary Security Procedures](#) on page 189 ).

➤ **To generate server certificates:**

1. From the Security menu, choose **Server Certificates Update**.

**Figure 23-19: Server Certificate Updates**

```

Main Menu> Security> Server Certificates Update
-----
Server's Certificate: Default
>1.Generate Server Private Key
2.Generate Server Certificate Signing Request (CSR)
3.Import Server Certificates from Certificate Authority (CA)
4.Display installed Server Certificate
5.Display installed Root Certificate
b.Back
q.Quit to main Menu
  
```

Information on the currently installed certificate is displayed (the currently installed certificate is the installation default).

➤ **Step 1: Generate a server private key:**

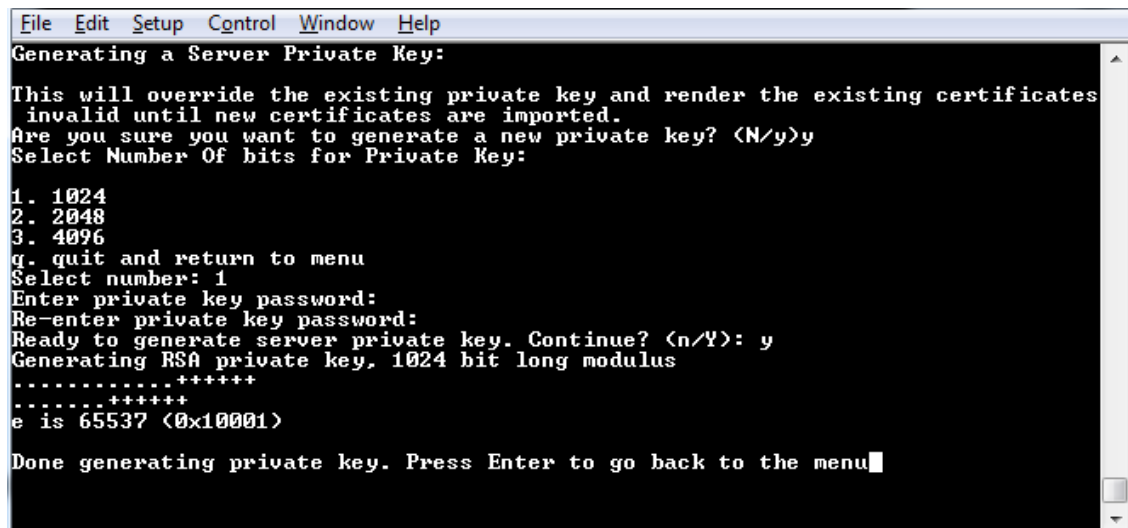
1. Select option **1**. The following screen is displayed:

Figure 23-20: Generate Server Private Key



2. Select the number of bits required for the server private key.
3. Enter and reenter the server private key password and type **Y** to continue.  
The private key is generated.

Figure 23-21: Server Private Key Generated



➤ **Step 2: Generate a CSR for the server:**

1. Select option 2.
2. Enter the private key password (the password that you entered in the procedure above).
3. Enter the Country Name code, state or province, locality, organization name, organization unit name, common name (server host name) and email address.
4. Enter a challenge password and optionally a company name.

You are notified that a server Certificate Signing Request has successfully been generated and saved to the specified location.

Figure 23-22: Generating a Server Certificate Signing Request (CSR)

```

File Edit Setup Control Window Help
Generating a Server Certificate Signing Request (CSR):
Enter the passphrase used in the server private key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name (full name) [Berkshire]:Berkshire
Locality Name (eg, city) [Newbury]:Newbury
Organization Name (eg, company) [My Company Ltd]:EA1
Organizational Unit Name (eg, section) []:Finance
Common Name (eg, your name or your server's hostname) []:EA1
Email Address []:Bradb@enterpriseA.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

```

➤ **Step 3: Transfer the CSR file to your PC and send to CA:**

- Transfer the CSR file from the /home/acems/server\_cert/server.csr directory to your PC and then send it to the Certificate Authority (CA). For instructions on transferring files, see Appendix [Transferring Files](#) on page 200.

Figure 23-23: Transfer CSR File to PC

```

File Edit Setup Control Window Help
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

A server certificate signing request was successfully generated and placed in /home
/acems/server_certs/server.csr
Please transfer this file to your PC, and send to the Certificate Authority (CA)

Press Enter to go back to the menu

```

➤ **Step 4: Transfer server certificates from the CA:**

- Transfer the files that you received from the CA to the /home/acems/server\_certs directory. The root certificate should have the name root.crt and that the server certificate should have the name server.crt. If you received intermediate certificates, then rename them to ca1.crt and ca2.crt. Make sure that all certificates are in PEM format. For instructions on transferring files, see Appendix [Transferring Files](#) on page 200.



Note: If your certificates are self-generated (you did not perform steps 1-3), the /home/acems/server\_certs directory does not exist; therefore you must create it using the following commands:

```

mkdir /home/acems/server_certs
chmod 777 /home/acems/server_certs

```

➤ **Step 5: Import certificates:**

- Select option **3** and follow the prompts.

The certificate files are installed.



- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
- Make sure that all certificates are in PEM format and appear as follows (see [Verifying and Converting Certificates](#) on page 201 for information on converting files):

-----BEGIN CERTIFICATE-----

```
MIIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGGA1UEAxMM
```

```
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTE1MDUwMzA4NTE0MFowKjET
```

...

```
Tl6vqn5l27Oq/24KbY9q6EK2Yc3K2EAadL2lF1jnb+yvREuewprOz6TEEuxNJol0
```

```
L6V8lzUYOfHrEiq/6g==
```

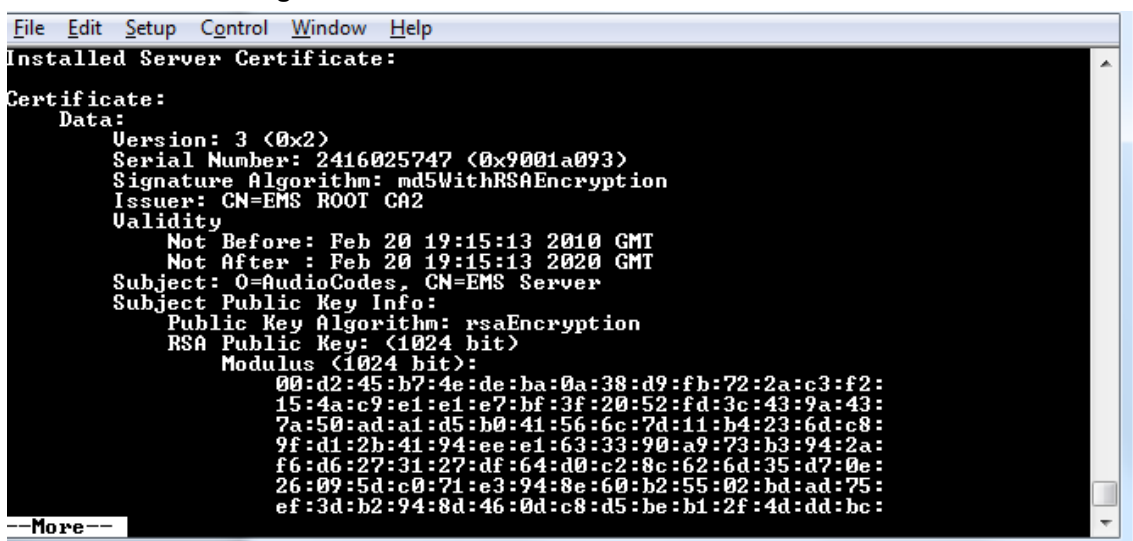
-----END CERTIFICATE-----

➤ **Step 6: Verify the installed server certificate:**

- Select option **4**.

The installed server certificate is displayed:

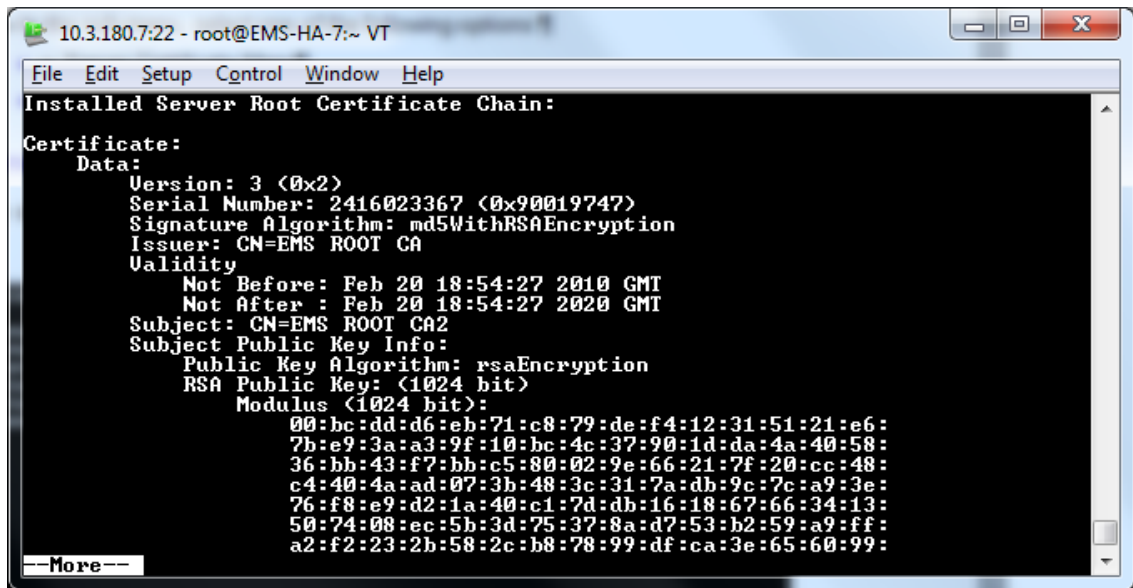
**Figure 23-24: Installed Server Certificate**



➤ **Step 7: Verify the installed root certificate:**

- Select Option **5**. The installed root certificate is displayed:

**Figure 23-25: Installed Root Certificate**



➤ **Step 8: Install device certificates and perform supplementary procedures**

- See [Supplementary Security Procedures](#) on page 189.

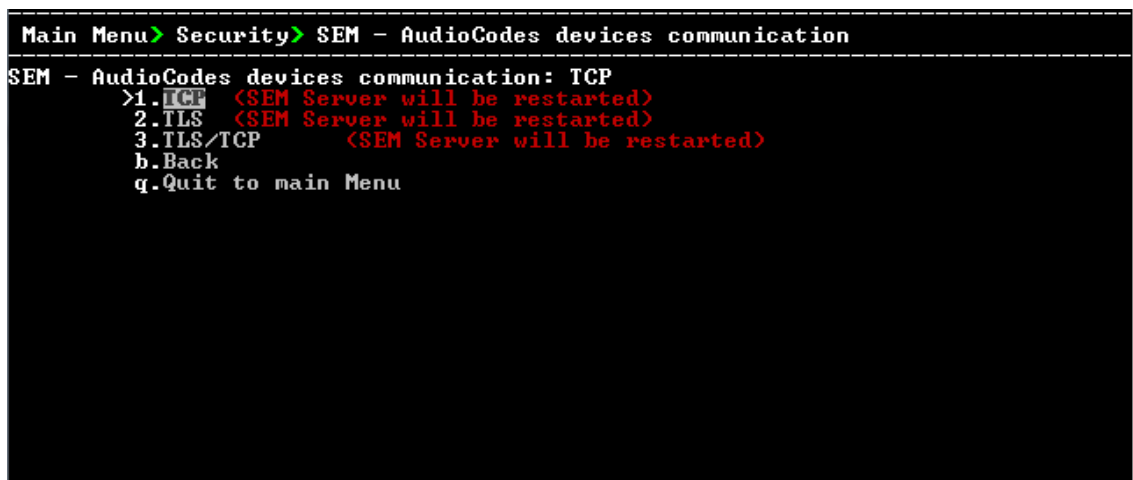
## OVOC Voice Quality Package - OVOC Managed Devices Communication

This option allows you to configure the transport type for the XML based OVOC Voice Quality Package communication from the OVOC managed devices to the OVOC server. You can enable the TCP port (port 5000), the TLS port (port 5001) connections or both port connections.

➤ **To configure the SEM - AudioCodes device communication:**

1. From the Security menu, select **SEM – AudioCodes device communication**.

**Figure 23-26: SEM - AudioCodes Device Communication**



2. Choose one of the following transport types:

- TCP (opens port 5000)
- TLS (opens port 5001)



- TLS/TCP (this setting opens both ports 5000 and 5001).

## HTTP Security Settings

From the OVOC Server Manager root menu, choose **HTTP Security Settings**.

```

Main Menu> Security> HTTP Security Settings
-----
!TLSv1.0: DISABLED
!TLSv1.1: DISABLED
!Cipher Suites Configuration String: !EDH:!AES:!RC4:!HIGH:!3DES:!aNULL
!Port 80 (HTTP): OPEN
!Port 8080 (IPPs FILES): OPEN
!Port 8081 (IPPs HTTP): OPEN
!Port 8082 (IPPs HTTPS): OPEN
!Port 911 (OVOC REST): OPEN
!Port 912 (Floating License REST): OPEN
!Port 915 (OVOC WebSocket): CLOSE
>1.Enable TLSv1.0 for Apache (Apache will be restarted)
2.Disable TLSv1.0 for Apache (Apache will be restarted)
3.Show allowed SSL Cipher Suites
4.Edit SSL Cipher Suites Configuration String (Apache will be restarted)
5.Restore SSL Cipher Suites Configuration Default (Apache will be restarted)
6.Close HTTP Service (Port 80)
7.Close IPP Files service (Port 8080)
8.Close IPPs HTTP (Port 8081)
9.Close IPPs HTTPS (Port 8082)
10.Close OVOC REST (Port 911)
11.Close Floating License REST (Port 912)
12.Open OVOC WebSocket (Port 915)
13.SBC HTTPS Authentication Mode
14.Enable IP Phone Manager Pro and NBIF Web pages Secured Communication (Apache will be restarted)
15.Change HTTP/S authentication password for NBIF directory (Apache will be restarted)
b.Back
q.Quit to main Menu

```

This menu allows you to configure the following Apache server security settings:

- TLS Version 1.0 ([TLS Version 1.0](#) below)
- TLS Version 1.1 ([TLS Version 1.1](#) on the next page)
- Show Allowed SSL Cipher Suites ([Show Allowed SSL Cipher Suites](#) on the next page)
- Edit SSL Cipher Suites Configuration String ([Edit SSL Cipher Suites Configuration String](#) on the next page)
- Restore SSL Cipher Suites Configuration Default ([Restore SSL Cipher Suites Configuration Default](#) on page 156)
- Manage HTTP Service (Port 80) ([Manage HTTP Service Port \(80\)](#) on page 156)
- Manage IPP Files Service (Port 8080) ([Manage IPP Files Service Port \(8080\)](#) on page 156)
- Manage IPPs HTTP (Port 8081) ([Manage IPPs HTTP Port \(8081\)](#) on page 157)
- Manage IPPs HTTPS (Port 8082) ([Manage IPPs HTTPS Port \(8082\)](#) on page 157)
- OVOC REST (Port 911) ([OVOC Rest \(Port 911\)](#) on page 157)
- Floating License REST (Port 912) ([Floating License \(Port 912\)](#) on page 157)
- OVOC WebSocket (Port 915) [OVOC WebSocket \(Port 915\)](#) on page 157
- SBC HTTPS Authentication ([SBC HTTPS Authentication Mode](#) on page 158 )
- Enable Device Manager Pro and NBIF Web Pages Secured Communication ( [Enable Device Manager Pro and NBIF Web Pages Secured Communication](#) on page 158)
- Change HTTP/S Authentication Password for NBIF Directory ( [Change HTTP/S Authentication Password for NBIF Directory](#) on page 159)

### TLS Version 1.0

This option enables/disables TLS Version 1.0 on port 443 (Apache server is restarted).

#### ➤ To enable or disable TLS Version 1.0:

- From the HTTP Security Settings menu, select option **Enable TLSv1.0 for Apache**.



When TLS Version 1.1 is disabled, TLS Version 1.0 is also disabled. Likewise, if TLS Version 1.0 is enabled, TLS Version 1.1 is also enabled.

Apache server is restarted. Default (enabled).

