

# One Voice Operations Center

Version 7.4



---

## Table of Contents

---

<b>1</b>	<b>Overview .....</b>	<b>17</b>
<hr/>		
	<b>Pre-installation Information .....</b>	<b>19</b>
<b>2</b>	<b>Managed VoIP Equipment .....</b>	<b>21</b>
<b>3</b>	<b>Hardware and Software Specifications .....</b>	<b>23</b>
<b>3.1</b>	<b>OVOC Server and Client Requirements.....</b>	<b>23</b>
<b>3.2</b>	<b>Bandwidth Requirements .....</b>	<b>25</b>
3.2.1	OVOC Bandwidth Requirements .....	25
3.2.2	Voice Quality Bandwidth Requirements .....	25
<b>3.3</b>	<b>Fault Management - Alarms History .....</b>	<b>26</b>
<b>3.4</b>	<b>Performance and Data Storage .....</b>	<b>26</b>
<b>3.5</b>	<b>Skype for Business Monitoring SQL Server Prerequisites.....</b>	<b>29</b>
<b>4</b>	<b>OVOC Software Deliverables .....</b>	<b>31</b>
<b>4.1</b>	<b>Dedicated Hardware Installation – DVDs 1-3.....</b>	<b>31</b>
<b>4.2</b>	<b>VMware Installation .....</b>	<b>32</b>
4.2.1	VMware Upgrade Media .....	32
<hr/>		
	<b>OVOC Server Installation .....</b>	<b>33</b>
<b>5</b>	<b>Testing Installation Requirements -Dedicated Hardware .....</b>	<b>35</b>
<b>6</b>	<b>Installing the OVOC Server on Dedicated Hardware.....</b>	<b>37</b>
<b>6.1</b>	<b>Files Verification.....</b>	<b>37</b>
6.1.1	Windows .....	37
6.1.2	Linux .....	38
6.1.3	OVOC Server Users .....	38
<b>6.2</b>	<b>DVD1: Linux CentOS 7.3 .....</b>	<b>39</b>
6.2.1	Installing DVD1 without a CD-ROM.....	43
<b>6.3</b>	<b>DVD2: Oracle DB Installation.....</b>	<b>47</b>
<b>6.4</b>	<b>DVD3: OVOC Server Application Installation.....</b>	<b>50</b>
<b>7</b>	<b>Installing OVOC on the AWS Platform .....</b>	<b>55</b>
<b>8</b>	<b>Installing the OVOC on a Virtual Server Platform.....</b>	<b>61</b>
<b>8.1</b>	<b>Installing the OVOC Server on the VMware Platform .....</b>	<b>61</b>
8.1.1	Installing the VMware Virtual Machine.....	61
8.1.2	Configuring the Virtual Machine Hardware Settings .....	69
8.1.3	Connecting OVOC Server to Network .....	71
8.1.4	Configuring OVOC Virtual Machines (VMs) in a VMware Cluster .....	72
8.1.4.1	Site Requirements .....	72
8.1.4.2	Cluster Host Node Failure .....	75
<b>8.2</b>	<b>Installing the OVOC Server on Microsoft Hyper-V Platform .....</b>	<b>75</b>
8.2.1	Installing the Microsoft Hyper-V Virtual Machine .....	76
8.2.2	Configuring the Virtual Machine Hardware Settings .....	80

8.2.2.1	Expanding Disk Capacity .....	82
8.2.3	Changing MAC Addresses from 'Dynamic' to 'Static' .....	85
8.2.4	Connecting OVOC Server to Network .....	86
8.2.5	Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster .....	87
8.2.5.1	Site Requirements .....	87
8.2.5.2	Add the OVOC VM in Failover Cluster Manager .....	88
8.2.5.3	Cluster Host Node Failure .....	90
<b>OVOC Server Upgrade .....</b>		<b>91</b>
<b>9</b>	<b>Upgrading the OVOC Server on Dedicated Hardware.....</b>	<b>93</b>
9.1	Upgrading the OVOC Server-DVD.....	93
9.2	Upgrading the OVOC server using an ISO File .....	96
<b>10</b>	<b>Upgrading OVOC on a Virtual Platform.....</b>	<b>97</b>
10.1	Step 1: Setup the Virtual Machine .....	97
10.1.1	VMware Platform .....	97
10.1.1.1	Setting up Using VMware Remote Console Application (VMRC) ....	101
10.1.1.2	Setting up Using VMware Server Host.....	104
10.1.2	Microsoft Hyper-V Platform.....	105
10.2	Step 2: Run the Upgrade Script.....	109
10.3	Step 3: Connect the OVOC Server to Network.....	111
10.3.1	VMware Platform .....	111
10.3.2	Hyper-V Platform .....	113
<b>OVOC Server Machine Backup and Restore .....</b>		<b>115</b>
<b>11</b>	<b>OVOC Server Backup.....</b>	<b>117</b>
11.1	Change Schedule Backup Time .....	117
<b>12</b>	<b>OVOC Server Restore .....</b>	<b>119</b>
<b>OVOC Server Manager .....</b>		<b>121</b>
<b>13</b>	<b>Getting Started .....</b>	<b>123</b>
13.1.1	Connecting to the EMS Server Manager .....	123
13.1.2	Using the EMS Server Manager .....	126
<b>14</b>	<b>Viewing Process Statuses.....</b>	<b>127</b>
<b>15</b>	<b>Viewing General Information.....</b>	<b>129</b>
<b>16</b>	<b>Collecting Logs .....</b>	<b>131</b>
<b>17</b>	<b>Application Maintenance .....</b>	<b>133</b>
17.1	Start /Stop the Application.....	133
17.2	Web Servers.....	134
17.2.1	Apache and Tomcat Server Processes .....	134
17.2.2	HTTP/HTTPS Services.....	135



17.3	Change Schedule Backup Time .....	135
17.4	Restore .....	135
17.5	License .....	136
17.5.1	OVOC Time License .....	137
17.6	Shutdown the OVOC Server Machine .....	138
17.7	Reboot the OVOC Server Machine .....	139
18	Network Configuration .....	141
18.1	Server IP Address .....	141
18.2	Ethernet Interfaces .....	143
18.2.1	OVOC Client Login on all OVOC Server Network Interfaces .....	143
18.2.2	Add Interface .....	144
18.2.3	Remove Interface .....	145
18.2.4	Modify Interface .....	145
18.3	Ethernet Redundancy .....	146
18.3.1	Add Redundant Interface .....	147
18.3.2	Remove Ethernet Redundancy .....	149
18.3.3	Modify Redundant Interface .....	150
18.4	DNS Client .....	151
18.5	NAT .....	152
18.6	Static Routes .....	152
18.7	SNMP Agent .....	153
18.7.1	SNMP Agent Listening Port .....	155
18.7.2	Linux Trap Forwarding Configuration .....	155
18.7.3	Server SNMPv3 Engine ID .....	156
19	Date and Time Settings .....	157
19.1	NTP .....	157
19.1.1	Stopping and Starting the NTP Server .....	158
19.1.2	Restrict Access to NTP Clients .....	159
19.2	Timezone Settings .....	159
19.3	Date and Time .....	159
20	Security .....	161
20.1	OVOC User .....	162
20.2	SSH .....	163
20.2.1	SSH Log Level .....	163
20.2.2	SSH Banner .....	164
20.2.3	SSH on Ethernet Interfaces .....	165
20.2.3.1	Add SSH to All Ethernet Interfaces .....	165
20.2.3.2	Add SSH to Ethernet Interface .....	166
20.2.3.3	Remove SSH from Ethernet Interface .....	166
20.2.4	Enable/Disable SSH Password Authentication .....	167
20.2.5	Enable SSH IgnoreUserKnownHosts Parameter .....	167
20.2.6	SSH Allowed Hosts .....	168
20.2.6.1	Allow ALL Hosts .....	168
20.2.6.2	Deny ALL Hosts .....	169
20.2.6.3	Add Hosts to Allowed Hosts .....	169
20.2.6.4	Remove Host/Subnet from Allowed Hosts .....	170

<b>20.3 DB Password .....</b>	<b>171</b>
<b>20.4 OS Users Passwords .....</b>	<b>172</b>
20.4.1 General Password Settings .....	172
20.4.2 Operating System Users Security Extensions .....	173
<b>20.5 File Integrity Checker .....</b>	<b>175</b>
<b>20.6 Software Integrity Checker (AIDE) and Pre-linking .....</b>	<b>175</b>
<b>20.7 USB Storage.....</b>	<b>176</b>
<b>20.8 Network Options.....</b>	<b>176</b>
<b>20.9 Auditd Options.....</b>	<b>177</b>
<b>20.10 HTTPS/SSL/TLS Security.....</b>	<b>178</b>
20.10.1 Enable Statistics Report Web Page Secured Connection .....	179
20.10.2 Server Certificates Update.....	179
20.10.3 OVOC Voice Quality Package - AudioCodes Devices Communication .....	184
20.10.4 Apache Security Settings.....	185
20.10.4.1 TLS Version 1.0 .....	185
20.10.4.2 TLS Version 1.1 .....	186
20.10.4.3 Show Allowed SSL Cipher Suites.....	186
20.10.4.4 Edit SSL Cipher Suites Configuration String .....	186
20.10.4.5 Restore SSL Cipher Suites Configuration Default.....	187
20.10.4.6 HTTPS Authentication .....	187
20.10.4.7 Enable IP Phone Manager Pro and NBIF Web Pages Secured Communication .....	188
20.10.4.8 Change HTTP/S Authentication Password for NBIF Directory.....	189
<b>21 Diagnostics.....</b>	<b>191</b>
<b>21.1 Server Syslog Configuration .....</b>	<b>191</b>
<b>21.2 Devices Syslog Configuration.....</b>	<b>194</b>
<b>21.3 Devices Debug Configuration .....</b>	<b>195</b>
<b>Configuring the Firewall.....</b>	<b>197</b>
<b>22 Configuring the Firewall .....</b>	<b>199</b>
<b>Appendix .....</b>	<b>211</b>
<b>A Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen8     Servers .....</b>	<b>213</b>
<b>A.1 Prerequisites.....</b>	<b>213</b>
<b>A.2 Hardware Preparation .....</b>	<b>213</b>
<b>A.3 Configuring RAID-0 .....</b>	<b>214</b>
<b>B Managing Clusters .....</b>	<b>221</b>
<b>B.1 Migrating OVOC Virtual Machines in a VMware Cluster .....</b>	<b>221</b>
<b>B.2 Moving OVOC VMs in a Hyper-V Cluster .....</b>	<b>223</b>
<b>C Supplementary Security Procedures.....</b>	<b>227</b>
<b>C.1 Installing Custom Certificates on AudioCodes Devices .....</b>	<b>227</b>
C.1.1 Enterprise Gateways and SBC Devices .....	228
C.1.1.1 Step 1: Generate a Certificate Signing Request (CSR) .....	228