## TLS Version 1.1

This option enables/disables TLS Version 1.1 on port 443 (Apache server is restarted).

### ➤ To enable or disable TLS Version 1.1:

- From the HTTP Security Settings menu, select option **Enable TLSv1.1 for Apache**.  
Default (enabled). Apache server is restarted.



- When TLS Version 1.1 is disabled, TLS Version 1.0 is also disabled. Likewise, if TLS Version 1.0 is enabled, TLS Version 1.1 is also enabled.

## Show Allowed SSL Cipher Suites

This option allows you to view the currently configured SSL cipher suites.

### ➤ To show allowed SSL cipher suites:

1. From the HTTP Security Settings menu, select option **Show Allowed SSL Cipher Suites**.  
The currently configured SSL cipher suites are displayed. The overall figure indicates the total number of entries.

**Figure 23-27: Show Allowed SSL Cipher Suites**

File	Edit	Setup	Control	Window	Help
>	AES				
DH-RSA-AES128-GCM-SHA256			TLSv1.2	DH/RSA	DH
>	AES				
DH-RSA-AES128-SHA256			TLSv1.2	DH/RSA	DH
>	AES				
DH-DSS-AES128-SHA256			TLSv1.2	DH/DSS	DH
>	AES				
ECDH-RSA-AES128-GCM-SHA256			TLSv1.2	ECDH/RSA	ECDH
>	AES				
ECDH-ECDSA-AES128-GCM-SHA256			TLSv1.2	ECDH/ECDSA	ECDH
>	AES				
ECDH-RSA-AES128-SHA256			TLSv1.2	ECDH/RSA	ECDH
>	AES				
ECDH-ECDSA-AES128-SHA256			TLSv1.2	ECDH/ECDSA	ECDH
>	AES				
AES128-GCM-SHA256			TLSv1.2	RSA	RSA
>	AES				
AES128-SHA256			TLSv1.2	RSA	RSA
>	AES				
Overall: 28					
Press ENTER to continue...					

## Edit SSL Cipher Suites Configuration String

This option allows you to edit the SSL Cipher Suites configuration string.

### ➤ To edit the SSL cipher suites configuration string:

1. From the HTTP Security Settings menu, select option **Edit SSL Cipher Suites Configuration String**.

Figure 23-28: Show SSL Cipher Suites Configuration

```

File Edit Setup Control Window Help
> AEAD
DH-RSA-AES128-GCM-SHA256      TLSv1.2  DH/RSA    DH      AESGCM<128>
> AEAD
DH-RSA-AES128-SHA256         TLSv1.2  DH/RSA    DH      AES<128>
SHA256
DH-DSS-AES128-SHA256         TLSv1.2  DH/DSS    DH      AES<128>
SHA256
ECDH-RSA-AES128-GCM-SHA256   TLSv1.2  ECDH/RSA  ECDH    AESGCM<128>
> AEAD
ECDH-ECDSA-AES128-GCM-SHA256 TLSv1.2  ECDH/ECDSA ECDH    AESGCM<128>
> AEAD
ECDH-RSA-AES128-SHA256       TLSv1.2  ECDH/RSA  ECDH    AES<128>
SHA256
ECDH-ECDSA-AES128-SHA256     TLSv1.2  ECDH/ECDSA ECDH    AES<128>
SHA256
AES128-GCM-SHA256             TLSv1.2  RSA       RSA     AESGCM<128>
> AEAD
AES128-SHA256                 TLSv1.2  RSA       RSA     AES<128>
SHA256

Overall: 28

New configuration: !EDH:!ADH:!DSS:!RC4-HIGH:!3DES:!aNULL
Would you like to apply this configuration? (y/n/q)

```

2. Edit the new configuration and select **y** to apply the changes.
3. Run the **Show Allowed SSL Cipher Suites** command to display the new configuration.

## Restore SSL Cipher Suites Configuration Default

This option allows you to restore the SSL Cipher Suites to the OVOC default values.

- **To restore the SSL Cipher Suites Configuration default:**
  - From the HTTP Security Settings menu, select **Restore SSL Cipher Suites Configuration Default**.

## Manage HTTP Service Port (80)

- **To open/close HTTP Service (Port 80):**
  - In the HTTP Security Settings menu, choose option **Open/Close HTTP Service (Port 80)**, and then press Enter.

This HTTP port is used for the connection between the OVOC server and all AudioCodes devices with the Device Manager Pro Web browser

## Manage IPP Files Service Port (8080)

- **To open/close IPPs files service (port 8080):**
  - In the HTTP Security Settings menu, choose option **Open/Close IPPs files(Port 8080)**, and then press Enter.

This HTTP port is used for downloading firmware and configuration files from the OVOC server to the endpoints.



This option is reserved for backward compatibility with older device versions.

## Manage IPPs HTTP Port (8081)

### ➤ To open/close IPPs HTTP (Port 8081):

- In the HTTP Security Settings menu, choose option **Open/Close IPPs HTTP (Port 8081)**, and then press Enter.

This HTTP port is used for sending REST updates from the endpoints to the OVOC server, such as alarms and statuses.



This option is reserved for backward compatibility with older device versions.

## Manage IPPs HTTPS Port (8082)

### ➤ To open/close IPPs HTTPS (Port 8082):

- In the HTTP Security Settings menu, choose option **Open/Close IPPs HTTPS (Port 8082)**, and then press Enter.

This HTTPS port is used for sending secure REST updates from the endpoints to the OVOC server, such as alarms and statuses (HTTPS without certificate authentication).



This option is reserved for backward compatibility with older device versions.

## OVOC Rest (Port 911)

This option allows you to open and close the REST port connection for (internal) port and server debugging.

### ➤ To configure OVOC REST:

1. From the HTTP Security Settings menu, choose option **Open/Close OVOC REST (Port 911)**.

## Floating License (Port 912)

This option allows you to open and close the Floating license REST service (internal) and Floating license service debugging.

### ➤ To open/close the Floating License port:

1. From the HTTP Security Settings menu, choose option **Open/Close Floating License REST (Port 912)**.

## OVOC WebSocket (Port 915)

This option allows you to open and close the OVOC WebSocket (Port 915) connection between the Websocket client and OVOC server.

### ➤ To open/close the WebSocket port:

1. From the HTTP Security Settings menu, choose option **Open/Close OVOC WebSocket (Port 915)**.

## SBC HTTPS Authentication Mode

This option enables you to configure whether certificates are used to authenticate the connection between the OVOC server and the devices in one direction or in both directions:

- **Mutual Authentication:** the OVOC authenticates the device connection request using certificates and the device authenticates the OVOC connection request using certificates. When this option is configured:
  - The same root CA must sign the certificate that is loaded to the device and certificate that is loaded to the OVOC server.
  - Mutual authentication must also be enabled on the device ( [Step 5: Configure HTTPS Parameters on the Device](#) on page 192).
- **One-way Authentication option:** the OVOC does not authenticate the device connection request using certificates; only the device authenticates the OVOC connection request.



You can use the procedure described in [Server Certificates Update](#) on page 149 to load the certificate file to the OVOC server.

### ➤ To enable HTTPS authentication:

1. In the HTTP Security Settings menu, choose the **SBC HTTPS Authentication** option.

**Figure 23-29: SBC HTTPS Authentication**

```

Main Menu> Security> Apache Security Settings> SBC HTTPS Authentication Mode
-----
HTTPS Authentication: Mutual
>1.Set Mutual Authentication
  2.Set One-Way Authentication
  b.Back
  q.Quit to main Menu
  
```

2. Choose one of the following options:
  - 1-Set Mutual Authentication
  - 2. Set One-Way Authentication

## Enable Device Manager Pro and NBIF Web Pages Secured Communication

This menu option enables you to secure the connection between the Device Manager Server and NBIF Web pages and the Apache server over HTTPS. When this option is enabled, the connection is secured through HTTPS port 443 (instead of port 80-HTTP).

- **To secure connection the Device Manager Pro and NBIF Web pages connection:**
  - From the HTTP Security Settings menu, choose **IP Phone Manager and NBIF Web pages Secured Communication**; the connection is secured.

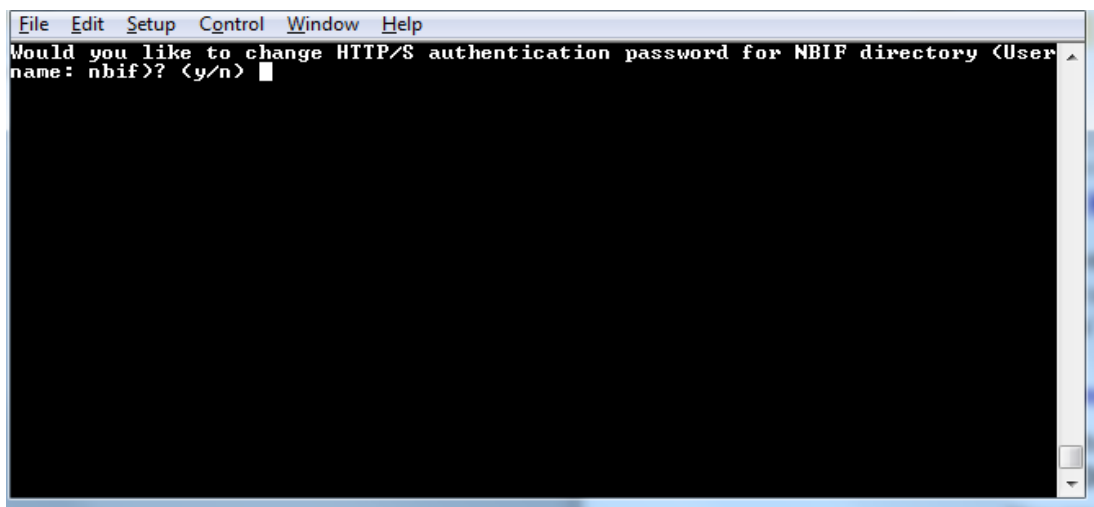
### Change HTTP/S Authentication Password for NBIF Directory

This option enables you to change the password for logging to the OVOC client from a NBIF client over an HTTP/S connection. The default user name is “nbif” and default password is “pass\_1234”.

- **To change the HTTP/S authentication password:**
  1. From the HTTP Security Settings menu, select **Change HTTP/S Authentication Password for NBIF Directory**.

You are prompted to change the HTTP/S authentication password. Enter **y** to change the password.

**Figure 23-30: Change HTTP/S Authentication Password for NBIF Directory**



2. Enter the new password.
3. Reenter the new password.

A confirmation message is displayed and the Apache server is restarted.

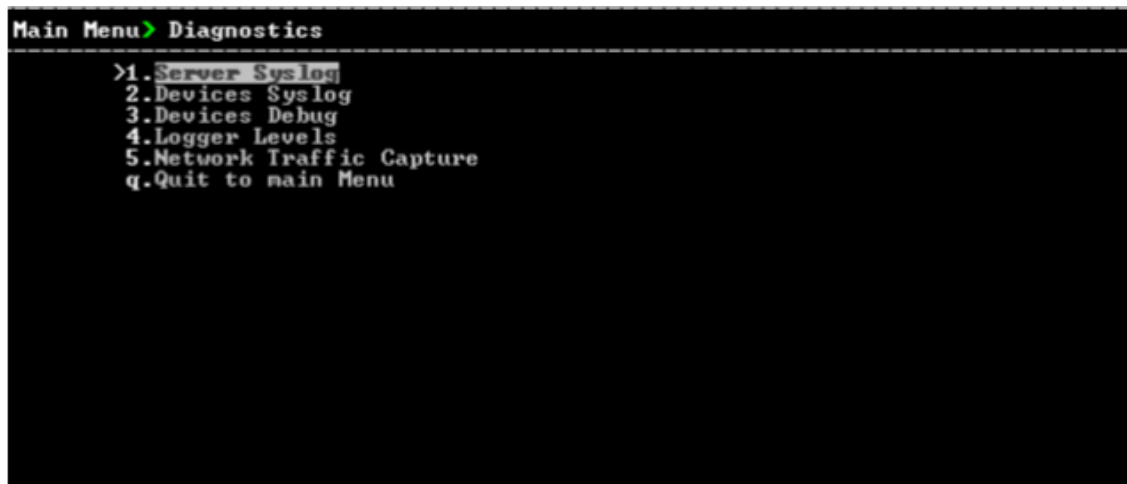
## 24 Diagnostics

This section describes the diagnostics procedures provided by the OVOC Server Manager.

➤ **To run OVOC server diagnostics:**

- From the OVOC Server ManagerRoot menu, choose **Diagnostics**, and then press Enter, the following is displayed:

**Figure 24-1: Diagnostics**



This menu includes the following options:

- Server Syslog Configuration ([Server Syslog Configuration](#) below).
- Devices Syslog Configuration ([Devices Syslog Configuration](#) on page 162).
- Devices Debug Configuration ([Devices Debug Configuration](#) on page 162).
- ServerLogger Levels ([Server Logger Levels](#) on page 163)
- Network Traffic Capture (see [Network Traffic Capture](#) on page 164)

### Server Syslog Configuration

This section describes how to send OVOC server Operating System (OS)-related syslog EMERG events to the system console and other OVOC server OS related messages to a designated external server.

➤ **To send EMERG event to the syslog console and other events to an external server:**

1. From the Diagnostics menu, choose **Server Syslog**, and then press Enter.
2. To send EMERG events to the system console, type **y**, press Enter, and then confirm by typing **y** again.

**Figure 24-2: Syslog Configuration**

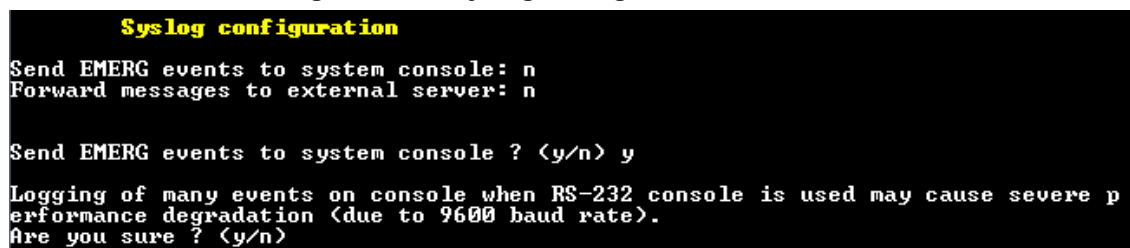


Figure 24-3: Forward Messages to an External Server

```

Forward messages to external server? (Server will reboot if settings changed) (y/n) y
  Facility (choose from this list):
*
AUTH
AUTHPRIV
CRON
DAEMON
FTP
KERN
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7
LPR
MAIL
NEWS
SYSLOG
USER
UUCP
[]: SYSLOG
  Severity (choose from this list):
EMERG
ALERT
CRIT
ERR
WARNING
NOTICE
INFO
DEBUG
[]: DEBUG
  Hostname[]: █

```

3. You are prompted to forward messages to an external server, type **y**, and then press Enter. If this is changed, the server is rebooted.
4. Type one of the following **Facilities** from the list (case-sensitive) or select the wildcard **\*** to select all facilities in the list, and then press Enter:
  - **auth** and **authpriv**: for authentication;
  - **cron**: comes from task scheduling services, **cron** and **atd**;
  - **daemon**: affects a daemon without any special classification (**DNS**, **NTP**, etc.)
  - **ftp**: concerns the **FTP** server;
  - **kern**: message coming from the kernel;
  - **lpr**: comes from the printing subsystem;
  - **mail**: comes from the e-mail subsystem;
  - **news**: Usenet subsystem message (especially from an **NNTP** — Network News Transfer Protocol — server that manages newsgroups);
  - **syslog**: messages from the **syslogd** server, itself;
  - **user**: user messages (generic);
  - **uucp**: messages from the **UUCP** server (Unix to Unix Copy Program, an old protocol notably used to distribute e-mail messages);
  - **local0** to **local7**: reserved for local use.
5. Each message is also associated with a **Severity** or priority level. Type one of the following severities (in decreasing order) and then press Enter:
  - **emerg**: “Help!” There’s an emergency, the system is probably unusable.



- **alert**: hurry up, any delay can be dangerous, action must be taken immediately;
- **crit**: conditions are critical;
- **err**: error;
- **warn**: warning (potential error);
- **notice**: conditions are normal, but the message is important;
- **info**: informative message;
- **debug**: debugging message.

6. Type the external server Hostname or IP address to which you wish to send the syslog.

## Devices Syslog Configuration

The capture of the device's Syslog can be logged directly to the OVOC server without the need for a third-party Syslog server in the same local network. The OVOC Server Manager is used to enable this feature.



Syslog is captured according to the device's configured Syslog parameters. For more information, see the relevant device User's manual.

The user needs to also enable the monitored device to send syslog messages to the standard syslog port (UDP 514) on the OVOC server machine.

The syslog log file 'syslog' is located in the following OVOC server directory:

/data/NBIF/mgDebug/syslog

The syslog file is automatically rotated once a week or when it reaches 100 MB. Up to four syslog files are stored.

### ➤ To enable device syslog logging:

1. From the Diagnostics menu, choose **Devices Syslog**, and then press Enter.
2. You are prompted whether you wish to send EMER events to system console; type **Y** or **N**.
3. You are prompted whether you wish to send events to an external server; type **Y** or **N**.

## Devices Debug Configuration

Debug recordings packets from all managed machines can be logged directly to the OVOC server without the need for a 3<sup>rd</sup> party network sniffer in the same local network.



Debug recording packets are collected according to the AudioCodes device's configured Debug parameters. For more information, see the relevant device User's Manual.

The OVOC server runs the Wireshark network sniffer, which listens on a particular configured port. The sniffer records the packets to a network capture file in the Debug Recording (DR) directory. You can then access this file from your PC through FTP.

The OVOC Server Manager is used to enable this feature. The user should configure the monitored device to send its debug record messages to a specific port (UDP 925) on the OVOC server IP.

The DR capture file is located in the following OVOC server directory:

/data/NBIF/mgDebug/DebugRecording

The file 'TPDebugRec<DATE>.cap' is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one

hour of recording (the first rule which is met causes the file to close i.e. if the file reaches 10MB in less than an hour of recording, it is closed). A cleanup process is run daily, deleting capture files that are 5 days old.

The user is able to retrieve this file from the OVOC server and open it locally on their own PC using Wireshark with the debug recording plug-in installed (Wireshark version 1.6.2 supports the Debug Recording plug-in).

➤ **To enable or disable devices debug:**

1. From the Diagnostics menu, choose **Devices Debug**, and then press Enter.  
A message is displayed indicating that debug recording is either enabled or disabled.
2. Type **y**, and then press Enter.  
Recording files are saved in /data/NBIF/mgDebug directory on the server.



It is highly recommended to disable the 'TP Debug Recording' feature when you have completed recording because this feature heavily utilizes system resources.

## Server Logger Levels

This option allows you to change the log level for the different OVOC server log directories.



After completing the debugging, revert to the previous configuration to prevent over utilization of CPU resources.

➤ **To change the <tc> server logger level:**

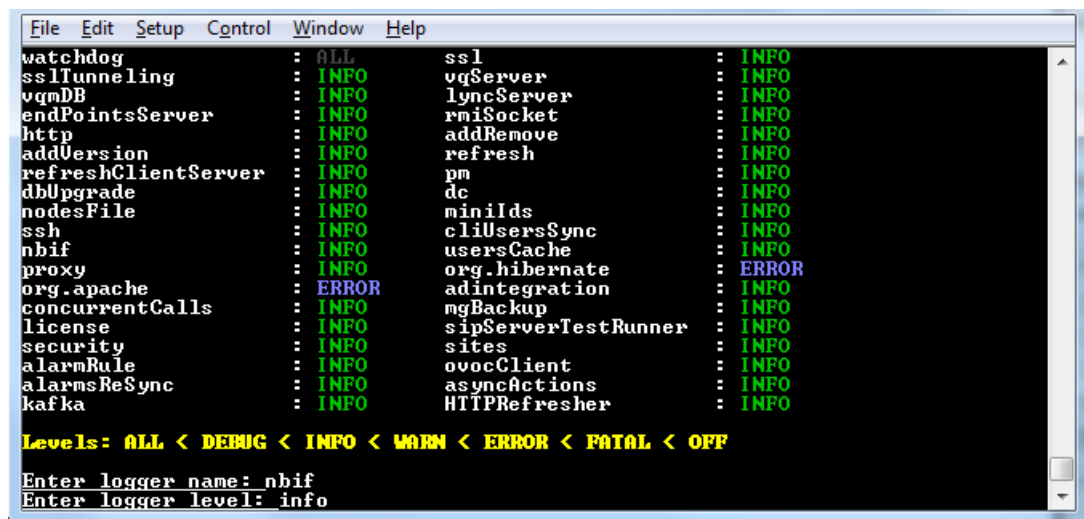
1. From the Diagnostics menu, choose **Logger Levels**.
2. Enter the name of the log whose level you wish to change.
3. Enter the desired logger level.
4. Select **Yes** at the prompt to confirm the change.

**Figure 24-4: Server Logger Name and Level**

Logger Name	Current Level
osu	DEBUG
watchdog	ALL
sslTunneling	INFO
vqmDB	INFO
endPointsServer	INFO
http	INFO
addVersion	INFO
refreshClientServer	INFO
dbUpgrade	INFO
nodesFile	INFO
ssh	INFO
nbif	INFO
proxy	INFO
org.apache	ERROR
concurrentCalls	INFO
license	INFO
security	INFO
alarmRule	INFO
alarmsReSync	INFO
kafka	INFO
v52	INFO
ssl	INFO
vgServer	INFO
lyncServer	INFO
rmiSocket	INFO
addRemove	INFO
refresh	INFO
pm	INFO
dc	INFO
miniIds	INFO
cliUsersSync	INFO
usersCache	INFO
org.hibernate	ERROR
adintegration	INFO
mgBackup	INFO
sipServerTestRunner	INFO
sites	INFO
ovocClient	INFO
asyncActions	INFO
HTTPRefresher	INFO

Levels: ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

Enter logger name: \_\_\_\_\_



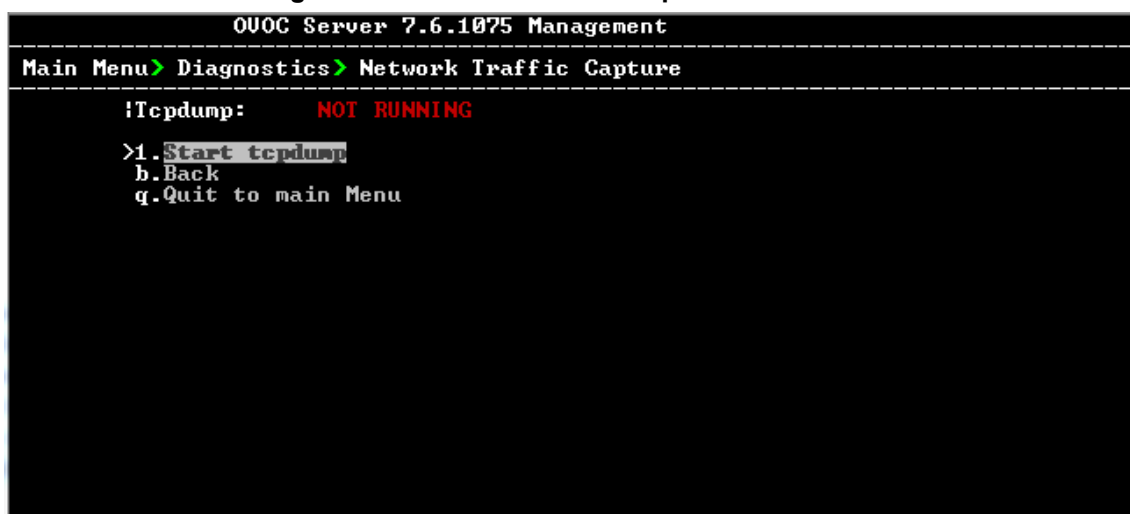
## Network Traffic Capture

Network traffic can be captured to a PCAP capture file according to a list of IP addresses and ports and a specified time period. The PCAP files can later be opened with a network sniffer program such as Wireshark.

### ➤ To capture TCP traffic:

1. From the Diagnostics menu, choose option **Network Traffic Capture**.

Figure 24-5: Network Traffic Capture



2. Select option **1 Start tcpdump**.
3. Select **y** to start the tcpdump.

Figure 24-6: TCP Dump

```

Would you like to start tcpdump capture? <y/n> y
At any stage, enter 'q' to abort and exit
IP(s) <comma-separated, or any>: any
Port(s) <comma-separated, or any>: 80,443,162,1161
Capture time <minutes, 1-60>: 10

```

4. Enter comma separated IP address (es) or accept the default "any" IP address.
5. Enter comma separated port (s) or accept the default "any".
6. Enter the capture time (in minutes). Default: network traffic for the last ten minutes is captured.

```

Starting tcpdump capture with the following parameters:
IP: any
Port: 80,443,162,1161
Time: 10 min
Proceed? <y/n/q> 

```

7. Select **y** to proceed.

Figure 24-7: TCP Dump Running

```

Main Menu> Diagnostics> Network Traffic Capture
-----
!Tcpdump:      RUNNING
!PID:          5713
!Start time:   09:57:00 13.02.19
!Run timeout:  10 minutes
!Port Filter:  80 or 443 or 162 or 1161
!Output file:  /var/log/ems/capture/190213095700_capture.pcap#ID

>1. Stop tcpdump
  b.Back
  q.Quit to main Menu

```

# Part VI

## Configuring the Firewall

This part describes how to configure the OVOC firewall.

## 25 Configuring the Firewall

The OVOC interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. You need to define firewall rules to secure communications for the OVOC client-server processes. Each of these processes use different communication ports. By default, all ports are open on the OVOC server side. When installing the OVOC server, you need to configure its network and open the ports in your Enterprise LAN according to your site requirements; based on the firewall configuration rules (representing these port connections) that are described in the table and figure below.

**Table 25-1: Firewall Configuration Rules**

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC Clients and OVOC server					
TCP/IP client ↔ OVOC server	TCP	√	22	SSH communication between OVOC server and TCP/IP client. Initiator: client PC	OVOC server side / Bi-directional.
HTTPS/NBIF Clients ↔ OVOC server	TCP (HTTPS)	√	443	Connection for OVOC/ NBIF clients. Initiator: Client	OVOC server side / Bi-directional
REST client ↔ OVOC Communication	TCP (HTTP)	×	911	Connection for OVOC server REST (internal) port and server debugging. Initiator (internal): OVOC server Initiator (debugging): REST client	OVOC server side / Bi-directional
	TCP (HTTP)	×	912	Floating license REST service (internal) communication and Floating license service debugging. Initiator (internal): OVOC server Initiator (debugging): REST client	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
WebSocket Client ↔ OVOC Server Communication	TCP (HTTP)	√	915	WebSocket Client and OVOC Server communication (internal) according to RFC 6455, used for managing the alarm and task notification mechanism in the OVOC Web. Initiator (internal): WebSocket Client	OVOC server side / Bi-directional
OVOC server and OVOC Managed Devices					
Device ↔ OVOC server (SNMP)	UDP	√	1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Initiator: AudioCodes OVOC managed device	OVOC server side / Receive only
	UDP	√	162	SNMP trap listening port on the OVOC server. Initiator: AudioCodes OVOC managed device	OVOC server side / Receive only
	UDP	√	161	SNMP Trap Manager port on the device that is used to send traps to the OVOC server. Initiator: OVOC server	AudioCodes OVOC managed device side / Bi-directional
Device ↔ OVOC server (NTP Server)	UDP (NTP server)	×	123	NTP server synchronization. Initiator: AudioCodes OVOC managed device (and OVOC server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Device ↔ OVOC server	TCP (HTTP)	×	80	HTTP connection for files transfer and REST communication. Initiator: OVOC server	OVOC server side / Bi-directional
	TCP (HTTPS)	√	443	HTTPS connection for files transfer (upload and download) and REST communication. Initiator: OVOC server	OVOC server side / Bi-directional
Device ↔ OVOC server Floating License Management	TCP (HTTPS)	√	443	HTTPS connection for files transfer (upload and download) and REST communication for device Floating License Management. Initiator: AudioCodes OVOC managed device	OVOC server side / Bi-directional
Device Manager Connections					
OVOC server ↔ Device Manager Pro	TCP (HTTP)	×	80	HTTP connection between the OVOC server and the Device Manager Pro Web browser. Initiator: Client browser	OVOC server side / Bi-Directional.
				HTTP connection that is used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoint	
	TCP	√	443	HTTPS connection	OVOC



Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	(HTTPS)			between the OVOC server and the Device Manager Pro Web browser. Initiator: Client browser	server side / Bi-Directional.
				HTTPS connection used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoint	
OVOC server ↔ Endpoints (used for backward compatibility)	TCP (HTTP)	×	8080	HTTP connection that is used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoint	OVOC server side / Bi-directional
	TCP (HTTP)	×	8081	HTTP REST updates connection. It is recommended to use this connection when managing more than 5000 IP Phones. In this case, you should change the provisioning URL port from 80 to 8081 in the phone's configuration file. Initiator: Endpoint	OVOC server side / Bi-directional
	TCP (HTTPS)	√	8082	HTTPS REST updates connection (encryption only without SSL authentication). It is recommended	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				to use this connection when managing more than 5000 IP Phones. In this case, you should change the provisioning URL port from 443 to 8082 in the phone's configuration file. Initiator: Endpoint	
OVOC Voice Quality Package Server and OVOC Managed Devices					
Media Gateways ↔ Voice Quality Package	TCP	×	5000	XML-based communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes OVOC managed device	OVOC server side / Bi-directional
	TCP (TLS)	√	5001	XML-based TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes - OVOC managed device	OVOC server side / Bi-directional
Statistics Reports					
Statistics Reports client page ↔ Tomcat server	TCP (HTTPS)	√	9400	HTTPS connection that is used for generating Statistics Reports. Initiator: Client's Web browser (Statistics Report page).	OVOC server side / Bi-directional
Skype for Business MS-SQL Server					
OVOC Voice Quality	TCP	√	1433	Connection between the OVOC	Skype for Business

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Package server ↔ Skype for Business MS-SQL Server				server and the MS-SQL Skype for Business Server. This port should be configured with SSL. Initiator: OVOC server	SQL server side / Bi-directional
LDAP Active Directory Server					
OVOC Voice Quality Package server ↔ Active Directory LDAP server (Skype for Business user authentication)	TCP	✖	389	Connection between the SEM server and the Active Directory LDAP server. Initiator: OVOC server	Active Directory server side / Bi-directional
	TCP (TLS)	√	636	Connection between the SEM server and the Active Directory LDAP server with SSL configured. Initiator: OVOC server	Active Directory server side / Bi-directional
OVOC server ↔ Active Directory LDAP server (OVOC user authentication)	TCP	✖	389	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users). Initiator: OVOC server	Active Directory server side / Bi-directional
	TCP (TLS)	√	636	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users) with SSL configured. Initiator: OVOC server	Active Directory server side / Bi-directional
RADIUS Server					

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC server ↔ RADIUS server	TCP	×	1812	Direct connection between the OVOC server and the RADIUS server (when OVOC user is authenticated using RADIUS server). Initiator: OVOC server	OVOC server side / Bi-directional
AudioCodes Floating License Service					
OVOC server ↔ AudioCodes Floating License Service	TCP	√	443	HTTPS for OVOC/ Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi-directional
Mail and Syslog Servers					
OVOC server ↔ Mail Server	TCP	×	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional
OVOC server ↔ Syslog Server	TCP	×	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side / Bi-directional
RFC 6035					
OVOC Voice Quality Package server ↔ Endpoints	UDP	×	5060	SIP Publish reports sent to the SEM server from the endpoints, including RFC 6035 SIP PUBLISH for reporting device voice quality metrics. Initiator: Endpoint	SEM server / Bi-directional