C.1.1.2	Step 2: Receive the New Certificates from the CA.....	229
C.1.1.3	Step 3: Update Device with New Certificate.....	230
C.1.1.4	Step 4: Update Device's Trusted Certificate Store.....	230
C.1.1.5	Step 5: Configure HTTPS Parameters on the Device.....	231
C.1.1.6	Step 6: Reset Device to Apply the New Configuration.....	233
C.1.2	MP-1xx Devices.....	234
C.1.2.1	Step 1: Generate a Certificate Signing Request (CSR) .....	234
C.1.2.2	Step 2: Receive the New Certificates from the CA.....	235
C.1.2.3	Step 3: Update Device with New Certificate.....	235
C.1.2.4	Step 4: Update Device's Trusted Certificate Store.....	236
C.1.2.5	Step 5: Configure HTTPS Parameters on Device .....	237
C.1.2.6	Step 6: Reset Device to Apply the New Configuration.....	237
<b>C.2</b>	<b>Cleaning up Temporary Files on OVOC Server .....</b>	<b>238</b>
<b>D</b>	<b>Transferring Files.....</b>	<b>239</b>
<b>E</b>	<b>Verifying and Converting Certificates .....</b>	<b>241</b>
<b>F</b>	<b>Self-Signed Certificates .....</b>	<b>243</b>
<b>F.1</b>	<b>Internet Explorer .....</b>	<b>243</b>
<b>F.2</b>	<b>Using Mozilla Firefox.....</b>	<b>244</b>
<b>F.3</b>	<b>Chrome .....</b>	<b>245</b>
<b>G</b>	<b>Datacenter Disaster Recovery .....</b>	<b>247</b>
<b>G.1</b>	<b>Introduction.....</b>	<b>247</b>
<b>G.2</b>	<b>Solution Description .....</b>	<b>247</b>
<b>G.3</b>	<b>Initial Requirements .....</b>	<b>248</b>
<b>G.4</b>	<b>New Customer Configuration.....</b>	<b>248</b>
<b>G.5</b>	<b>Data Synchronization Process .....</b>	<b>249</b>
<b>G.6</b>	<b>Recovery Process .....</b>	<b>249</b>
<b>H</b>	<b>Service Provider - Enhanced Specifications .....</b>	<b>251</b>
<b>H.1</b>	<b>Required Updates.....</b>	<b>253</b>
H.1.1	Property Files Updates .....	253
H.1.2	REST API Updates.....	254
H.1.3	Database Updates .....	255

## List of Figures

Figure 5-1: Linux Testing Requirements .....	36
Figure 6-1: ISO File Integrity Verification .....	38
Figure 6-2: Linux CentOS Installation .....	39
Figure 6-3: CentOS 7.3 .....	40
Figure 6-4: CentOS Installation .....	40
Figure 6-5: Linux CentOS Installation Complete .....	41
Figure 6-6: Linux CentOS Network Configuration .....	42
Figure 6-7: Information-iLO Overview .....	43
Figure 6-8: iLO Integrated Remote Console .....	43
Figure 6-9: Momentary Press .....	44
Figure 6-10: Boot Menu.....	44
Figure 6-11: Boot Sequence .....	45
Figure 6-12: Install CentOS.....	45
Figure 6-13: Start CentOS.....	46
Figure 6-14: Server Rebooted .....	46
Figure 6-15: Boot Menu.....	47
Figure 6-16: Oracle DB Installation (Linux) .....	48
Figure 6-17: Oracle DB Installation - License Agreement (Linux).....	48
Figure 6-18: Oracle DB Installation (Linux) (cont).....	48
Figure 6-19: Oracle DB Installation (Linux) (cont).....	49
Figure 6-20: OVOC Server Application Installation (Linux).....	50
Figure 6-21: OVOC Server Application Installation (Linux) – License Agreement.....	51
Figure 6-22: OVOC Server Application Installation (Linux) (cont).....	51
Figure 6-23: OVOC Server Application Install with Patches .....	52
Figure 6-24: OVOC Server Installation Complete .....	52
Figure 7-1: Select Region.....	55
Figure 7-2: Services Menu - EC2 .....	55
Figure 7-3: Images .....	56
Figure 7-4: Launch Public Images.....	57
Figure 7-5: Select an Existing Key Pair.....	58
Figure 7-6: Instance State and Status Checks.....	58
Figure 7-7: Login to OVOC Server.....	59
Figure 8-1: VMware vSphere Web Client.....	62
Figure 8-2: Hosts and Clusters.....	62
Figure 8-3: Deploy OVF Template Option.....	63
Figure 8-4: Client Integration Plug-in.....	63
Figure 8-5: Browse to OVF Package.....	64
Figure 8-6: OVF Template Details Screen .....	65
Figure 8-7: Virtual Machine Name and Location Screen .....	65
Figure 8-8: Destination Storage Screen .....	66
Figure 8-9: Setup Networking Screen .....	66
Figure 8-10: Ready to Complete Screen.....	67
Figure 8-11: Deployment Progress Screen.....	67
Figure 8-12: Edit Settings option .....	69
Figure 8-13: CPU, Memory and Hard Disk Settings .....	70
Figure 8-14: Recent Tasks .....	70
Figure 8-15: Power On .....	71
Figure 8-16: Storage Adapters .....	72
Figure 8-17: Turn On vSphere HA .....	72

Figure 8-18: Activate HA on each Cluster Node .....	73
Figure 8-19: Networking .....	73
Figure 8-20: Switch Properties .....	74
Figure 8-21: Protected VM .....	74
Figure 8-22: Installing the OVOC server on Hyper-V – Hyper-V Manager .....	76
Figure 8-23: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard .....	77
Figure 8-24: Installing OVOC server on Hyper-V – Locate Folder.....	77
Figure 8-25: Installing OVOC server on Hyper-V – Choose Import Type .....	78
Figure 8-26: Installing OVOC server on Hyper-V – Choose Destination .....	78
Figure 8-27: Installing OVOC server on Hyper-V – Choose Storage Folders.....	79
Figure 8-28: File Copy Progress Bar .....	79
Figure 8-29: Adjusting VM for OVOC server – Settings - Memory.....	80
Figure 8-30: Adjusting VM for OVOC Server - Settings - Processor.....	81
Figure 8-31: Expanding Disk Capacity .....	82
Figure 8-32: Edit Virtual Hard Disk Wizard.....	83
Figure 8-33: Edit Virtual Hard Disk Wizard-Choose Action.....	83
Figure 8-34: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk.....	84
Figure 8-35: Edit Virtual Hard Disk Wizard-Completion .....	84
Figure 8-36: Advanced Features - Network Adapter – Static MAC Address .....	85
Figure 8-37: Power On Virtual Machine .....	86
Figure 8-38: Connect to OVOC Server Console .....	87
Figure 8-39: Hyper-V-Failover Cluster Manager Nodes.....	88
Figure 8-40: Configure Role .....	88
Figure 8-41: Choose Virtual Machine .....	89
Figure 8-42: Confirm Virtual Machine.....	89
Figure 8-43: Virtual Machine Successfully Added.....	90
Figure 9-1: OVOC server Upgrade (Linux).....	94
Figure 9-2: OVOC server Upgrade (Linux) – License Agreement .....	94
Figure 9-3: OVOC Server Application Install with Patches .....	95
Figure 9-4: OVOC Server Installation Complete .....	95
Figure 9-5: OVOC server Upgrade (Linux).....	96
Figure 10-1: VMware vSphere Web Client.....	98
Figure 10-2: Hosts and Clusters.....	98
Figure 10-3: Edit Settings Option .....	99
Figure 10-4: Connection Options .....	100
Figure 10-5: Help Link to Launch Remote Console .....	101
Figure 10-6: VMware Web Client .....	102
Figure 10-7: Remote Console Application.....	102
Figure 10-8: Virtual Machine Settings .....	103
Figure 10-9: Connect to Host CD Device/ Datastore ISO file .....	104
Figure 10-10: CD/DVD Drive - Connected Status .....	104
Figure 10-11: Installing the OVOC server on Hyper-V – Hyper-V Manager .....	105
Figure 10-12: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard .....	106
Figure 10-13: Installing OVOC server on Hyper-V – Locate Folder.....	106
Figure 10-14: Installing OVOC server on Hyper-V – Choose Import Type .....	107
Figure 10-15: Installing OVOC server on Hyper-V – Choose Destination .....	107
Figure 10-16: Installing OVOC server on Hyper-V – Choose Storage Folders.....	108
Figure 10-17: File Copy Progress Bar .....	108
Figure 10-18: OVOC server Installation Script.....	109
Figure 10-19: OVOC server Upgrade (Linux) – License Agreement .....	110
Figure 10-20: OVOC Server Application Install with Patches .....	110

Figure 10-21: OVOC Server Installation Complete .....	111
Figure 10-22: Power On .....	111
Figure 10-23: Power On Virtual Machine .....	113
Figure 10-24: Connect to OVOC Server Console .....	114
Figure 13-1: EMS Server Manager Menu .....	124
Figure 14-1: Application Status .....	127
Figure 15-1: General Information .....	129
Figure 15-2: General Information .....	130
Figure 16-1: EMS Server Manager – Collect Logs .....	131
Figure 16-2: TAR File Location .....	132
Figure 17-1: Application Maintenance .....	133
Figure 17-2: Start or Stop the OVOC Server.....	134
Figure 17-3: – Web Servers .....	134
Figure 17-4: License Manager .....	137
Table 17-5: License Pool Parameters .....	137
Figure 18-1: Network Configuration .....	141
Figure 18-2: EMS Server Manager – Change Server's IP Address.....	142
Figure 18-3: IP Configuration Complete.....	142
Figure 18-4: OVOC Server: Triple Ethernet Interfaces .....	143
Figure 18-5: EMS Server Manager – Configure Ethernet Interfaces .....	144
Figure 18-6: Physical Ethernet Interfaces Redundancy.....	146
Figure 18-7: Ethernet Redundancy Configuration.....	147
Figure 18-8: Add Redundant Interface (Linux).....	148
Figure 18-9: Ethernet Redundancy Interface to Disable .....	149
Figure 18-10: Modify Redundant Interface (Linux).....	150
Figure 18-11: DNS Setup .....	151
Figure 18-12: Routing Table and Menu.....	152
Figure 18-13: SNMP Agent .....	154
Figure 18-14: Configure SNMP Agent.....	154
Figure 18-15: SNMP Agent Listening Port .....	155
Figure 18-16: EMS Server Manager – Configure SNMPv3 Engine ID .....	156
Figure 18-17: SNMPv3 Engine ID Configuration – Complete Configuration .....	156
Figure 19-1: EMS Server Manager - Change System Time & Date .....	157
Figure 19-2: EMS Server Manager - Configure NTP .....	158
Figure 19-3: Change System Time and Date Prompt.....	159
Figure 20-1: Security Settings .....	161
Figure 20-2: SSH Configuration .....	163
Figure 20-3: SSH Log Level Manager.....	164
Figure 20-4: SSH Banner Manager.....	164
Figure 20-5: Configure SSH on Ethernet Interfaces .....	165
Figure 20-6: Disable Password Authentication .....	167
Figure 20-7: SSH IgnoreUserKnowHosts Parameter - Confirm.....	167
Figure 20-8: Configure SSH Allowed Hosts .....	168
Figure 20-9: Add Host/Subnet to Allowed Hosts.....	169
Figure 20-10: Add Host/Subnet to Allowed Hosts-Configured Host .....	170
Figure 20-11: EMS Server Manager – Change DB Password.....	171
Figure 20-12: OS Passwords Settings with Security Extensions.....	174
Figure 20-13: Maximum Active SSH Sessions.....	174
Figure 20-14: Software Integrity Checker (AIDE) and Pre-linking.....	175
Figure 20-15: USB Storage .....	176
Figure 20-16: Network Options .....	177

Figure 20-17: Auditd Options .....	177
Figure 20-18: OVOC Maximum Security Implementation .....	178
Figure 20-19: Server Certificate Updates .....	180
Figure 20-20: Generate Server Private Key .....	180
Figure 20-21: Server Private Key Generated .....	181
Figure 20-22: Generating a Server Certificate Signing Request (CSR) .....	181
Figure 20-23: Transfer CSR File to PC .....	182
Figure 20-24: Installed Server Certificate .....	183
Figure 20-25: Installed Root Certificate .....	184
Figure 20-26: SEM - AudioCodes Device Communication .....	184
Figure 20-27: Show Allowed SSL Cipher Suites .....	186
Figure 20-28: Show SSL Cipher Suites Configuration .....	187
Figure 20-29: HTTPS Authentication .....	188
Figure 20-30: Change HTTP/S Authentication Password for NBIF Directory .....	189
Figure 21-1: Diagnostics .....	191
Figure 21-2: Syslog Configuration .....	192
Figure 21-3: Forward Messages to an External Server .....	192
Figure 22-1: Firewall Configuration Schema .....	210
Figure A-1: Hardware Preparation .....	213
Figure A-2: HP Array Configuration Utility (ACU) .....	214
Figure A-3: RAID-Latest Firmware Versions .....	215
Figure A-4: Actions Menu .....	215
Figure A-5: Clear Configuration .....	216
Figure A-6: Summary Screen .....	216
Figure A-7: Main Screen .....	217
Figure A-8: Logical Drive .....	217
Figure A-9: Summary Screen .....	218
Figure A-10: Set Bootable Logical Drive/Volume .....	218
Figure A-11: Set Bootable Logical Drive/Volume .....	219
Figure A-12: Exit Application .....	219
Figure A-13: Power Button .....	220
Figure A-14: Reboot Button .....	220
Figure B-1: Migration .....	221
Figure B-2: Change Host .....	221
Figure B-3: Target Host for Migration .....	222
Figure B-4: Migration Process Started .....	222
Figure B-5: Hyper-V Live Migration .....	223
Figure B-6: Move Virtual Machine .....	224
Figure B-7: Hyper-V Migration Process Started .....	225
Figure C-8: Context Certificates .....	228
Figure C-9: Certificate Signing Request Group .....	229
Figure C-10: Upload Certificate Files from your Computer Group .....	230
Figure C-11: Importing Certificate into Trusted Certificates Store .....	231
Figure C-12: TLS Contexts: Edit Record .....	232
Figure C-13: Device Reset .....	233
Figure C-14: Certificate Signing Request Group .....	234
Figure C-15: Maintenance Actions Page .....	237
Figure F-1: Continue to Website .....	243
Figure F-2: Mozilla Firefox Settings .....	244
Figure F-3: Chrome Browser Settings .....	245
Figure G-4: Disaster Recovery Between Two Datacenters with VMware HA .....	247

## List of Tables

Table 2-1: Managed VoIP Equipment .....	21
Table 3-1: OVOC- Minimum Platform Requirements .....	23
Table 3-2: Voice Quality Bandwidth Requirements.....	25
Table 3-3: Performance and Data Storage .....	26
Table 8-1: Virtual Machine Configuration .....	69
Table 8-2: Virtual Machine Configuration .....	80
Table 14-1: Application Statuses.....	127
Table 22-1: Firewall Configuration Rules .....	199
Table 22-2: OAM Flows: NOC/OSS → OVOC .....	209
Table 22-3: OAM Flows: OVOC → NOC/OSS.....	209
Table G-1: Features Affected by Disaster Recovery Functionality .....	250
Table H-1: Service provider custom VMware Hardware Specification .....	251
Table H-2: Service Provider - Enhanced Capacity.....	251



## 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: August-07-2018

## 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 Web site at <https://www.audiocodes.com/services-support/maintenance-and-support>.

## 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: Update to the upgrade procedure with tar file. Replaced the “OVOC Maximum Security Implementation” diagram. Updated several old EMS Server Manager screens 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 EMS Server Manager options for managing TLS version and cipher strings. New EMS Server Manager menu “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.

## 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 Web site at <https://online.audiocodes.com/documentation-feedback>.

## Related Documentation

Manual Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500 E-SBC User's Manual
Mediant 500L E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
One Voice Operations Center Server Installation, Operation and Maintenance Manual
One Voice Operations Center Integration with Northbound Interfaces
One Voice Operations Center User's Manual
IP Phone Manager Pro Administrator's Manual
IP Phone Manager Express Administrator's Manual
One Voice Operations Center Product Description
One Voice Operations Center Alarms Guide
One Voice Operations Center Security Guidelines
ARM User's Manual

**This page is intentionally left blank.**

# 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.

**This page is intentionally left blank.**

# 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 Server Edition (SE) SBC	versions 7.2, 7.0 and 6.8
Mediant 3000 Media Gateways (TP-8410 and TP-6310)	versions 7.0 (SIP), 6.8 (SIP) and 6.6 (SIP)
Mediant Virtual Edition (VE) SBC	versions 7.2 (including support for MTC), 7.0 and 6.8
<b>Mediant Cloud Edition</b>	<b>version 7.2</b>
Mediant 2000 Media Gateways	version 6.6
*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
Mediant 800 MSBR	versions 7.2, 6.8 and 6.6
Mediant 500 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
*Mediant 600	version 6.6
MediaPack MP-11x series	version 6.6 (SIP)
MediaPack MP-124	Rev. D and E – version 6.6 (SIP)
MP-1288	version 7.2

SBA	
*Mediant 800B SBA	SBA version 1.1.12.x and later and gateway versions 7.2, 7.0 and 6.8
*Mediant 1000B SBA	SBA version 1.1.12.x and later and gateway versions 7.2, 7.0 and 6.8
*Mediant 2600B SBA devices	SBA version 1.1.12.x and later and gateway versions 7.2, 7.0 and 6.8
CloudBond*	
Standard Edition (Mediant 800B platform)	Version <b>7.4</b>
Standard Plus Edition (Mediant 800B platform);	Version <b>7.4</b>
Pro Edition (Mediant Server platform)	Version <b>7.4</b>
Enterprise Edition (Mediant Server platform)	Version <b>7.4</b>
Virtualized Edition (Mediant Server platform).	Version <b>7.4</b>
CCE Appliance*	
*Mediant 800 CCE Appliance	Version <b>2.1</b>
*Mediant Server CCE Appliance	Version <b>2.1</b>
IP Phones	Supported Software Versions/Models
400HD Series Lync server	From version 2.0.13: 420HD, 430HD 440HD
400HD Series Non-Lync server	From version 2.2.2: 420HD, 430HD 440HD and 405
400HD Series Skype for Business	From version 3.0.0: 420HD, 430HD 440HD and 405HD
400HD Series Skype for Business	From version 3.0.1: 420HD, 430HD 440HD, 405HD and 450HD
	From version 3.0.2: HRS (with Jabra firmware support)



**Note:**

- \* Refers to products that do not support Voice Quality Management.
- \* To support Voice Quality Management for these devices, customers should add the SBC/Media Gateway platform of the CloudBond 365 /CCE Appliances as standalone devices to the OVOC. Once this is done, the SBC/Gateway calls passing through the CloudBond 365 /CCE Appliances can be monitored.
- 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.

### 3.1 OVOC Server and Client Requirements

This section lists the platform and software required to run the OVOC dedicated hardware version and the VMware and Hyper-V version.



**Note:** For enhanced service provider specifications, refer to Appendix H.

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

Resource	OVOC Server				OVOC Web Client
	Dedicated OVOC Server - Linux OS	Amazon	Virtual OVOC - High Profile	Virtual OVOC – Low Profile	
<b>Hardware</b>	<ul style="list-style-type: none"> <li><b>G8:</b> HP DL360p</li> <li><b>G10:</b> HP DL360p</li> </ul>	—	—	—	Browser Document Size: 1280 x 768
<b>Operating System</b>	Linux CentOS Version 7.3-1611 64-bit, Rev.18	Linux CentOS Version 7.3-1611 64-bit, Rev.19	Linux CentOS Version 7.3-1611 64-bit, Rev.19	Linux CentOS Version 7.3-1611 64-bit, Rev.19	Windows™ 10/Windows 8/Windows 8.1/Windows 7/Windows 7 Enterprise/Windows Server 2012 R2 Standard

Resource	OVOC Server				OVOC Web Client
	Dedicated OVOC Server - Linux OS	Amazon	Virtual OVOC - High Profile	Virtual OVOC – Low Profile	
Virtualization platform	—	Amazon Cloud c4.4xlarge Instance Type	VMware: ESXi 6.0 <sup>1</sup> VMware HA cluster: VMware ESXi 6.0 Microsoft Hyper-V Windows server 2012R2 Microsoft Hyper-V Windows server HA cluster: 2012R2	—	—
Memory	<ul style="list-style-type: none"> <li><b>G8:</b> 32 GB RAM</li> <li><b>G10:</b> 64 GB RAM</li> </ul>	As defined in Amazon c4.4xlarge	32 GB RAM	16 GB RAM	8 GB RAM
Disk space	<ul style="list-style-type: none"> <li><b>G8:</b> Disk: 2 X 1.2 TB SAS 10K RPM in RAID 0</li> <li><b>G10:</b> Disk: 2x 1.92 TB SSD configured in RAID 0</li> </ul>	AWS EBS: General Purpose SSD (GP2)	1.2 TB	500 GB	—
Processor	<ul style="list-style-type: none"> <li><b>G8:</b> CPU: Intel Xeon E5-2690 (8 cores 2.9 GHz each)</li> <li><b>G10:</b> CPU: Intel (R) Xeon(R) Gold 6126 (12 cores 2.60 GHz each)</li> </ul>	As defined in Amazon c4.4xlarge	6 cores not less than 2 GHz	1 core not less than 2.5 GHz	—
DVD-ROM	Local ( <b>G8</b> only)	—	—	—	—

- The working space requirements on the OVOC server are as follows:
  - Linux: Executable bash
- 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.