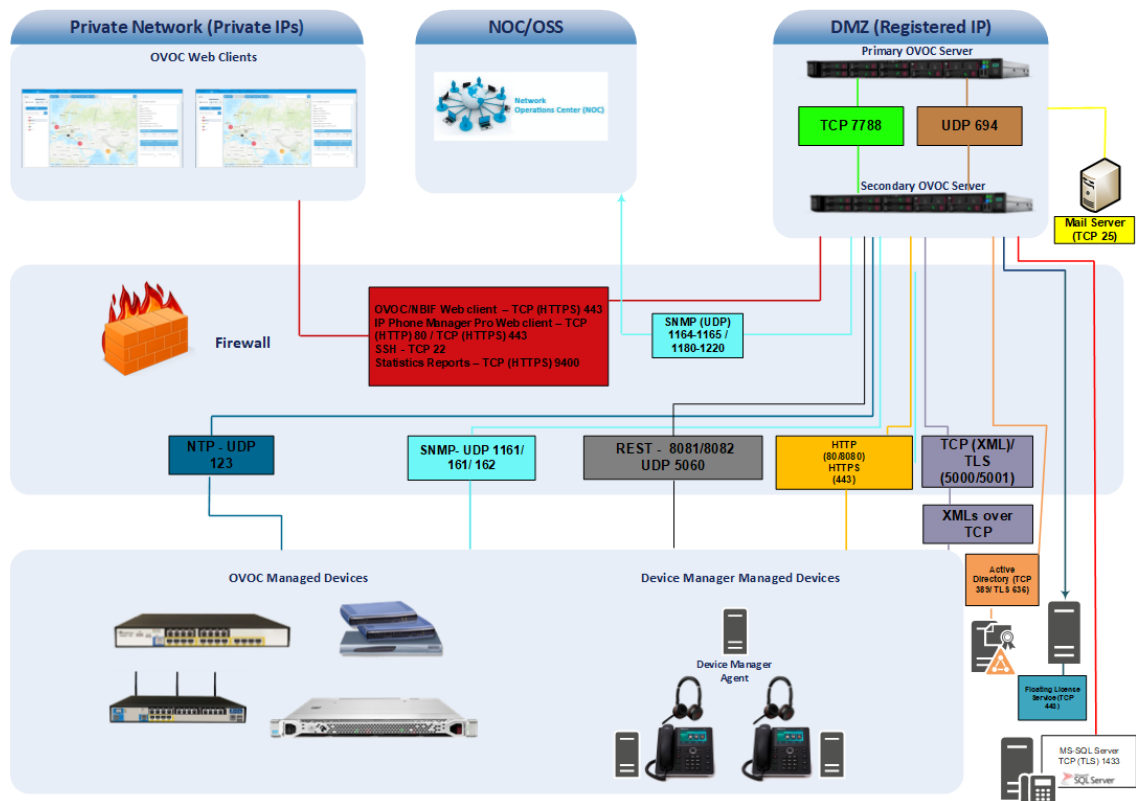
**Table 25-2: OAM Flows: NOC/OSS → OVOC**

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
NOC/OSS	OVOC	SFTP	1024 - 65535	20

		FTP	1024 - 65535	21
		SSH	1024 - 65535	22
		Telnet	1024 - 65535	23
		NTP	123	123
		HTTP/HTTPS	N/A	80/443
		SNMP (UDP) Set for the Active alarms Resync feature.	N/A	161

**Table 25-3: OAM Flows: OVOC → NOC/OSS**

Source IP Address Range	Destination IP Address Range	Protocol	Source Port Range	Destination Port Range
OVOC	NOC/OSS	NTP	123	123
		SNMP (UDP) Trap	1024 – 65535	162
		SNMP (UDP) port for the Active alarms Resync feature	1164 - 1165	-
		SNMP (UDP) port for alarm forwarding	1180-1220	-

**Figure 25-1: Firewall Configuration Schema**

The above figure displays images of devices. For the full list of supported products, see [Managed VoIP Equipment](#) on page 3.

# Part VII

## Appendix

This part describes additional OVOC server procedures.

## 26 Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Servers

This appendix describes the required equipment and the steps for configuring the HP ProLiant server to support RAID-0 Disk Array configuration for the OVOC server installation.



This procedure erases any residual data on the designated disk drives.

### Prerequisites

This procedure requires the following:

- ProLiant DL360p Gen8 server pre-installed in a compatible rack and connected to power.
- Two 1.2TB SAS disk drives
- A VGA display, USB keyboard, and USB mouse must be connected to the server back I/O panel.

### Hardware Preparation

Make sure that two 1.2TB SAS disk drives are installed on slot 1 and 2 of the server. If required, refer to the *HP Service Manual*.

**Figure 26-1: Hardware Preparation**



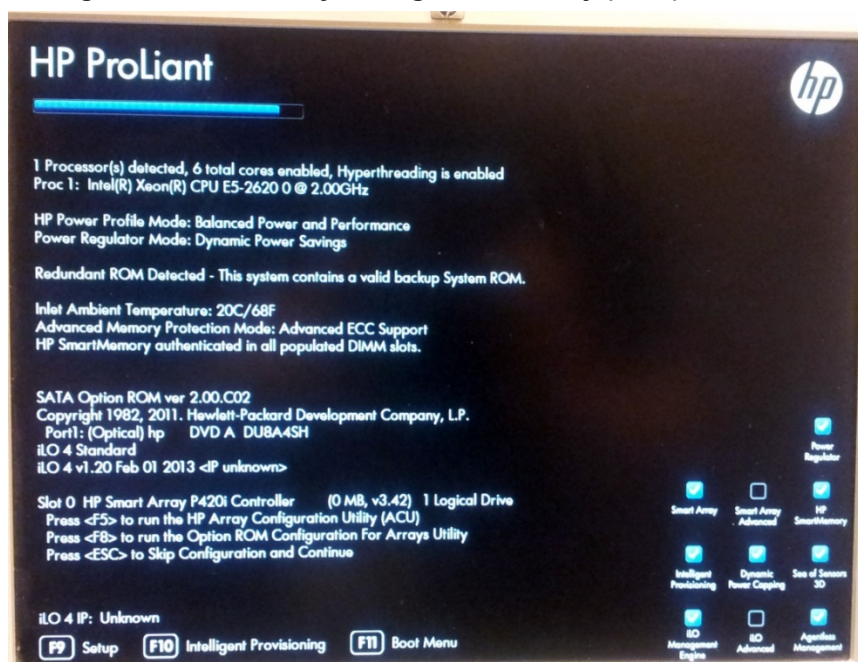
### Configuring RAID-0

This procedure describes how to configure RAID-0 using the HP Array Configuration Utility (ACU).

#### ➤ To configure RAID-0:

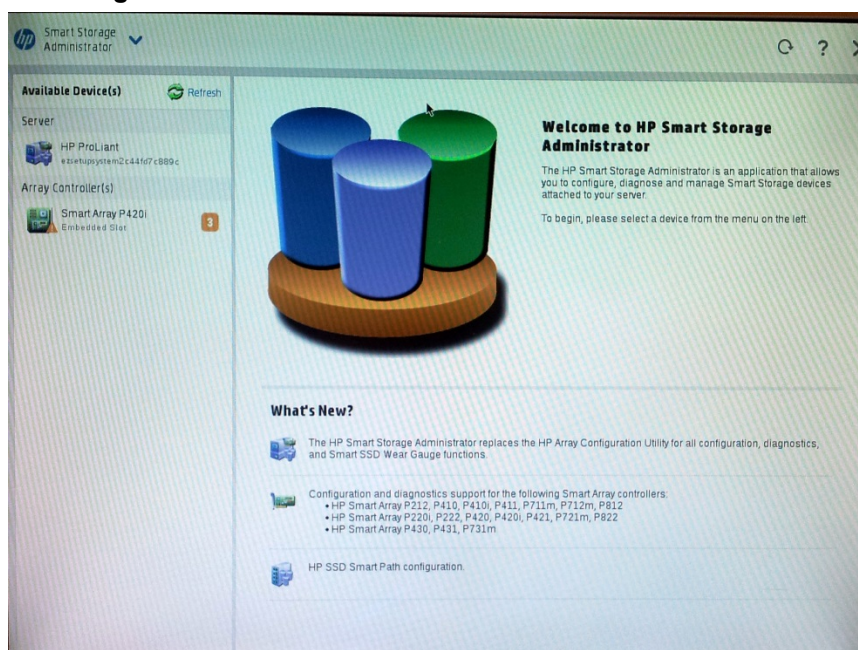
1. Power up the server. If the server is already powered up and running, use the 'reboot' command (from system console as user root) to reboot the server.
2. While the server is powering up, monitor the server and wait for the following screen:



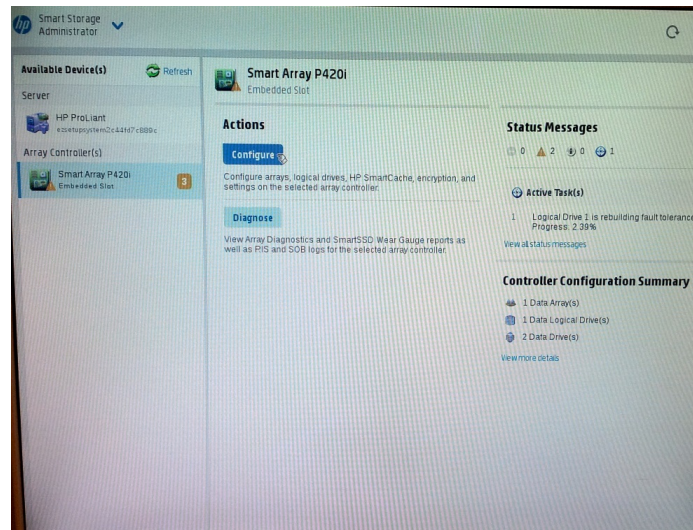
**Figure 26-2: HP Array Configuration Utility (ACU)**

3. Press <F5> to run the HP Array Configuration Utility (ACU).
4. Wait for the ACU to finish loading.

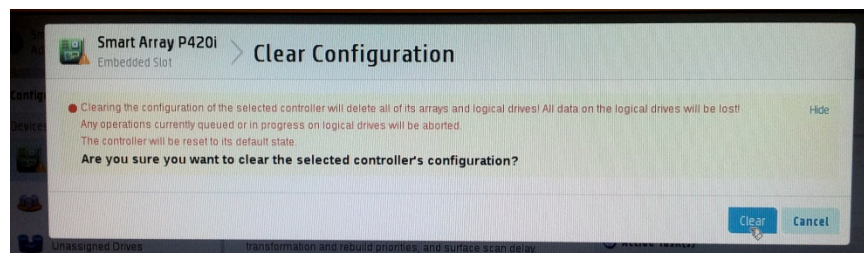
When the ACU is ready, the following screen is displayed:

**Figure 26-3: RAID-Latest Firmware Versions**

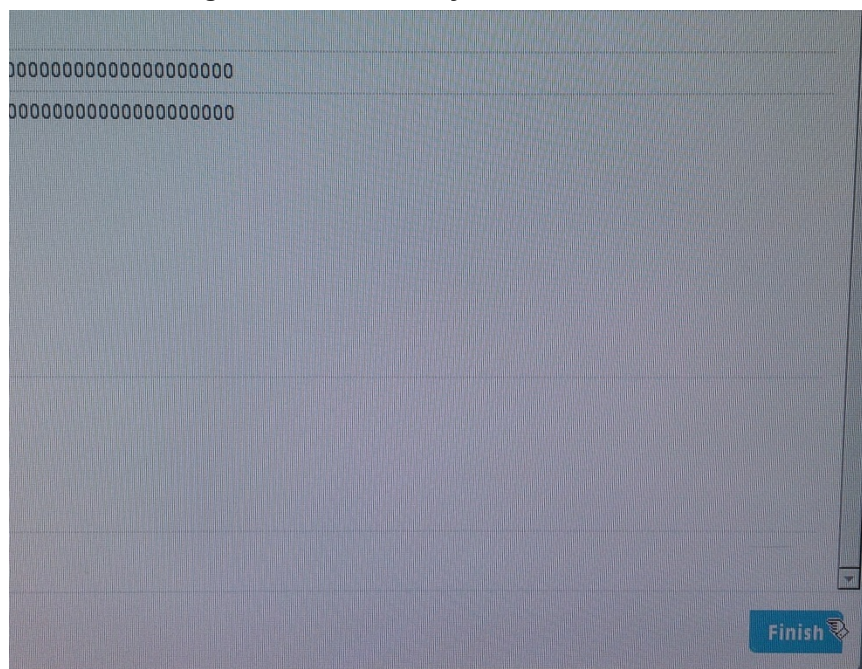
5. In the left-hand pane, select **Smart Array P420i**; an Actions menu is displayed:

**Figure 26-4: Actions Menu**

6. Click **Configure**, and then click **Clear Configuration** to clear any previous configuration; the following confirmation is displayed:

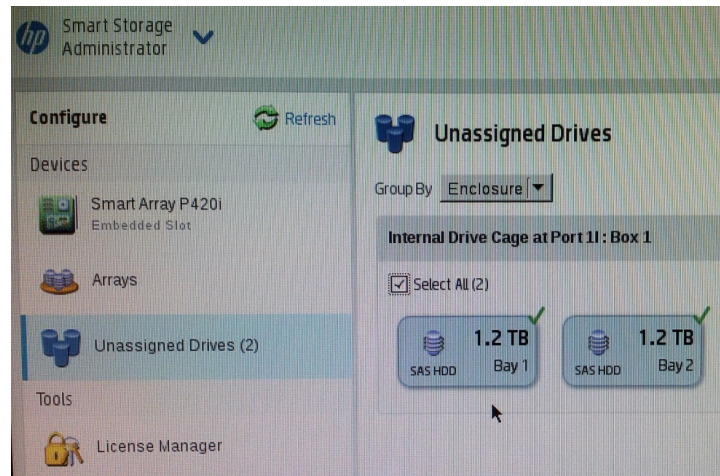
**Figure 26-5: Clear Configuration**

7. Click **Clear** to confirm; a summary display appears:

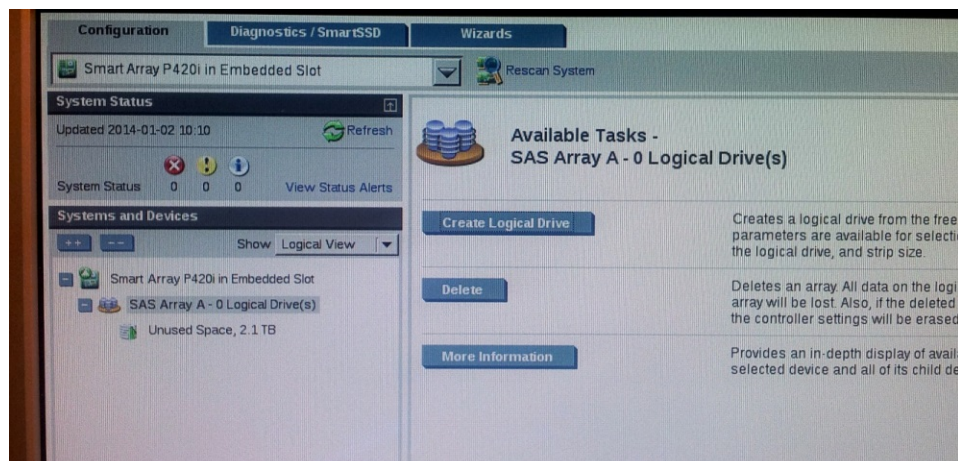
**Figure 26-6: Summary Screen**

8. Click **Finish** to return to the main menu. The following screen is displayed:



**Figure 26-7: Main Screen**

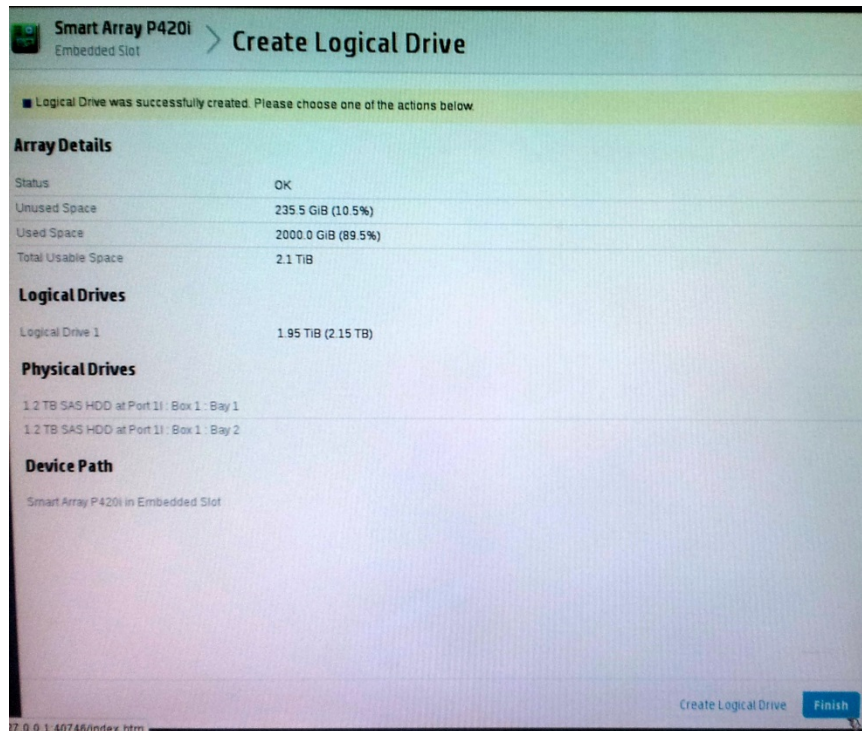
9. In the left-hand pane, select **Unassigned Drives (2)**; make sure that both the drives are selected, and then click **Create Array**.
10. Select **RAID 0** for RAID Level.
11. Select the 'Custom Size' check box, and then enter **2000 GiB**.
12. At the bottom of the screen, click **Create Logical Drive**; the following screen is displayed:

**Figure 26-8: Logical Drive**

After the array is created, a logical drive should be created.

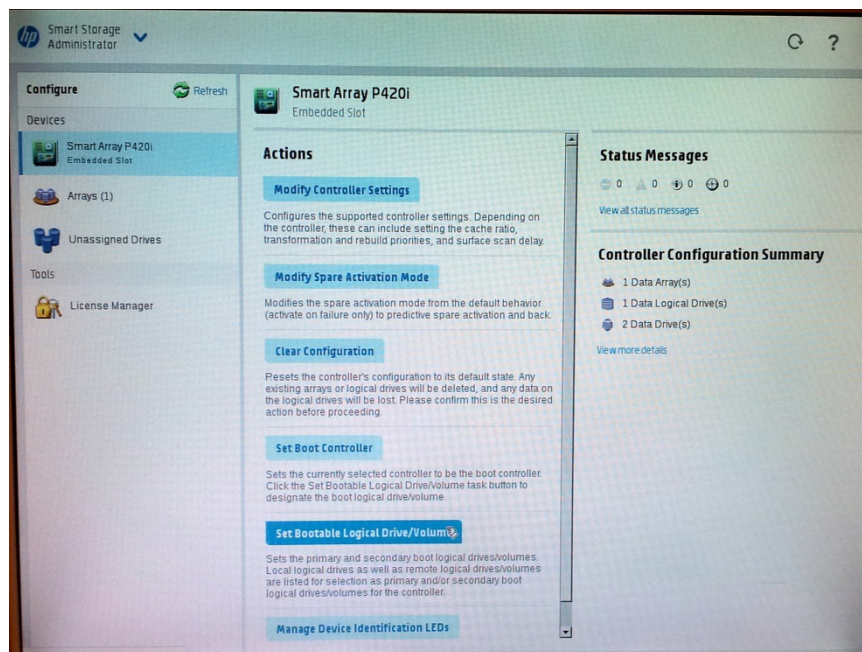
13. Click **Create Logical Drive**.  
A summary screen is displayed:

Figure 26-9: Summary Screen



14. Click **Finish**.

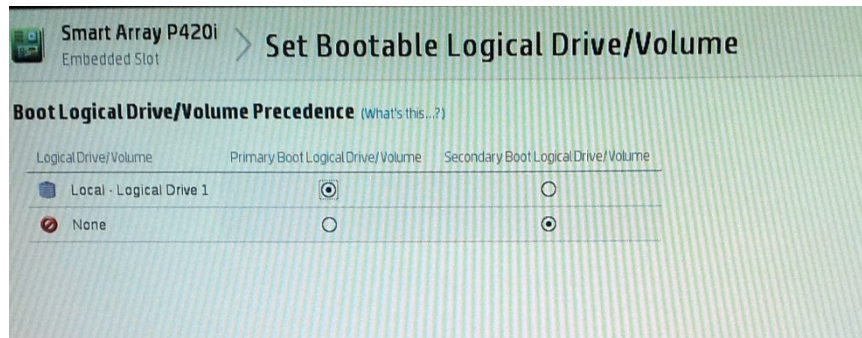
Figure 26-10: Set Bootable Logical Drive/Volume



The new logical volume needs to be set as a bootable volume.

15. In the left-hand pane, select **Smart Array P420i**, and then click **Set Bootable Logical Drive/Volume**; the following screen is displayed:



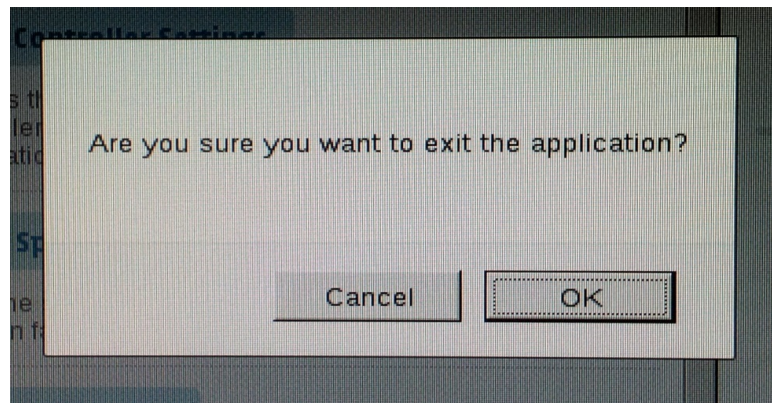
**Figure 26-11: Set Bootable Logical Drive/Volume**

16. Select the "Local - Logical Drive 1" as **Primary Boot Logical Drive/Volume**, and then click **Save**.

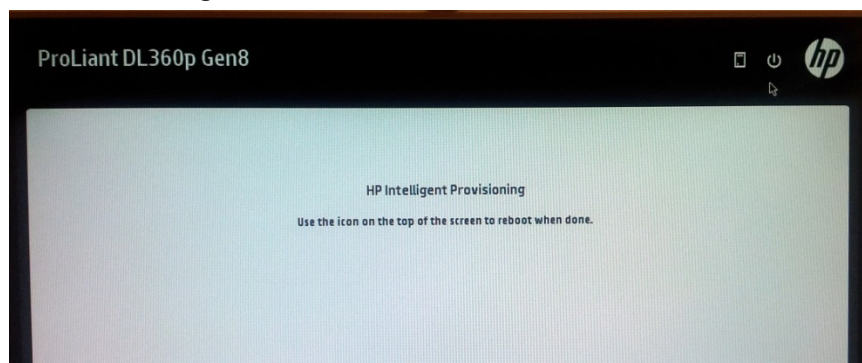
A summary window is displayed.

17. Click **Finish**.

18. Exit the ACU by clicking the **X** sign on the top right-hand side of the screen, and then confirm the following dialog:

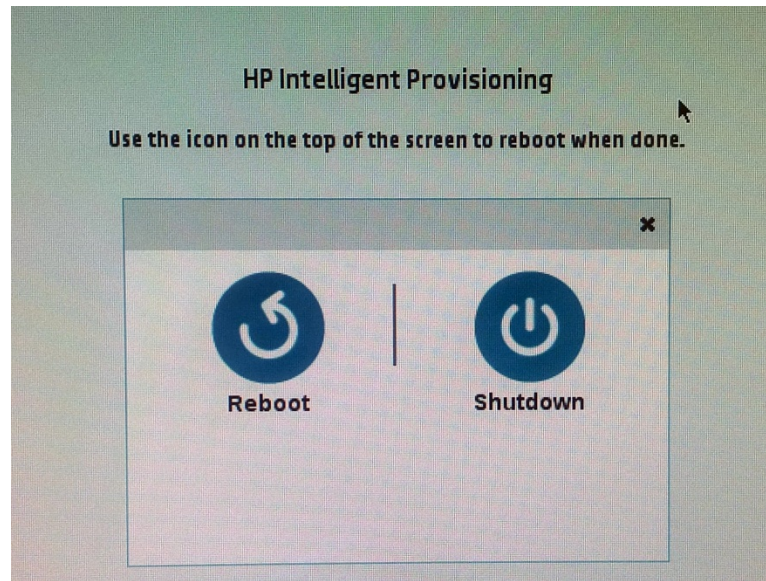
**Figure 26-12: Exit Application**

19. Click **Exit ACU** at the bottom left-hand corner of the screen; the following screen is displayed:

**Figure 26-13: Power Button**

20. Click the **Power** icon in the upper right-hand corner of the screen.

The following screen is displayed:

**Figure 26-14: Reboot Button**

21. Click **Reboot** to reboot the server.  
The Disk Array configuration is now complete.
22. Install the OVOC server installation (Installing the OVOC server on Dedicated Hardware).

## 27 Managing Clusters

This appendix describes how to manually migrate or move OVOC VMs to another cluster node.

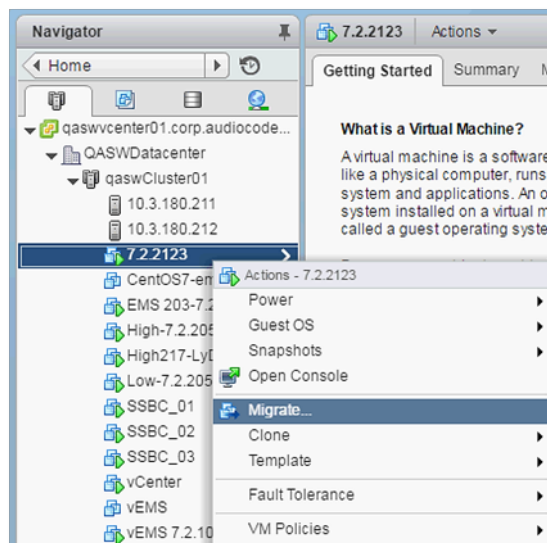
### Migrating OVOC Virtual Machines in a VMware Cluster

This section describes how to migrate your OVOC Virtual Machine from one ESXi host to another.

➤ **To migrate your OVOC VM:**

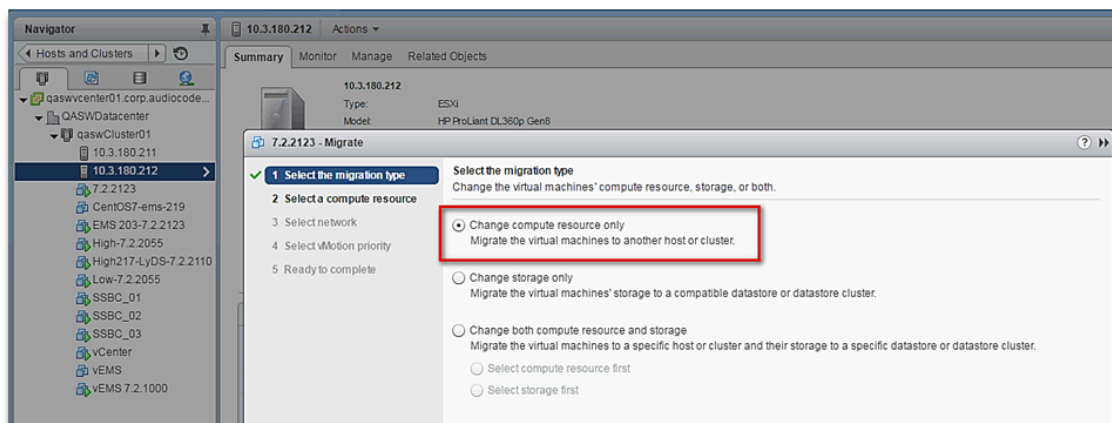
1. Select the OVOC VM that you wish to migrate and then choose the **Migrate** option:

**Figure 27-1: Migration**



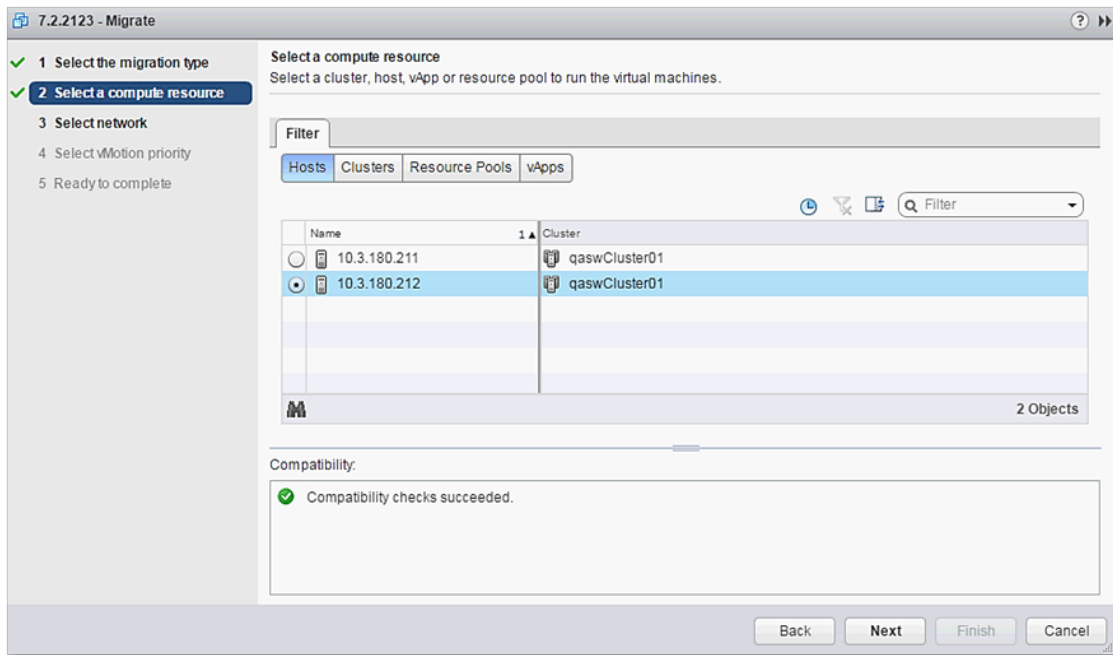
2. Change a cluster host for migration:

**Figure 27-2: Change Host**



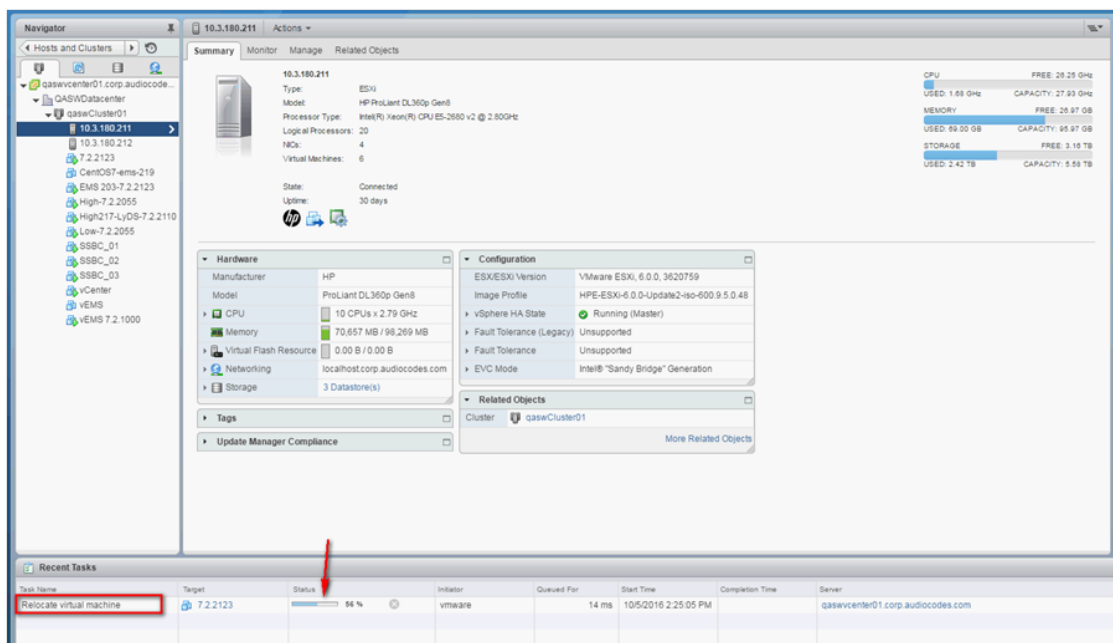
3. Choose the target host for migration:

Figure 27-3: Target Host for Migration



The migration process commences:

Figure 27-4: Migration Process Started



After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's host.