<sup>1</sup> \* The VMware and VMware HA cluster with OVOC Server Version 7.4 (ESXi 6.0) are backward compatible with Version 7.2 (ESXi 5.5).

- Supported browsers for Web client applications are as follows:
  - Internet Explorer version 11 and higher
  - Mozilla Firefox version 38 and higher
  - Google Chrome version 60 and higher
- Flash Version 11 is required for generating Statistics Reports.

**Note:**

- 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.

## 3.2 Bandwidth Requirements

This section lists the OVOC bandwidth requirements.

### 3.2.1 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.

### 3.2.2 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 3-2: Voice Quality Bandwidth Requirements**

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
<b>SBC</b>		
MP-118	—	—
MP-124	—	—
Mediant 800 Mediant 850	60	135 Kbits/sec
Mediant 1000	150	330 Kbits / sec

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/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
<b>Gateway</b>		
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	–	–
<b>Endpoints</b>	–	56 Kbits/sec

### 3.3 Fault Management - Alarms History

The OVOC server can store history alarms for up to one year or ten million alarms.

### 3.4 Performance and Data Storage

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

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

Machine Specifications	HP DL360p G8/G10	VMware/Microsoft Hyper-V – High Profile	VMware/Microsoft Hyper-V - Low Profile
OVOC Managed Devices	5000	5000	100
Maximum number of managed endpoints in OVOC (IP Phone Manager Pro only).	10,000	<ul style="list-style-type: none"> <li>30,000 (IP Manager only)</li> <li>5,000 – including SBC/gateway management and monitoring</li> </ul>	1,000

<b>Voice Quality</b>			
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
Maximum number of calls per Day	-	-	1.9 million calls
Call Details Storage – Detailed information per Call	Up to one year or 80 million calls.	Up to one year or 80 million calls.	Up to one year or 6 million calls.
<p>Calls Statistics Storage - Statistic information storage. Statistics are collected for the following entities: Devices; Links; Sites; Endpoints and Users. Statistical data point refers to statistical information collected over a 5-minute interval.</p> <p>The following shows the exact historical statistical data time calculation example: Assuming the number of devices are 3000, the overall statistical information per device</p>	Up to one year or 150 million statistical data points per entity.	Up to one year or 150 million statistical data points per entity.	Up to one year or 12 million statistical data points per entity.

is calculated as follows:			
<ul style="list-style-type: none"> <li>150,000,000 / 3000 devices = 50,000 statistical data points per device.</li> <li>50,000 / 12 statistical data points per hour / 24 hours a day / 30 days a month = 5.78 months of historical data per device.</li> </ul>			
<b>RFC 6035 Endpoints Quality Monitoring</b>			
Maximum number of CAPS	10	5	1
<b>SIP Call Flow (for SBC calls only)</b>			
Maximum Number of CAPS (calls attempts per second) per server.	100	25	6
Maximum number of devices	100	100	10
Maximum number of calls per day	-	-	350,000 calls
Call Details Storage - Call Flow information per Call	Up to one year or 1 million calls.	Up to one year or 1 million calls.	Up to one year or 1 million calls.
<b>Capacity with SBC Floating License Capability</b>			
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.	1000	500	100



Maximum number of calls per day with SIP Call Flow	-	-	250,000 calls
Maximum number of calls per day without SIP Call Flow	-	-	1.7 million calls

## 3.5 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>

**This page is intentionally left blank.**

## 4 OVOC Software Deliverables

This section describes the OVOC software deliverables.

### 4.1 Dedicated Hardware Installation – DVDs 1-3

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

- **DVD1:** Operating System DVD for Linux (see Section 3.1):
- **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.
- Documentation – All documentation related to the present OVOC version. The documentation folder includes the following documents and sub-folders:
  - ◆ One Voice Operations Center Integration with Northbound Interfaces
  - ◆ One Voice Operations Center Alarms Guide
  - ◆ One Voice Operations Center Release Notes
  - ◆ One Voice Operations Center User's Manual
  - ◆ Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center Ver. 7.4
  - ◆ P Phone Manager Pro Administrator's Manual
  - ◆ One Voice Operations Center Product Description
  - ◆ AudioCodes One Voice Operations Center Security Guidelines
  - ◆ One Voice Operations Center IOM Manual



**Note:** Installation files can also be downloaded from the AudioCodes Website by registered customers at <https://services.audiocodes.com>.

## 4.2 VMware Installation

The OVOC DVD software delivery (**DVD5**) for the clean installation of the VMware includes the following folders:

- VMware for clean install
- Documentation

### 4.2.1 VMware Upgrade Media

The Virtual Machine software delivery (OVA file or ZIP file) and the documentation set is provided on **DVD3**.



**Note:** Installation files can also be downloaded from the AudioCodes Website by registered customers at <https://services.audiocodes.com>.

# Part II

## OVOC Server Installation

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



## 5 Testing Installation Requirements - Dedicated Hardware

Before commencing the OVOC server installation procedure, verify that your system meets the hardware, disk space, operating system and other requirements that are necessary for a successful installation.

To ensure that your machine meets the minimal hardware requirements for running the OVOC application on both dedicated and virtual hardware, run the commands described below in **tbash**.

- **RAM** - A minimum of <machine type\_RAM> GB is required (see Chapter 3). To determine the amount of random access memory installed on your system, enter the following command:

```
more /proc/meminfo | grep MemTotal
```

- **Swap Space** - Swap space is twice the system's physical memory, or 4 GB, whichever is greater.

To determine the amount of swap space currently configured in your system, enter the following command:

```
more /proc/meminfo | grep SwapTotal
```

**Disk Space** – A minimum of <machine type\_disk space> GB is required (see Chapter 3). To determine the amount of disk space on your system, enter the following command:

```
fdisk -l | grep Disk
```

During the application installation, you are required to reserve up to 2 GB of Temporary disk space in the **/tmp**. If you do not have enough space in the **/tmp** directory, set the **TMPDIR** and **TMP** environment variables to specify a directory with sufficient space.

- **DVD-ROM device** - A DVD-ROM drive capable of reading ISO 9660 format.

**Figure 5-1: Linux Testing Requirements**

```
[root@EMS-Server-Linux113 ~]# tssh
[root@EMS-Server-Linux113 ~]# uname
Linux
[root@EMS-Server-Linux113 ~]# more /proc/meminfo | grep MemTotal
MemTotal:      2017056 kB
[root@EMS-Server-Linux113 ~]# more /proc/meminfo | grep SwapTotal
SwapTotal:      3020180 kB
[root@EMS-Server-Linux113 ~]# fdisk -l | grep Disk
Disk /dev/sda: 250.0 GB, 250059350016 bytes
[root@EMS-Server-Linux113 ~]#
```



**Note:** Use the AudioCodes' DVD1 to install the Linux Operating System.



## 6 Installing the 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.



**Important:** If you are upgrading from Version 7.2.3000, you can optionally migrate this platform to Version 7.4 (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center Version 7.4*).

### 6.1 Files Verification

You need to verify the contents of the ISO, Zip or OVA 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 below)
- Linux (see Section 6.1.2).

#### 6.1.1 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))

## 6.1.2 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 6-1: 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
```

## 6.1.3 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 EMS Server Manager and OVOC application execution.
- *acems* user: The **only available user** for login through SSH/SFTP tasks.
- *emsadmin* user: User with permissions for mainly the EMS 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.
- *oralsnr* user: User in charge of oracle listener startup.

## 6.2 DVD1: Linux CentOS 7.3

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



**Note:** Before commencing the installation, you must configure RAID-0 (see Appendix A).

➤ **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 6-2: Linux CentOS Installation**

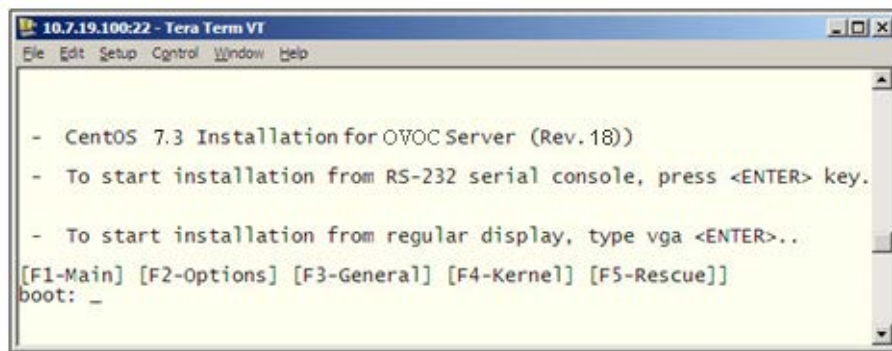
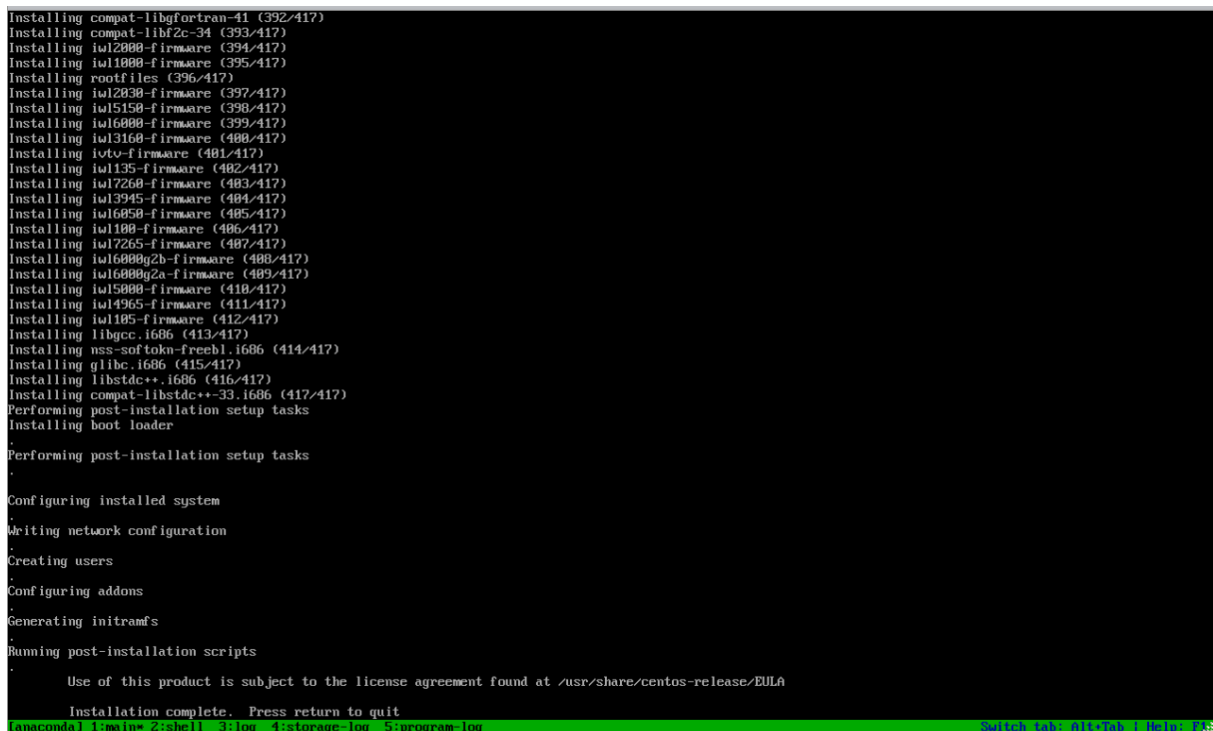


Figure 6-3: CentOS 7.3



6. Wait for the installation to complete.

Figure 6-4: CentOS Installation

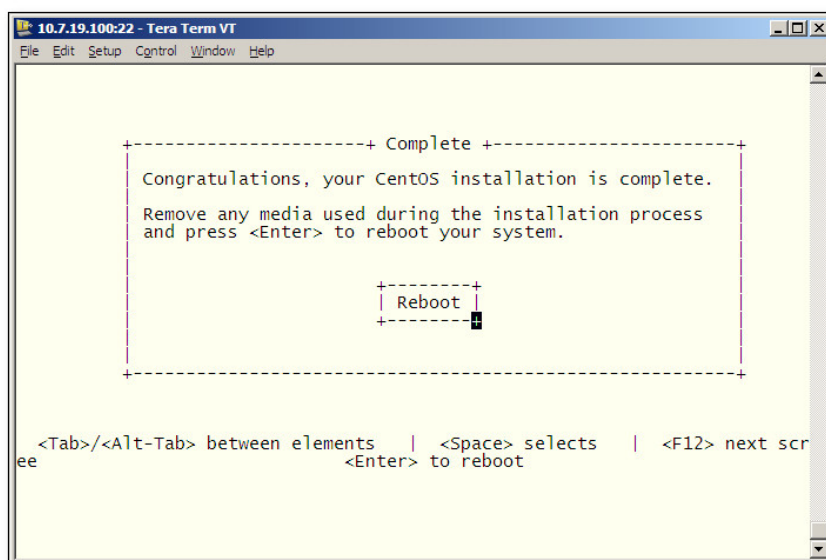


7. Reboot your machine by pressing Enter.



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

**Figure 6-5: 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 6-6: 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.
```



**Note:** This script can only be used during the server installation process. Any additional Network configuration should later be performed using the EMS 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**.

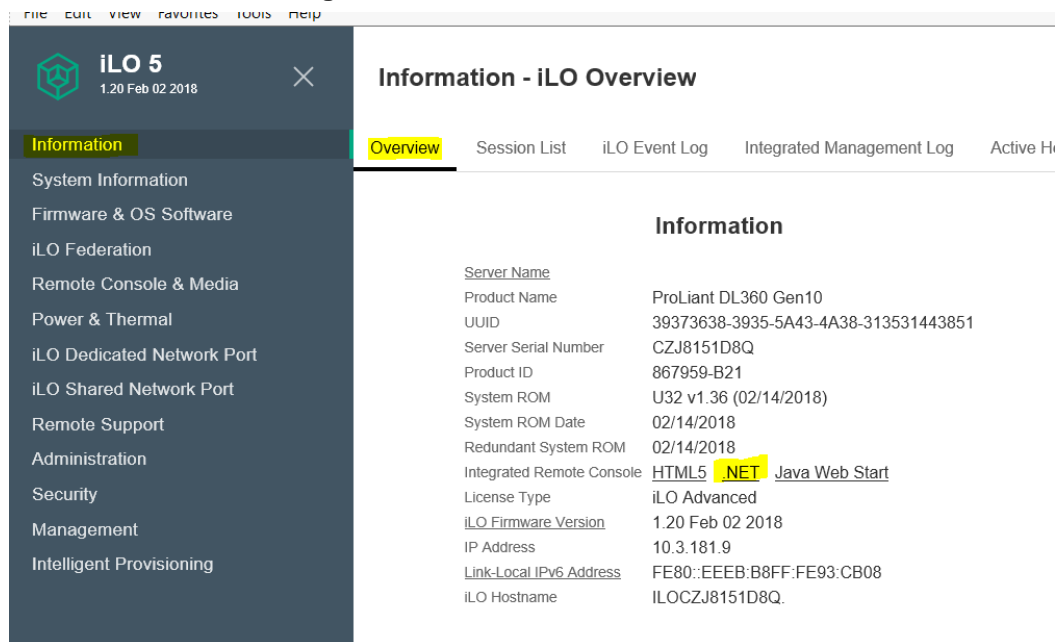
## 6.2.1 Installing DVD1 without a CD-ROM

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

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

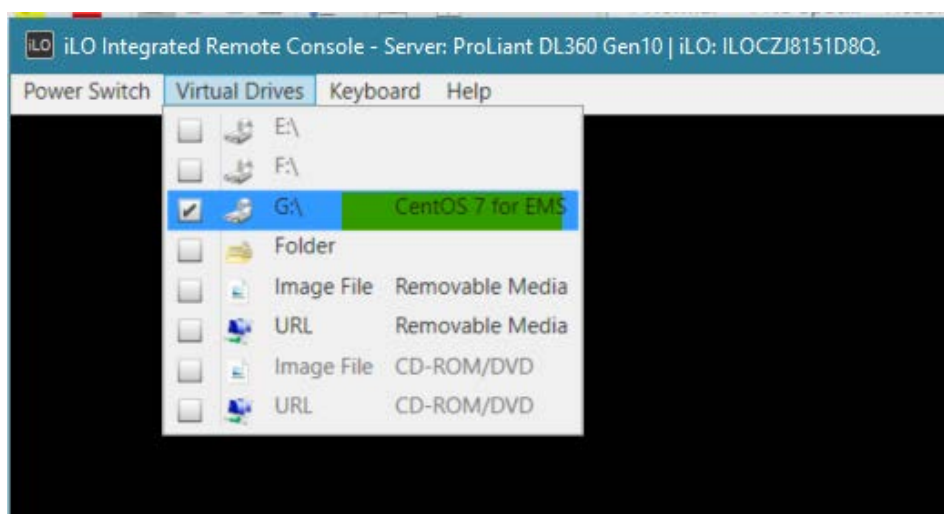
1. Login to iLO 5 with “Administrator” privileges.
2. Launch the Integrated Remote Console.

**Figure 6-7: Information-iLO Overview**



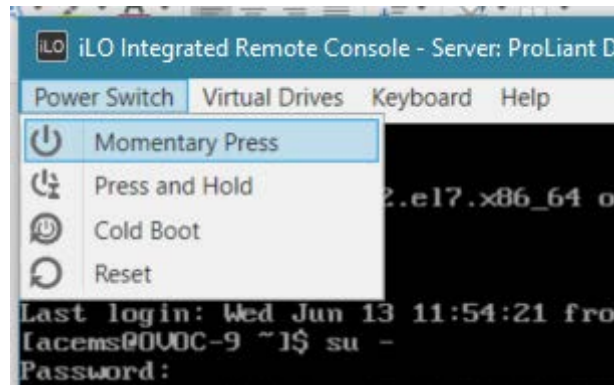
3. On your PC insert the OVOC DVD1 to the drive and note the drive letter.
4. From Integrated Remote Console, click **Virtual Drives** and select the appropriate drive letter.

**Figure 6-8: iLO Integrated Remote Console**



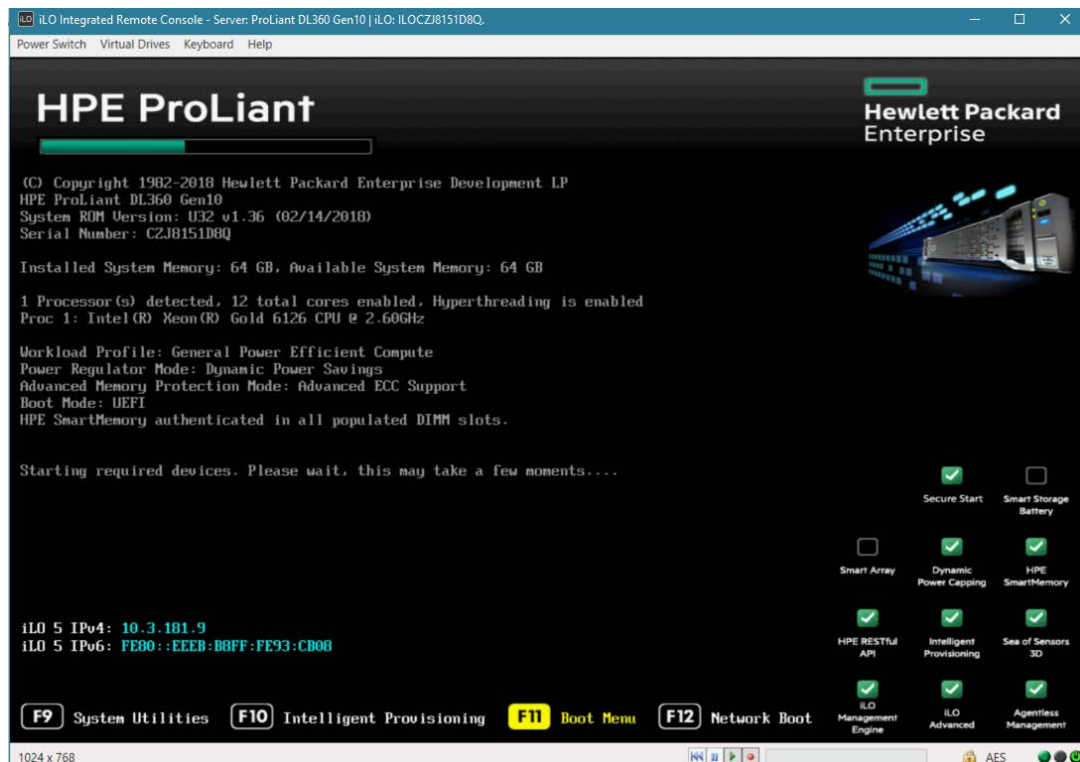
5. From Integrated Remote Console, click **Power Switch > Momentary Press**, the server is shutdown. Click **Momentary Press** to power the server back on.