## Moving OVOC VMs in a Hyper-V Cluster

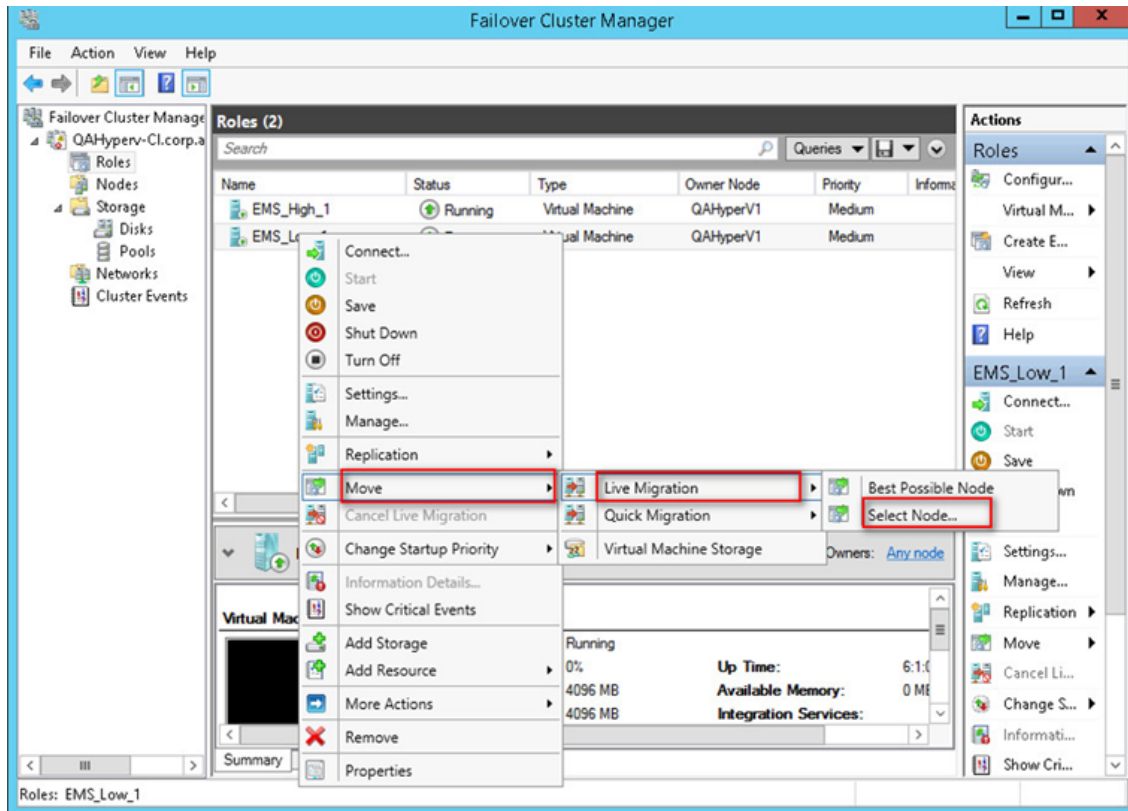
### Moving OVOC VMs in a Hyper-V Cluster

This section describes how to move a Virtual Machine to another host node in a Hyper-V cluster.

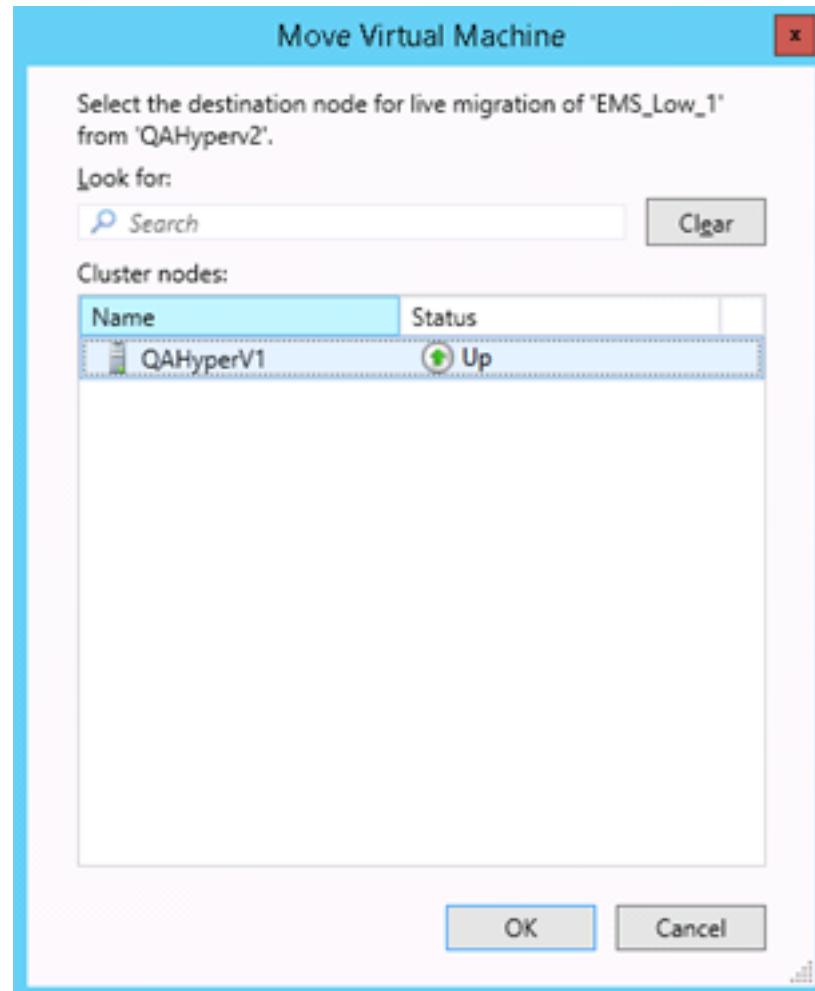
#### ➤ To move a Virtual Machine to another node of the cluster:

1. Select the Virtual Machine, right-click and from the menu, choose **Move > Live Migration > Select Node**.



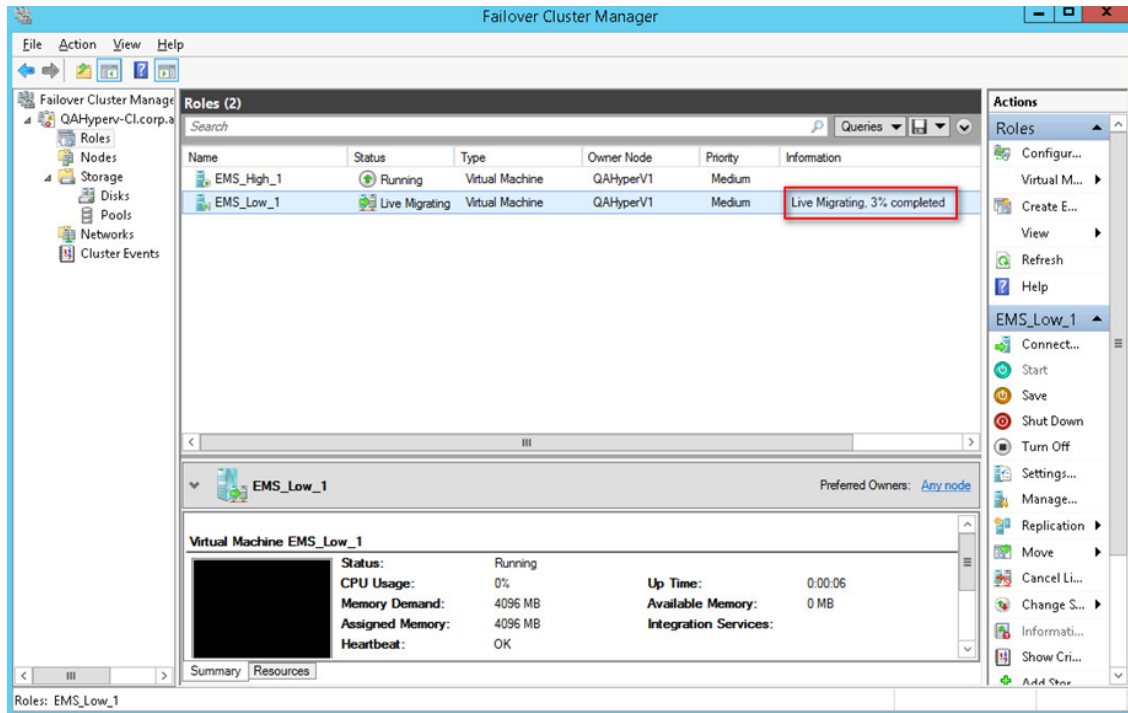
**Figure 27-5: Hyper-V Live Migration**

The following screen is displayed:

**Figure 27-6: Move Virtual Machine**

2. Select the relevant node and click **OK**.

The migration process starts.

**Figure 27-7: Hyper-V Migration Process Started**

After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's node.

## 28 Supplementary Security Procedures

The procedures in this appendix describe supplementary procedures for completing the setup of X.509 Custom certificates.



For more information on the implementation of custom certificates, refer to the OVOC Security Guidelines document.

This appendix describes the following procedures:

- Downloading certificates to the AudioCodes device ([Installing Custom Certificates on OVOC Managed Devices](#) below)
- Cleaning up Temporary files on the OVOC server ( [Cleaning up Temporary Files on OVOC Server](#) on page 199)

### Installing Custom Certificates on OVOC Managed Devices

This section describes how to install Custom certificates on OVOC managed devices. These certificates will be used to secure the connection between the device and OVOC server. This procedure is performed using the device's embedded Web server. This section describes how to install certificates for the following devices:

- Enterprise gateways and SBC devices ([Enterprise Gateways and SBC Devices](#) below).
- MP-1xx devices ([MP-1xx Devices](#) on page 194).



- When securing the device connection over HTTPS, the certificate loaded to the device must be signed by the same CA as the certificate loaded to the OVOC server.
- The Single-Sign On mechanism is used to enable automatic login to the devices embedded Web server tool from the device's status screen in the OVOC. This connection is secured over port 443. OVOC logs into the OVOC managed device using the credentials that you configure in the AudioCodes device details or Tenant Details in the OVOC Web. You can also login to the AudioCodes device using the RADIUS or LDAP credentials (for more information, refer to the OVOC User's Manual).

### Enterprise Gateways and SBC Devices

This section describes how to install custom certificates on Enterprise gateways and SBC devices. The device uses TLS Context #0 to communicate with the OVOC server. Therefore, the configuration described below should be performed for **TLS Context #0**.

#### Step 1: Generate a Certificate Signing Request (CSR)

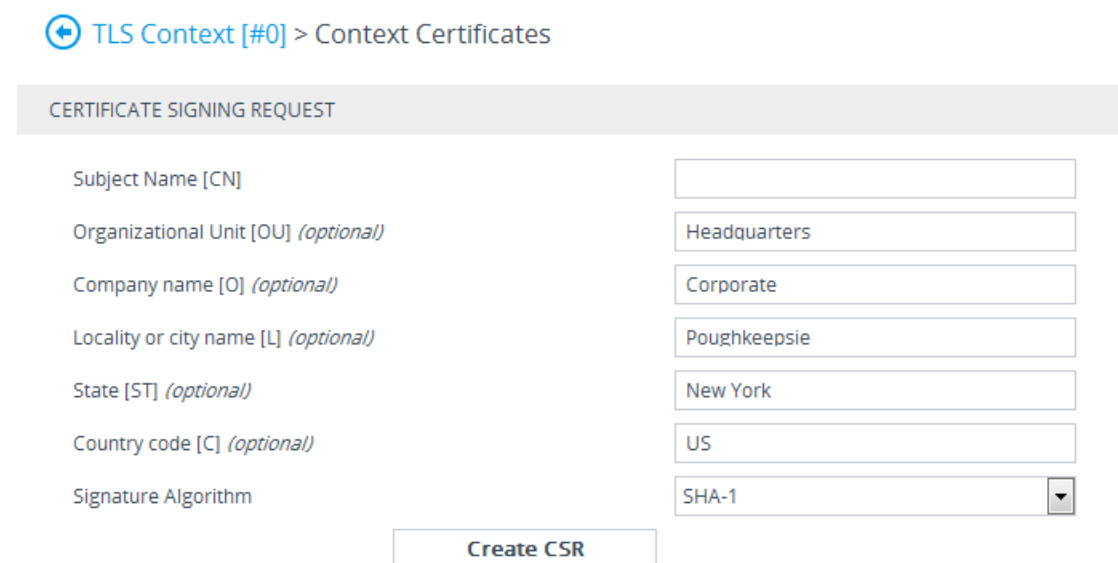
This step describes how to generate a Certificate Signing Request (CSR).

##### ➤ To generate certificate signing request:

1. Login to the device's Web server.
2. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

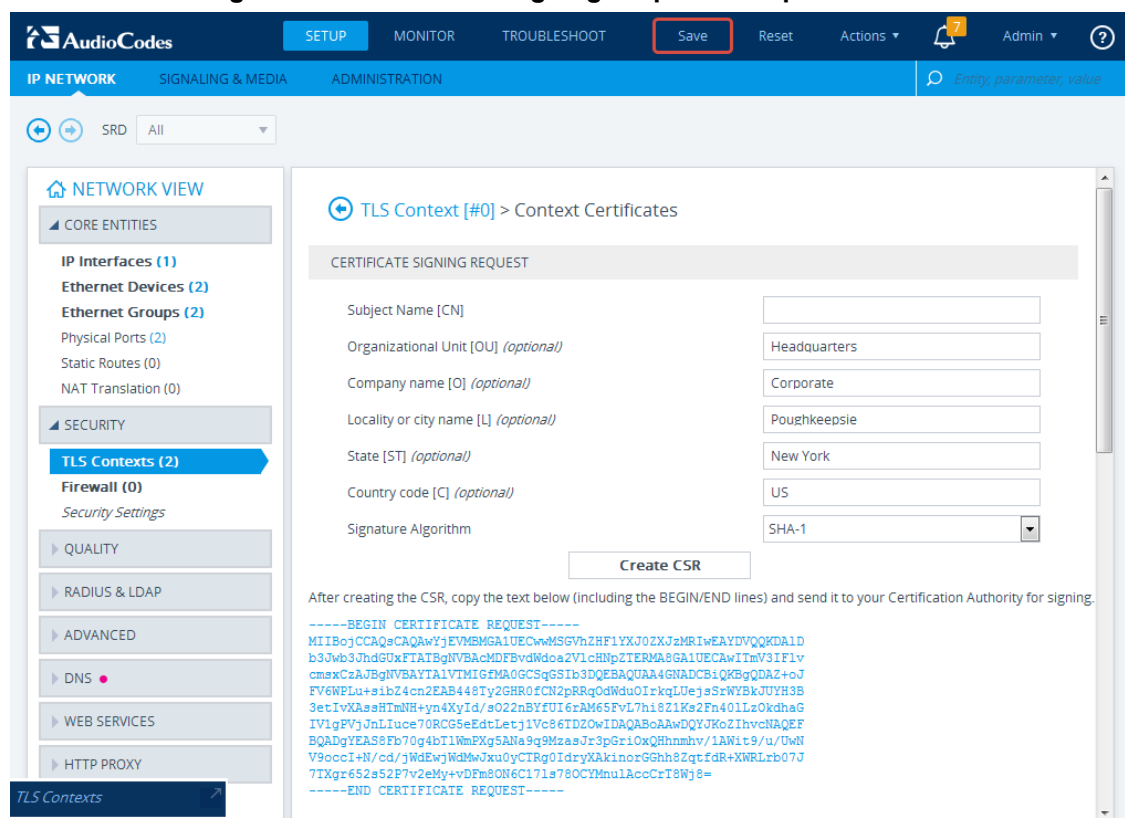
- In the table, select the **TLS Context #0**, and then click the **TLS Context Certificate** button, located below the table; the Context Certificates page appears.

### Figure 28-1: Context Certificates



4. Under the **Certificate Signing Request** group, do the following:
  - a. In the 'Subject Name [CN]' field, enter the device's DNS name, if such exists, or device's IP address
  - b. Fill in the rest of the request fields according to your security provider's instructions.
  - c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

### Figure 28-2: Certificate Signing Request Group



- Copy the text and send it to the certificate authority (CA) to sign this request.

## Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to "device.crt"
- Root certificate – rename this file to "root.crt"
- Intermediate CA certificates (if such files exist) – rename these files to "ca1.crt", "ca2.crt" etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----
```

```
MIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA1U  
EAxMM
```

```
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE0M  
FowKJET
```

```
...
```

```
TI6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol0  
L6V8IzUYOfHrEiq/6g==
```

```
-----END CERTIFICATE-----
```



- The above files are required in the following steps. Make sure that you obtain these files before proceeding and save them to the desired location.
- Use the exact filenames as mentioned above

## Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

### ➤ To update device with new certificate:

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the table, select the **TLS Context #0**, and then click the **TLS Context Certificate** button, located below the table; the Context Certificates page appears.
3. Under the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.

**Figure 28-3: Upload Certificate Files from your Computer Group**

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*

Send **Private Key** file from your computer to the device.  
The file must be in either PEM or PFX (PKCS#12) format.

Browse...

No file selected.

Send File

audc

**Note:** Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.  
The file must be in textual PEM format.

Browse...

No file selected.

Send File

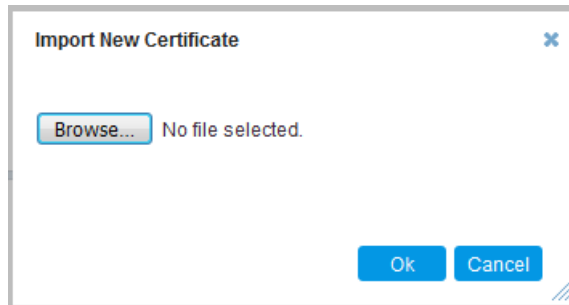
## Step 4: Update Device's Trusted Certificate Store

This step describes how to update the device's Trusted Certificate Store.

### ➤ To update device's trusted certificate store:

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the table, select the **TLS Context #0**, and then click the **TLS Context Trusted Root Certificates** button, located below the table; the Trusted Certificates page appears.
3. Click the **Import** button, and then browse to the root.crt file. Click **OK** to import the root certificate.

**Figure 28-4: Importing Certificate into Trusted Certificates Store**



4. If you received intermediary CA certificates – ca1.crt, ca2.crt, etc. – import them in a similar way.

## Step 5: Configure HTTPS Parameters on the Device

This section describes how to configure HTTPS related parameters on the device.



- You can optionally pre-stage the device with a pre-loaded ini file including this configuration (for more information, contact your AudioCodes representative).
- If you have enabled the Interoperability Automatic Provisioning feature, ensure that your template file is also configured as described in this procedure to maintain an active HTTPS connection after the template file has been loaded to the device.
- When you setup an HTTPS connection on the device, you must also enable HTTPS ("Enable HTTPS Connection") when adding the device to the OVOC (refer to the *OVOC User's manual*).

### ➤ To configure HTTPS parameters on the device:

1. Create a new text file using a text-based editor (e.g., Notepad).
2. Include the following ini file parameters for server-side authentication:
  - For Media Gateway and SBC devices:  
AUPDVerifyCertificates=1
  - For MP-1xx devices, the ini file should include the following two lines::  
AUPDVerifyCertificates=1  
ServerRespondTimeout=10000
  - When working with SEM TLS ( [OVOC Voice Quality Package - OVOC Managed Devices Communication](#) on page 153), add the following parameter.  
QOEENABLETLS=1
3. Save and close the file.

4. Load the generated file as "Incremental INI file" (Maintenance menu > Software Update > Load Auxiliary Files > INI file (incremental)).
5. Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
6. In the table, select the TLS Context #0, and then click Edit button. The following screen is displayed:

**Figure 28-5: TLS Contexts: Edit Record**

GENERAL		OCSP	
Index	0	OCSP Server	Disable
Name	default	Primary OCSP Server	
TLS Version	Any - Including SSLv3	Secondary OCSP Server	
DTLS Version	Any	OCSP Port	2560
Cipher Server	RC4:AES128	OCSP Default Response	Reject
Cipher Client	RC4:DEFAULT		
Strict Certificate Extension Validation	Disable		
DH key Size	1024		

Cancel **APPLY**

7. Set the required 'TLS Version' (default TLS Version 1.0).
8. Set 'HTTPS Cipher Server' to ALL.
9. Set 'HTTPS Cipher Client' to ALL.

### Step 6: Reset Device to Apply the New Configuration

This step describes how to reset the device to apply the new configuration.

➤ **To reset the device:**

1. In the top-level menu, click Device Actions > Reset. The following screen is displayed.



Figure 28-6: Device Reset

AudioCodes SETUP MONITOR TROUBLESHOOT

IP NETWORK SIGNALING & MEDIA **ADMINISTRATION** Save Reset Actions Admin

Entity, parameter, value

SRD All

**TIME & DATE**

- WEB & CLI
- SNMP
- MAINTENANCE**
  - Configuration File
  - Auxiliary Files
  - Maintenance Actions**
  - License Key
  - Software Upgrade

**Maintenance Actions**

RESET DEVICE		LOCK / UNLOCK	
Reset Device	<input type="button" value="Reset"/>	Lock	<input type="button" value="LOC"/>
Save To Flash	<input type="text" value="Yes"/>	Graceful Option	<input type="text" value="No"/>
Graceful Option	<input type="text" value="No"/>	Gateway Operational State	UNLOCKED

**For Reset Device :** If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.

**For Save Configuration:** Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods

- From the Burn to FLASH drop-down list, select Yes, and then click Reset button.  
The device will save the new configuration to non-volatile memory and reset itself.

## MP-1xx Devices

This section describes how to install Custom certificates on the MP 1xx devices.

### Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

#### ➤ To generate a CSR:

- Your network administrator should allocate a unique DNS name for the device (e.g., dns\_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
- If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPSOnly) to **HTTP and HTTPS** (refer to the *MP-11x and MP-124 User's Manual*). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
- Login to the MP-1xx Web server.
- Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
- Under the **Certificate Signing Request** group, do the following:
  - In the 'Subject Name [CN]' field, enter the DNS name.
  - Fill in the rest of the request fields according to your security provider's instructions.

- c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

**Figure 28-7: Certificate Signing Request Group**

▼ Certificate Signing Request

Subject Name [CN]	audio.com
Organizational Unit [OU] (optional)	Headquarters
Company name [O] (optional)	Corporate
Locality or city name [L] (optional)	Poughkeepsie
State [ST] (optional)	New York
Country code [C] (optional)	US

Create CSR

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwZjESMBAGA1UEAxMJYXVkaW8uY29tMRUwEwYDVQQLZwZk
cXVhcnRlcnMxMjEjAQBGAoTCUNvbnBvcnF0ZTEVMBMGA1UEBxMMUG91Z2hrZWVw
c211MREwDwYDVQQLZwZkZG9yYzELMAkGA1UEBhMCVVMwZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPhpf2t4OLy3FRk5Bw7F1ZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1CboIPgoZNS0g6+5JAmJAA
1LNUnoqjEsK7CF32uvolH//gFkhy5zleNvObI+25Pn38aJzEXc8DkGwZ19rROqRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbc1zkHdLFr+5BRuScKyGUXBM6
q7FGjFXAf2k1MmgnBMc/MYfSGTbawrQF7p6dNJ60DivmuCPf6Gzz5m2uqC6LqoIi
nLnQpVCmbdva/B1QyEpPbQhZqpULJ8CSeSrrY3ru23AZeDUBvYyho90IkRbAp//+3
ZvnZZe5M5CBSLg==
-----END CERTIFICATE REQUEST-----

```

6. Copy the text and send it to the certificate authority (CA) to sign this request.

## Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to “device.crt”
- Root certificate – rename this file to “root.crt”
- Intermediate CA certificates (if such files exist) – rename these files to “ca1.crt”, “ca2.crt” etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

-----BEGIN CERTIFICATE-----

```

MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEw
JGUjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBT
ZXJ2ZXVyMB4XDTE4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAk
GA1UEBhMCRCllxEzARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG
9zdGUgU2VydMv1cjCCASEwDQYJKoZIhvcNAQEBBQADggEAOADCCAQkCggEAPqd4
MziR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfX7jJpreWULf7v7Cv
pr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4
k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwv
REXfFcUW+w==

```

-----END CERTIFICATE-----



- The above files are required in the following steps. Make sure that you obtain these files before proceeding.
- Use the exact filenames as mentioned above.

### Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

#### ➤ To update the device with the new certificate:

1. In the Certificates page, scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.
2. After the certificate successfully loads to the device, save the configuration with a device reset ([Step 6: Reset Device to Apply the New Configuration](#) on page 198 below).

### Step 4: Update Device's Trusted Certificate Store

For the device to trust a whole chain of certificates you need to combine the contents of the root.crt and ca.crt certificates into a single text file (using a text editor).

#### ➤ To update the device with the new certificate:

1. Open the root.crt file (using a text-based editor, e.g., Notepad).
2. Open the ca.crt file (using a text-based editor, e.g., Notepad).
3. Copy the content of the ca.crt file and paste it into the root.crt file above the existing content.

Below is an example of two certificate files combined (the file "ca2.crt" and the "root.crt") where the ca2.crt file contents are pasted above the root.crt file contents:

-----BEGIN CERTIFICATE-----

MIIDNjCCAh6gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx

ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFOXTIwMD  
EwMTAwMDAw

MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVnfQ0EyMIIBIjANB  
gkqhkiG

9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5UgxflPjJeNggwnlQiUY  
hOK  
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsnCSxpVqcYfMoBbCL/

0fmXKHWIPIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqE4  
yk  
ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu  
5B6wYNPOTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZPBKI  
hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAM

BgNVHRMEBTADAQH/MB0GA1UdDgQWBBrY2JQ1yZrvN4GifsXUB7AvctWvrTB  
JBgNV

HSMEQjBAGBTf6GbMQbO5b0CkLV8kW+Rg0AAhqElpCMwITEMMAoGA1UEChMDQUNM

MREwDwYDVQQDFAhFTVNfUk9PVII BATANBgkqhkiG9w0BAQUFAAOCAQEA

sYyfcg  
TdkF/uDxIOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAWroGwx7tsn1/o+  
CNV5Yalstlz7BDIEIjTzCDRpO9sUsiHqxGuOnNhjLDUoLre1GDC0OyiKb4BOhICq  
hiemkXRe+eN7xcg0lfUo78VLTpuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJGO

RUoslqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+  
V

XoAhN6pH17PMXLPclm9L/MlkVkmf0tp1bPmefrEBIO+np/O8F+P551uH0iOYA6Cc  
Cj6oHGLq8RIndA==

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIDNzCCAh+gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx

ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTEwMDAwMTAwMDAw

MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVDCCASIWdQYJKoZI

hvcNAQEBBQADggEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FSFhn  
UQrS

667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEols+7/q  
ebESJyW8pTLTszGQns2E214+U18sKHltpUZvs1dVUIX6xQiSYFDG1CDIPR5/70pq  
zwtdblpsSkgYijos0yRV3roVqNi4e+hmLVZA9OIpl6LR72Ta9HMFJ4gyxJPUQA

jV3Led2Y4JObvBTNIka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPUf1wRjDWgl4  
G

BRw2MACYsu/M9z/H821UOICtsZ4oKUJMqbwjQ9IXI/HQkKRSTf8CAwEAAaN6MH  
gw

DAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYNAAI  
YwSQYD

VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCEXDDAKBgNVBAoTA0FD

TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADggEBAHqkg4F6

wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFcz1q4QVpQNYAwdBdEAKENznZttoP3aPZ  
E

3EOx1C8Mw2wU4pOxD7B6pH0XO+oJ4LrxLB3SAJd5hW495X1RDF99BBA9eGUZ2  
nXJ

9pin4PWbnfc8eppq8Tpl8jJMW0Zl3prfPt012q93iEalkDEZX+wxkHGZEqs4ayBn  
8bU3NHt5qh0Egpai8hB/nth1xnA1m841wxCbJW86AMRs2NznROyG695InAYAnllo

```
HU9zBRdRRASV5vmBN/q5JnDhshZhL1Bm+M6QxOyGoNjL1DqE+aWZkmsw2k9S
TopN
itSUgGYwEagnsMU=
-----END CERTIFICATE-----
```



The maximum supported size of the combined file of trusted chain of certificates is 100,000 bytes (including the certificate's headers).

4. Save the combined content to a file named "chain.pem" and close the file.
5. Open the Certificates page and upload chain.pem file using the 'Trusted Root Certificate Store' field.

### Step 5: Configure HTTPS Parameters on Device

- Configure HTTPS Parameters on the device ([Step 5: Configure HTTPS Parameters on the Device](#) on page 192 above).

### Step 6: Reset Device to Apply the New Configuration

This section describes how to apply the new configuration.

#### ➤ To save the changes and reset the device:

1. Do one of the following:
  - On the toolbar, click the **Device Actions** button, and then from the drop-down menu, choose **Reset**.
  - On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu and choose **Maintenance Actions**.

**Figure 28-8: Maintenance Actions Page**

▼ Reset Configuration	
Reset Board	<b>Reset</b>
Burn To FLASH	Yes ▼
Graceful Option	No ▼
▼ LOCK / UNLOCK	
Lock	<b>LOCK</b>
Graceful Option	No ▼
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<b>BURN</b>

2. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
3. Click **OK** to confirm device reset; when the device begins to reset, a notification message is displayed.

## Cleaning up Temporary Files on OVOC Server

It is highly recommended to cleanup temporary files on the OVOC server after certificates have been successfully installed. This is necessary to prevent access to security-sensitive material (certificates and private keys) by malicious users.

➤ **To delete temporary certificate files:**

1. Login to the OVOC server as user *root*.
2. Remove the temporary directories:

```
rm -rf /home/acems/server_certs  
rm -rf /home/acems/client_certs
```

## 29 Transferring Files

This appendix describes how to transfer files to and from the OVOC server using any SFTP/SCP file transfer application.



FTP by default is disabled on the OVOC server.

➤ **To transfer files to and from the OVOC server:**

1. Open your SFTP/SCP application, such as WinSCP or FileZilla.
2. Login with the acems/acems credential (all files transferred to the OVOC server host machine are then by default saved to /home/acems directory).
3. Copy the relevant file(s) from your PC to the host machine (or vice-versa). For example, using the FileZilla program, you drag the relevant file from the left pane i.e. in your PC directory to the right pane i.e. the /home/acems directory on the OVOC server host machine.

## 30 Verifying and Converting Certificates

This appendix describes how to verify that certificates are in PEM format and describes how to convert them from DER to PEM if necessary.

➤ **To verify and convert certificates:**

1. Login to the OVOC server as user *root*.
2. Transfer the generated certificate to the OVOC server.
3. Execute the following command on the same directory that you transfer the certificate to verify that the certificate file is in PEM format:

```
Openssl x509 -in certfilename.crt -text -noout
```

4. Do one of the following:
  - a. If the certificate is displayed in text format, then this implies that the file is in PEM format, and therefore you can skip the steps below.
  - b. If you receive an error similar to the one displayed below, this implies that you are trying to view a DER encoded certificate and therefore need to convert it to the PEM format.

```
unable to load certificate
12626:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_
lib.c:647:Expecting: TRUSTED CERTIFICATE
```

5. Convert the DER certificate to PEM format:

```
openssl x509 -inform der -in certfilename.crt -out certfilename.crt
```



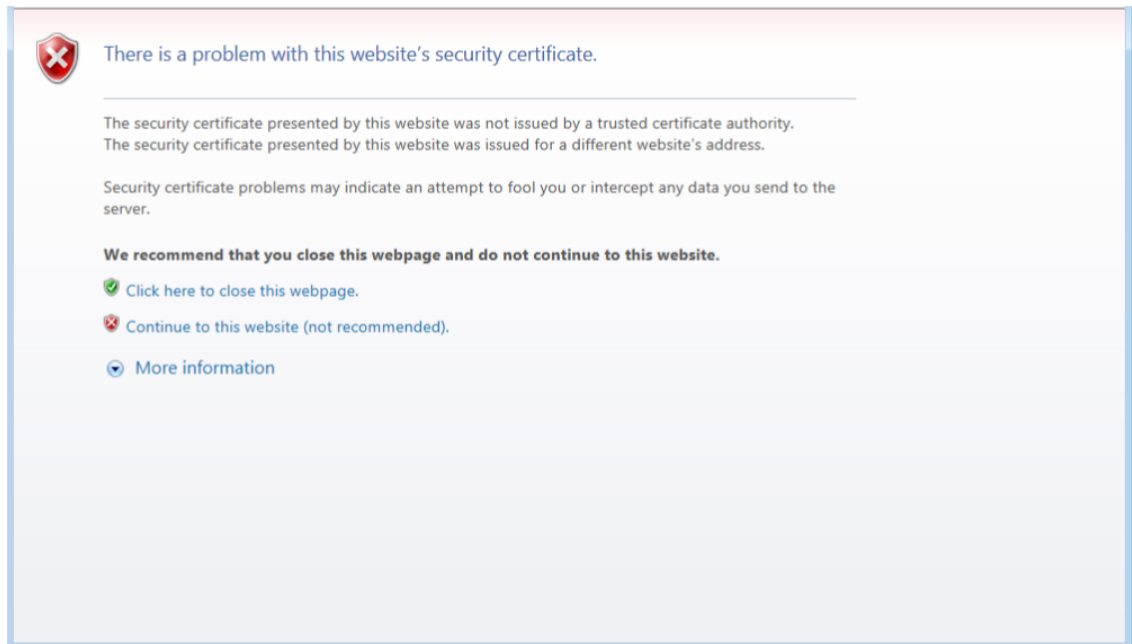
## 31 Self-Signed Certificates

When using self-signed certificates, use the following instructions for recognizing the secure connection with the OVOC server from your OVOC client browsers.