**Figure 6-9: Momentary Press**



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

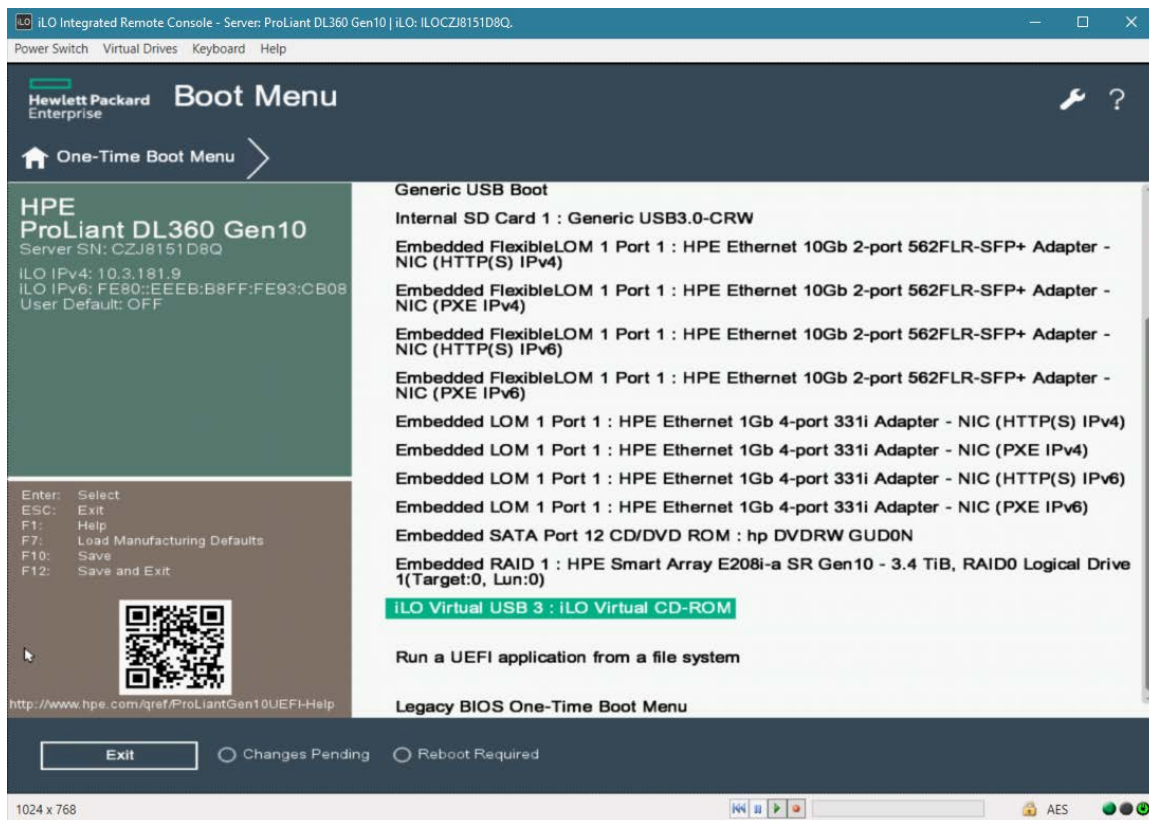
**Figure 6-10: Boot Menu**



7. 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.

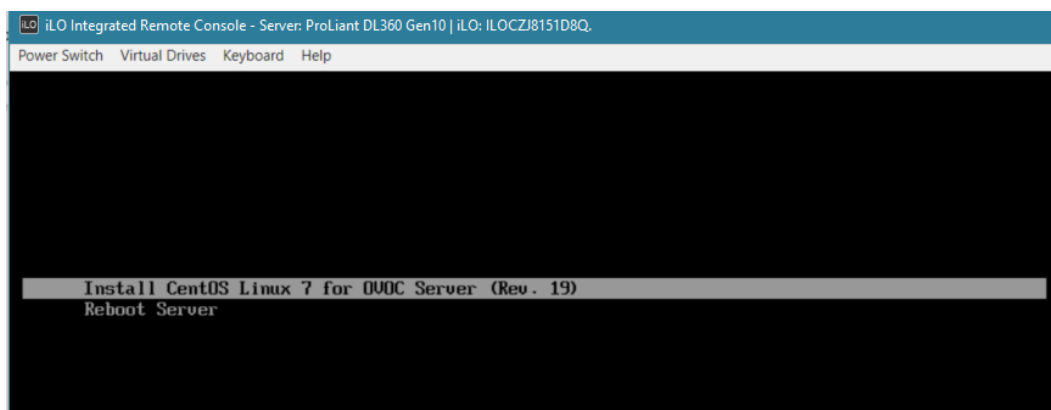


Figure 6-11: Boot Sequence



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

Figure 6-12: Install CentOS



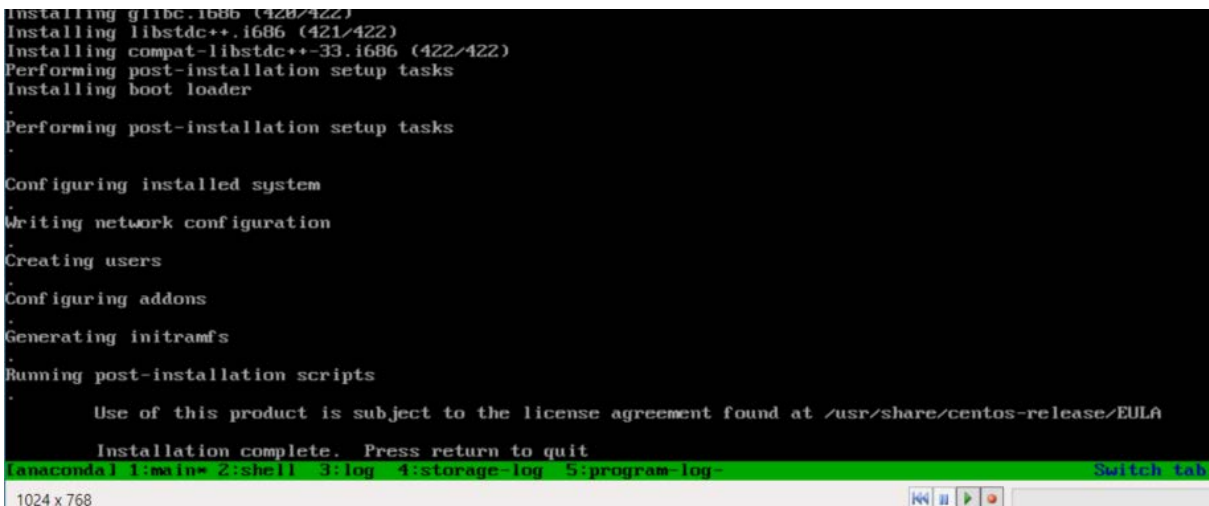
9. After a while the CentOS installation commences:

Figure 6-13: Start CentOS



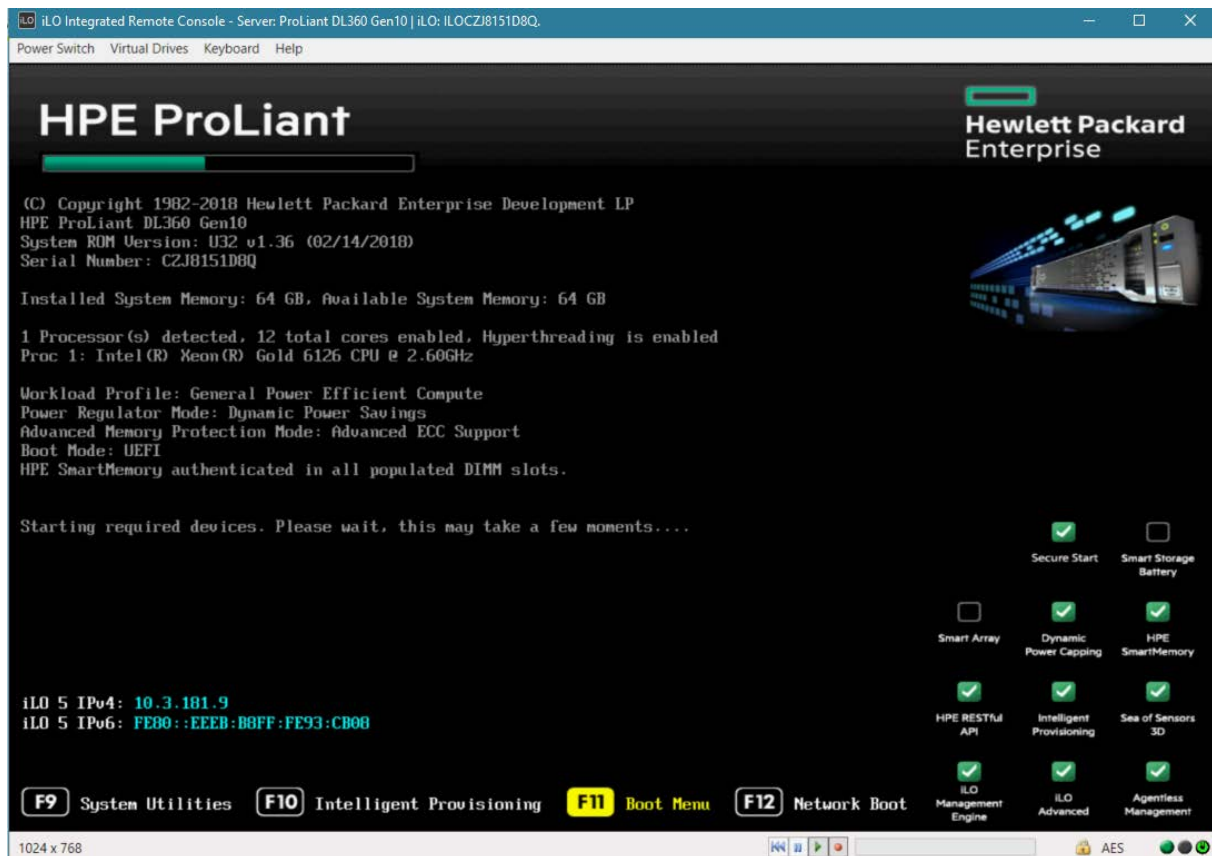
10. Wait for the installation to finish, from "Virtual Drives" menu deselect the selected drive and press Enter, the server is rebooted.