### Internet Explorer

When the following screen is displayed, select the “Continue to website (not recommended)” option.

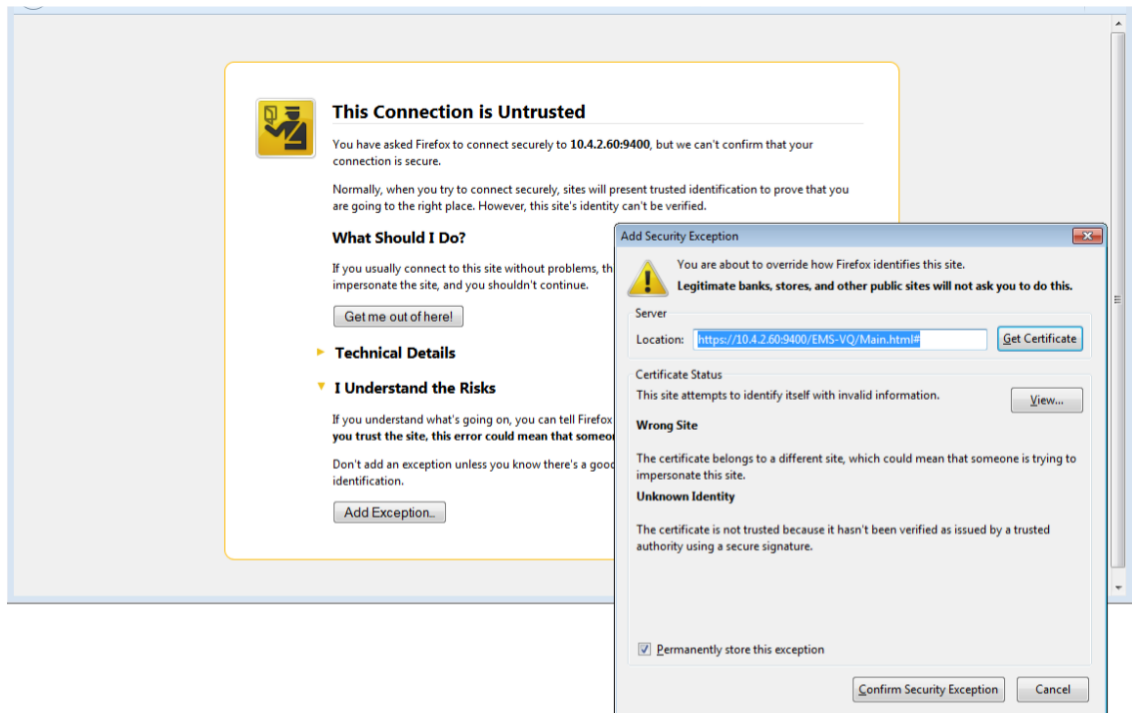
**Figure 31-1: Continue to Website**



### Using Mozilla Firefox

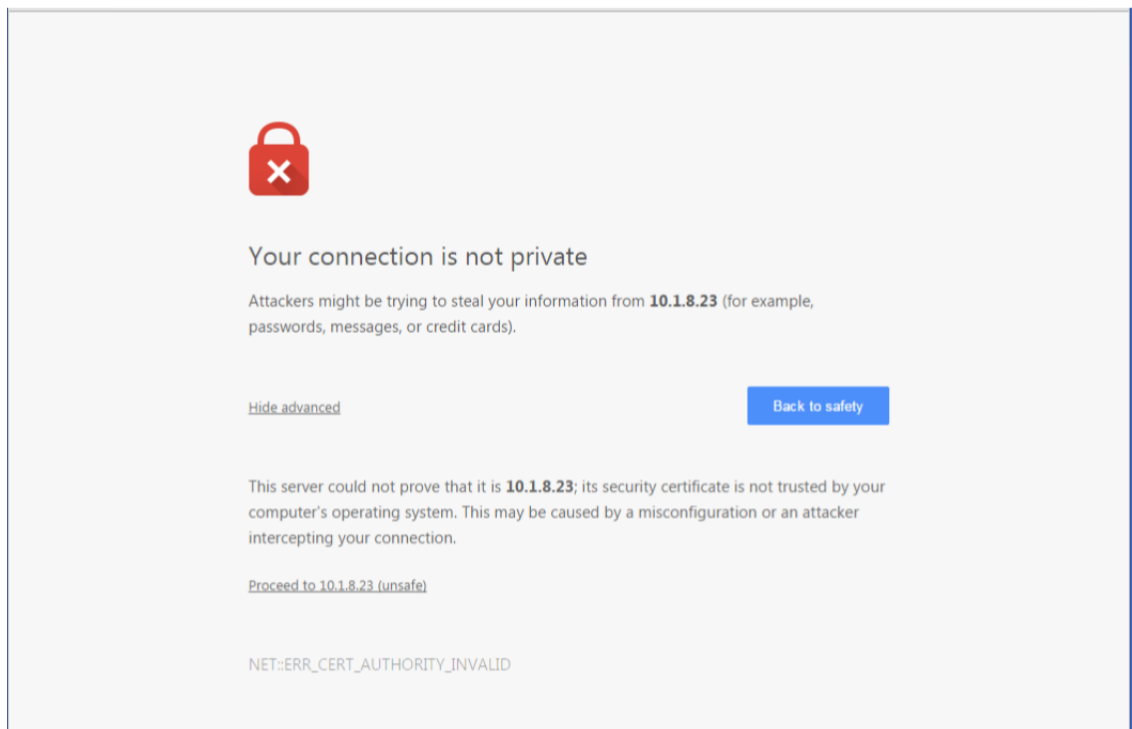
Do the following:

1. When the following screen is displayed, click the “I Understand the Risks” option.
2. Click the **Add Exception** button, and then click the **Confirm Security Exception** button.

**Figure 31-2: Mozilla Firefox Settings**

## Chrome

When the following screen is displayed, click **Advanced** and then click the "Proceed to <Server IP> (unsafe)" link.

**Figure 31-3: Chrome Browser Settings**

## 32 Datacenter Disaster Recovery

### Introduction

This appendix describes the OVOC Disaster Recovery procedure for deployments where OVOC is deployed in two separately geographically located datacenters with two different network spaces, in which minimal impact on the SBC/Gateway and OVOC downtime is desired.



Examples shown in this Appendix are for the VMware platform; however, these procedures are also relevant for Hyper-V platform.

### Solution Description

The Disaster Recovery solution is composed of two virtual machines answering today's OVOC system requirements. Virtual Low and Virtual High setups are supported.

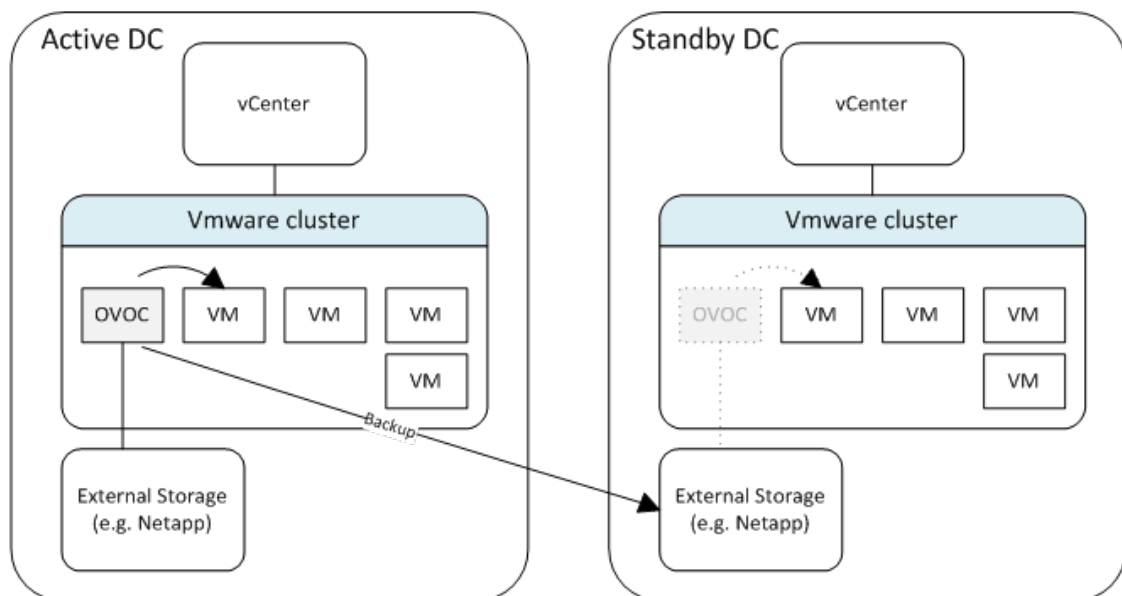
It is recommended that each OVOC machine will have a VMware High Availability (HA) setup to support local Data Center (DC) HA.

Both machines should have identical hardware configuration and installed with the exactly same OVOC software version. One of the machines will work as 'Active' and will be constantly up and running. The second machine will be defined as 'Redundant'. It should not be turned off and the application should be stopped and always remain off.

The primary machine backup files should be saved and periodically transferred to the external storage of the standby location.

If the primary machine fails, the user should run the Disaster Recovery procedure as shown below.

**Figure 32-1: Disaster Recovery Between Two Datacenters with VMware HA**



### Initial Requirements

The following initial requirements need to be adhered to before implementing the Disaster Recovery procedure:

- Both machines should have identical hardware (CPU, Memory, Disk, IO).

- An identical Linux OS (the same DVD), database, and the OVOC software version should be used.
- Identical database passwords need to be configured on both servers.
- Identical OVOC Server Manager settings must be configured on both servers (e.g., HTTP/HTTPS communication, etc.).
- If non-default certificates are used, they must be pre-installed on both servers.
- Both machines should have a valid license per each Machine ID with identical capabilities.
- When upgrading the OVOC server software, both machines should be upgraded. Make sure that redundant machine is not rebooted after the upgrade process and the OVOC application remains closed.



When upgrading OVOC, the backup that was created before the upgrade cannot be used anymore. You should only use the backups created after the upgrade process. For more information on backing up the OVOC server, see [OVOC Server Backup](#) on page 98.

- Make sure that active server backups are not stored on the server machine.

## New Customer Configuration

The procedure below describes the steps for a New Customer configuration.

### ➤ To perform a New Customer configuration:

1. Install and properly configure both servers.
2. Make sure the primary OVOC server is up and running.
3. For each device added and managed by the OVOC server, the following features should be provisioned with both primary and secondary servers' IP addresses:
  - Trap Destination Server
  - Session Experience Manager
  - NTP Server Address

## Data Synchronization Process

To save recovery time, it is advised that at the end of the daily / weekly backup, transfer the latest backup files from the primary to the secondary server machine. The data transfer may be done automatically using a script which can be defined by the customer. It is out of the OVOC scope to copy the backup files from the primary to the secondary server.

## Recovery Process

The procedure below describes the recovery process.

### ➤ To run the recovery process:

1. If the primary machine fails, use the Server Manager to make sure the OVOC application has been closed, before starting the secondary machine recovery process.
2. Do not run the OVOC software on the secondary machine at this stage. Just make sure the machine is up and running.
3. Verify that server software version is the same as on the Primary server, by checking the OVOC server Manager title.
4. Start the secondary server machine, making sure that all the processes are up and running.

5. Make sure that all backup files are in the /data/NBIF directory.
6. In EMS Server Manager, go to the Application Maintenance menu and select the **Restore** option (OVOC Server Restore on page 99).
7. Follow the instructions during the process; you might need to press **Enter** a few times.
8. After the restore operation has completed, you are prompted to reboot the OVOC server.
9. If you have installed custom certificates prior to the restore, you must re-install them.
10. Login to the OVOC Web client and verify that there is connectivity and the application is functioning correctly.
11. If you are using one or more features which are marked in the table below as 'Not Supported', please provision all the managed devices with a new Management Server IP address.
12. For SBC Fixed and Floating License Pool customers, run the *Update* command for all the managed devices .

See the table below summarizing the features affected by Disaster Recovery functionality.

**Table 32-1: Features Affected by Disaster Recovery Functionality**

Feature	Status
Management	
Alarms+ NAT communication based on Keepalive traps	Supported
Fixed License Pool and Floating License	Not Supported
IP Phones Manager Pro: Alarms / Status reports	Not Supported
Advanced Quality Package	-
SBC/GW Voice Quality Monitoring	Supported
Endpoint Quality monitoring (RFC 6035)	Not Supported
Server	-
Server: Device NTP Server	Supported
Server: Device Syslog Server	Not Supported
Server: Device TP Debug recording server	Not Supported

## 33 Service Provider - Enhanced Specifications for VMware Virtual Platform

This Appendix describes the specifications for supporting an enhanced customized platform for service providers. Additional manual operations are required to be performed by customers to support this enhancement (Required Updates ).

The following table describes the machine specifications for this platform.

**Table 33-1: Service Provider Custom Specification for VMware Virtual Platform**

Item	Machine Specification
Memory	256GB
CPU	24 cores at 2.60 GHz
Disk	SSD 6TB
Ethernet	1x10GB + 4x1 GB ports

The following table specifies the enhanced service provider capacities.

**Table 33-2: Service Provider - Enhanced Capacity**

Item	Capacity
Topology	
OVOC Managed Devices <sup>1</sup>	11000
Tenants	100
Regions	100 (1 per Tenant)
Devices	10,000 MP 1xx devices or equivalent + 1000 SBCs (100 MPs + 10 SBCs per Region)
Maximum number of managed endpoints in OVOC (IP Phone Manager Pro only).	-
Voice Quality	
Maximum Number of CAPS (calls attempts per second) per device.	0.1
Maximum number of CAPS per server (SBC and Skype for Business).	1000
Maximum concurrent sessions	100,000
Maximum number of devices per region	100
Maximum number of managed devices.	10,000
Call Details Storage - Detailed information	Up to one year or 250 million calls.

<sup>1</sup>If OVOC links are not used, up to 10,000 devices are supported.

Item	Capacity
per Call (not including Trends)	
Calls Statistics Storage - Statistic information storage.	Up to one year or 500 million intervals.
Device Manager Pro	
Maximum number of devices managed by the Device Manager Pro	-
Maximum number of CAPS per IP Phone	-
SIP Call Flow (for SBC calls only)	
Maximum Number of CAPS (calls attempts per second) per device.	-
Maximum number of devices	-
Alarms	
Steady state	50 alarms per second
Burst rate	200,000 alarms per second
Accumulative alarm rate	5 alarms per second (apply filter if more)
Alarm Forwarding	1 rule per type (syslog, SNMP, mail)

**International Headquarters**

1 Hayarden Street,  
Airport City  
Lod 7019900, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

200 Cottontail Lane  
Suite A101E  
Somerset NJ 08873  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

**Contact us:** <https://www.audiocodes.com/corporate/offices-worldwide>

**Website:** <https://www.audiocodes.com/>

©2020 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-94171