Figure 6-14: Server Rebooted



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

Figure 6-15: Boot Menu



## 6.3 DVD2: Oracle DB Installation

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



**Note:** 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
```



Figure 6-19: Oracle DB Installation (Linux) (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# █
```

## 6.4 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 6-20: OVOC Server Application Installation (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 AC
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 6-21: OVOC Server Application Installation (Linux) – License Agreement

```

based upon the net income of Licensors.
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 Licensors and any attempt to do so shall be without effe
ffered 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 Licensors 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 6-22: OVOC Server Application Installation (Linux) (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 9.



**Note:** After the OVOC server has rebooted, repeat steps 2 to 6.

Figure 6-23: OVOC Server Application Install with Patches

```
Done
>>> Copy Oracle Security Patch
...
>>> Remove Old Oracle Security Patch Files
...
>>> Applying Oracle Security Patch
...

-----
Installing Oracle CPU patch 9655014
-----

NOTE: patch installation may take up to 30 min, so be patient

Oracle patch 9655014 is already installed
>>> ===== ...
>>> Installation Completed, Oracle is Now Secured ...
>>> ===== ...
>>> Remove /tmp/EmsServerInstall ...
EMS-Server17# reboot
```

Figure 6-24: 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 (see Chapter 14) and verify login to the OVOC Web client is successful.



14. Verify that the Date and Time are set correctly (see Section 19.3 to set the date and time).
15. Configure other settings as required (see Chapter 13).

**This page is intentionally left blank.**

## 7 Installing OVOC on the AWS Platform

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

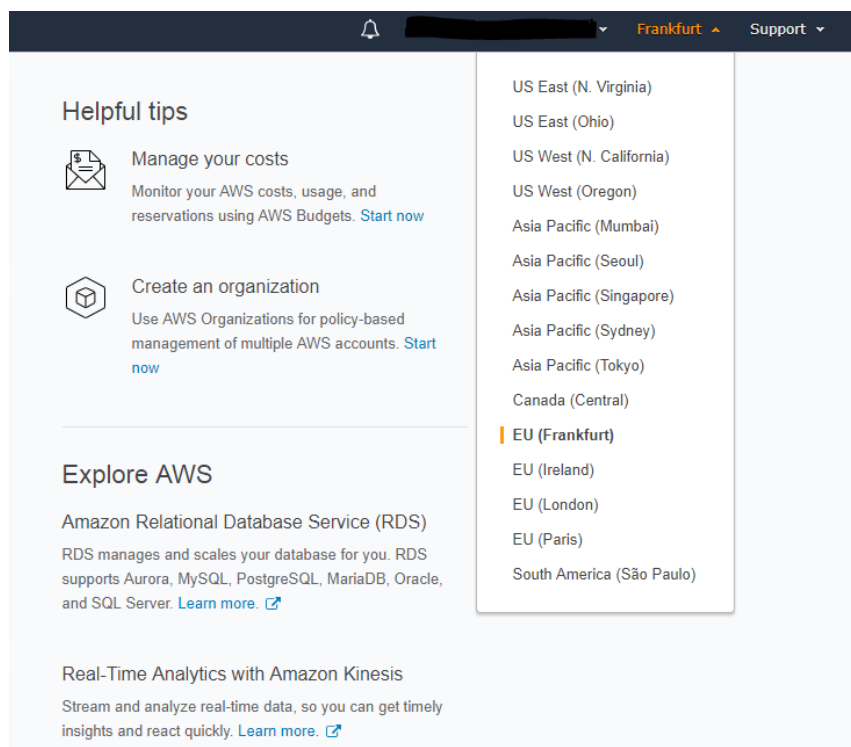
➤ **To install OVOC on the AWS platform:**

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)



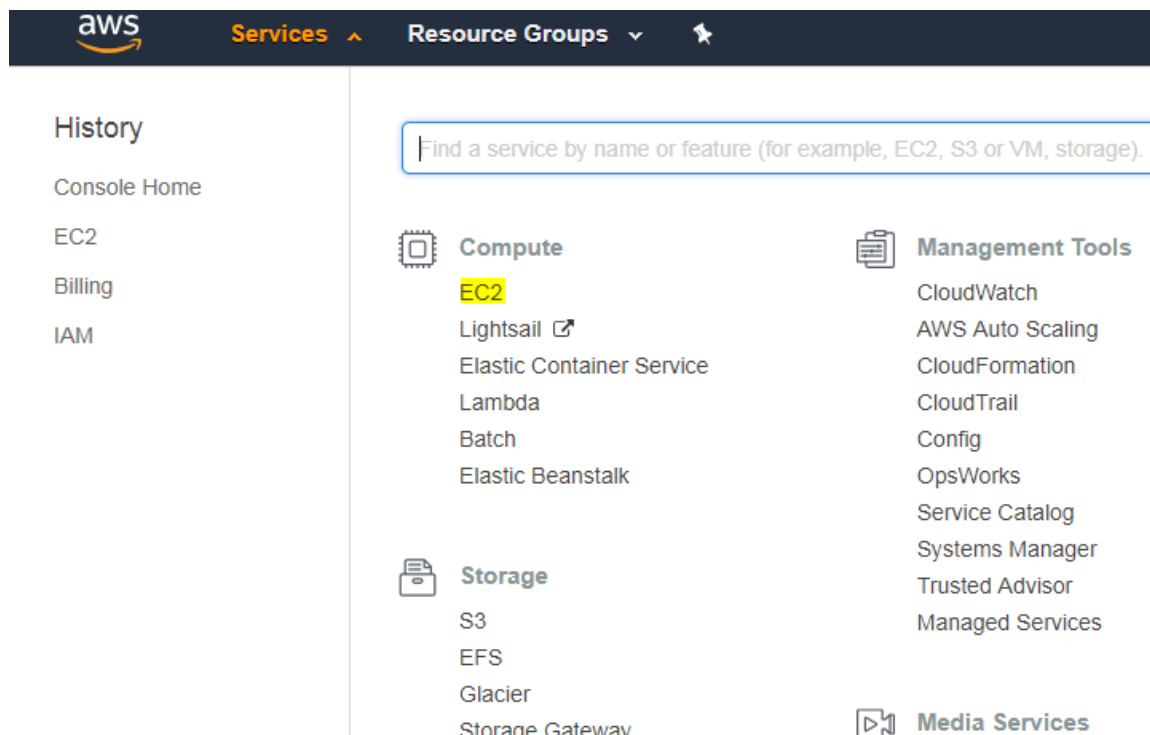
**Note:** For verifying AMI IDs, refer to <https://services.audiocodes.com>.

**Figure 7-1: Select Region**



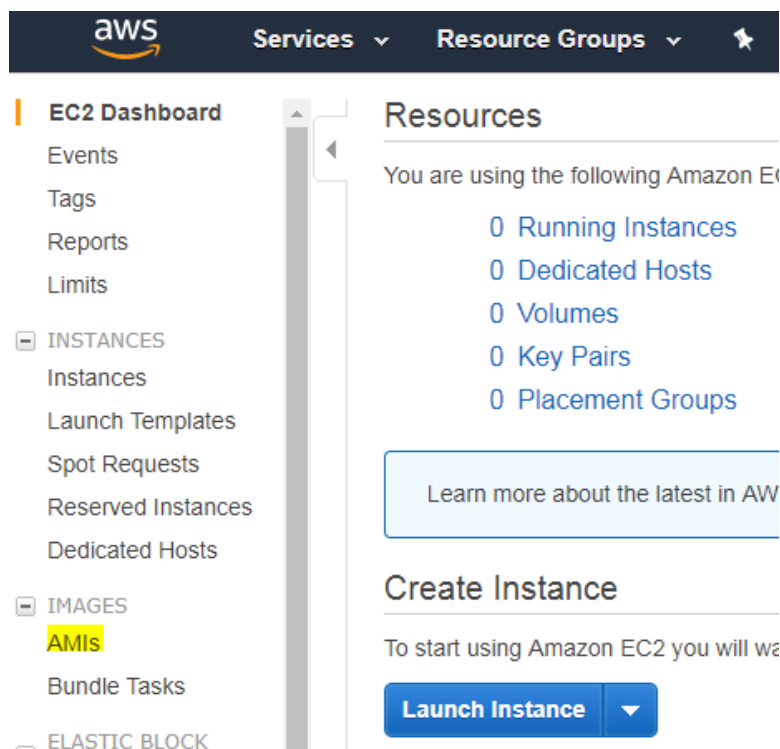
3. In the “Services” menu, choose **EC2**.

**Figure 7-2: Services Menu - EC2**



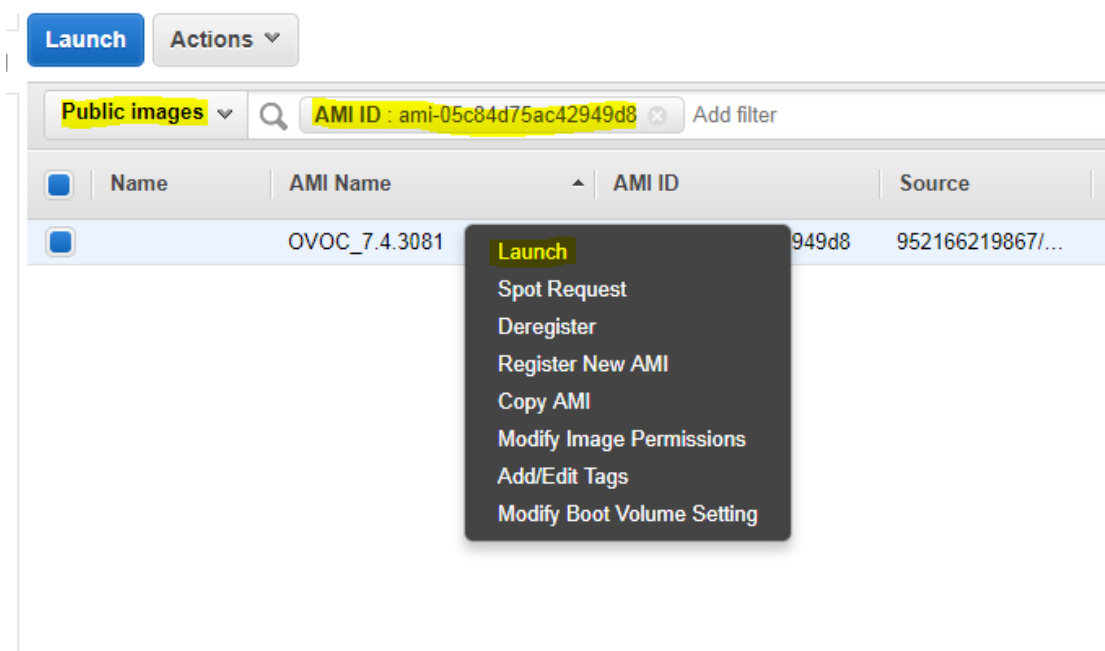
4. In the Dashboard, navigate to **IMAGES > AMIs**.

**Figure 7-3: 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 7-4: 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 22).
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 7-5: Select an Existing Key Pair

Select an existing key pair or create a new key pair

X

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

- 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 7-6: 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

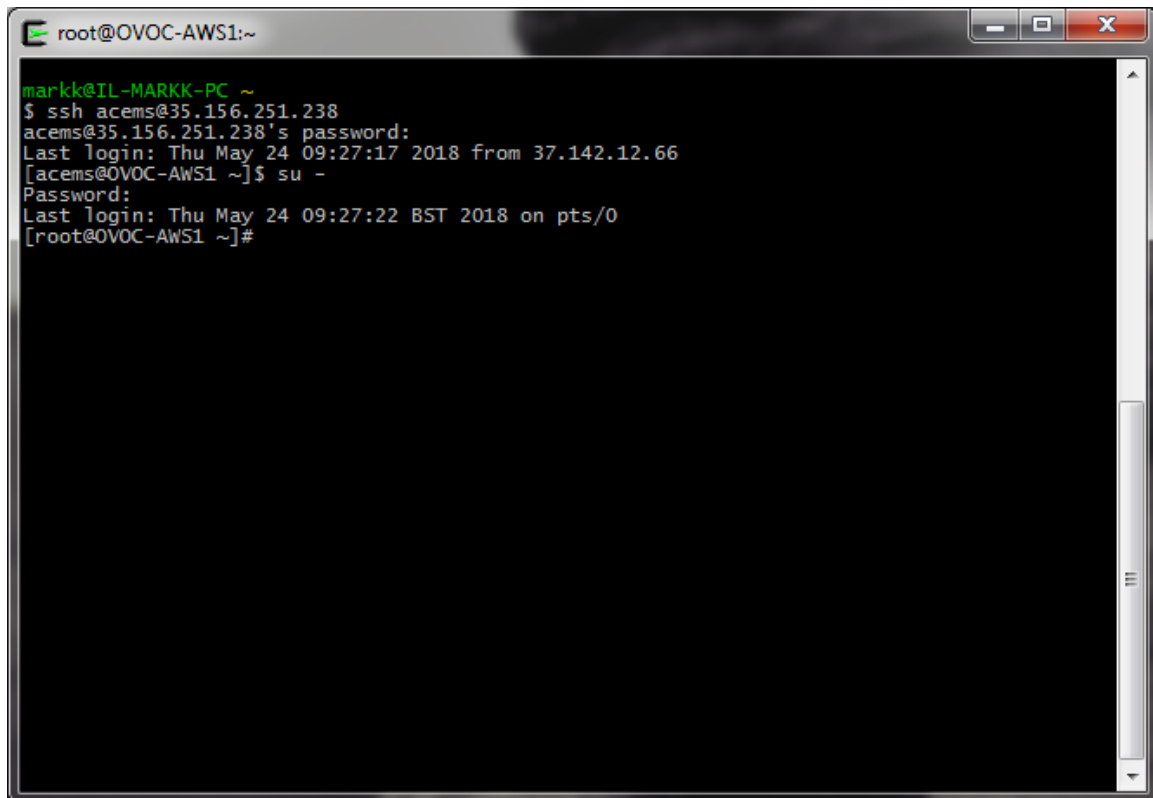
Public DNS: ec2-35-156-251-238.eu-central-1.compute.amazonaws.com

Description	Status Checks	Monitoring	Tags
<div>Instance ID</div> <div>Instance state</div> <div>Instance type</div> <div>Elastic IPs</div> <div>Availability zone</div> <div>Security groups</div> <div>Scheduled events</div> <div>AMI ID</div> <div>Platform</div>	<div>Public DNS (IPv4)</div> <div>IPv4 Public IP</div> <div>IPv6 IPs</div> <div>Private DNS</div> <div>Private IPs</div> <div>Secondary private IPs</div> <div>VPC ID</div> <div>Subnet ID</div> <div>Network interfaces</div>	<div>ec2-35-156-251-238.eu-central-1.compute.amazonaws.com</div> <div>35.156.251.238</div> <div>-</div> <div>ip-172-31-43-55.eu-central-1.compute.internal</div> <div>172.31.43.55</div> <div>-</div> <div>vpc-9044cbfb</div> <div>subnet-a66befdb</div> <div>eth0</div>	

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

```
su - root
```

Figure 7-7: Login to OVOC Server



```
root@OVOC-AWS1:~  
mark@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 EMS Server Manager, change the following default passwords:
- acems OS user (see Section 20.4)
  - acladmin OVOC user (see Section 20.1)



**Important:** 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 Section 17.5).

**This page is intentionally left blank.**



## 8 Installing the OVOC on a Virtual Server Platform

This chapter describes how to install the OVOC on a Virtual Server platform. The following procedures are described:

- Installing the OVOC server on the VMware platform (see Section 8.18.1).
- Installing the OVOC server on Microsoft Hyper-V platform (see Section 8.2).

**Note:**

- The AudioCodes OVOC supports the VMware vSphere High Availability (HA) feature.
- RmanBackup files are deleted during an OVOC upgrade.

### 8.1 Installing the OVOC Server on the VMware Platform

The installation of the OVOC server on VMware vSphere platform includes the following procedures:

- Installing the Virtual Machine (VM) (see Section 8.1.1).
- Configuring the Virtual machine hardware settings (see Section 8.2.2).
- Connecting OVOC server to network (see Section 8.1.3).
- Configuring OVOC Virtual Machines (VMs) in a VMware Cluster (see Section 8.1.4)

#### 8.1.1 Installing the VMware Virtual Machine

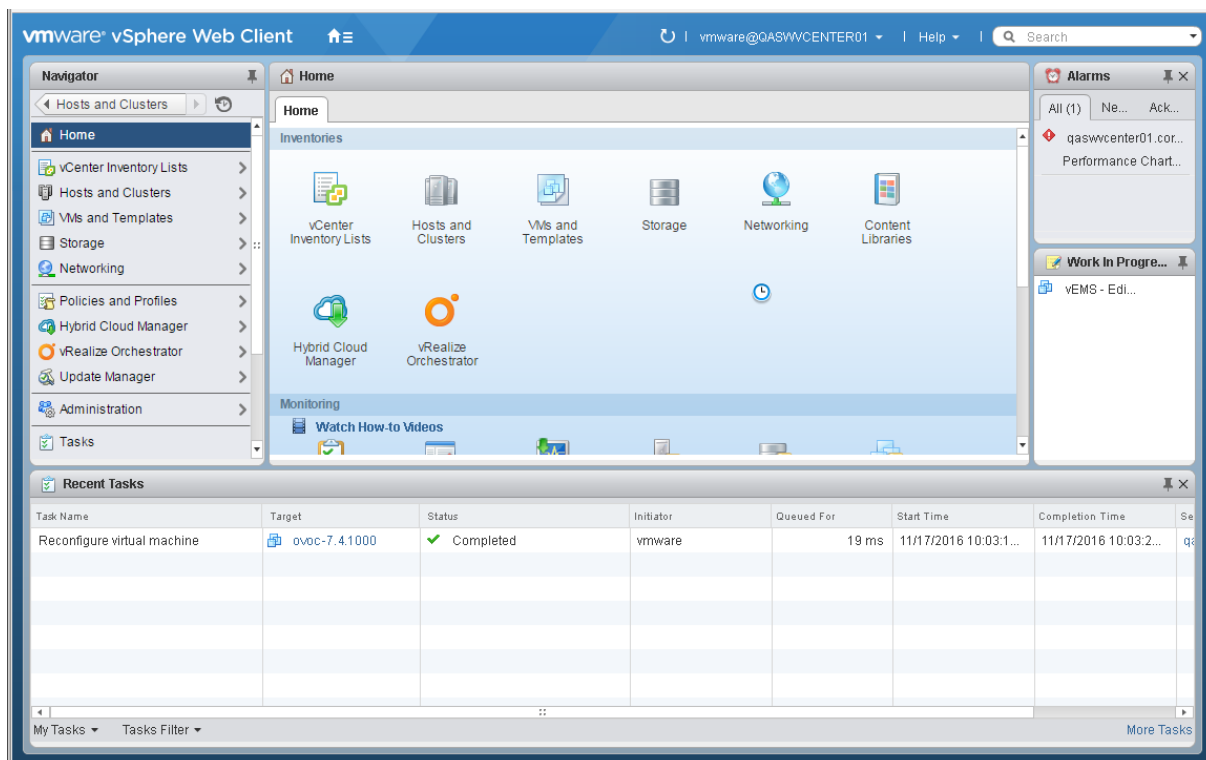
This section describes how to install the OVOC server on the VMware vSphere platform. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in Section 8.2.2). The upgrade time depends on the hardware machine where the VMware vSphere platform is installed.

The VMware Virtual Machine installation package is provided on **DVD 5** (see Section 4.2).

➤ **To install the OVOC Server on VMware vSphere:**

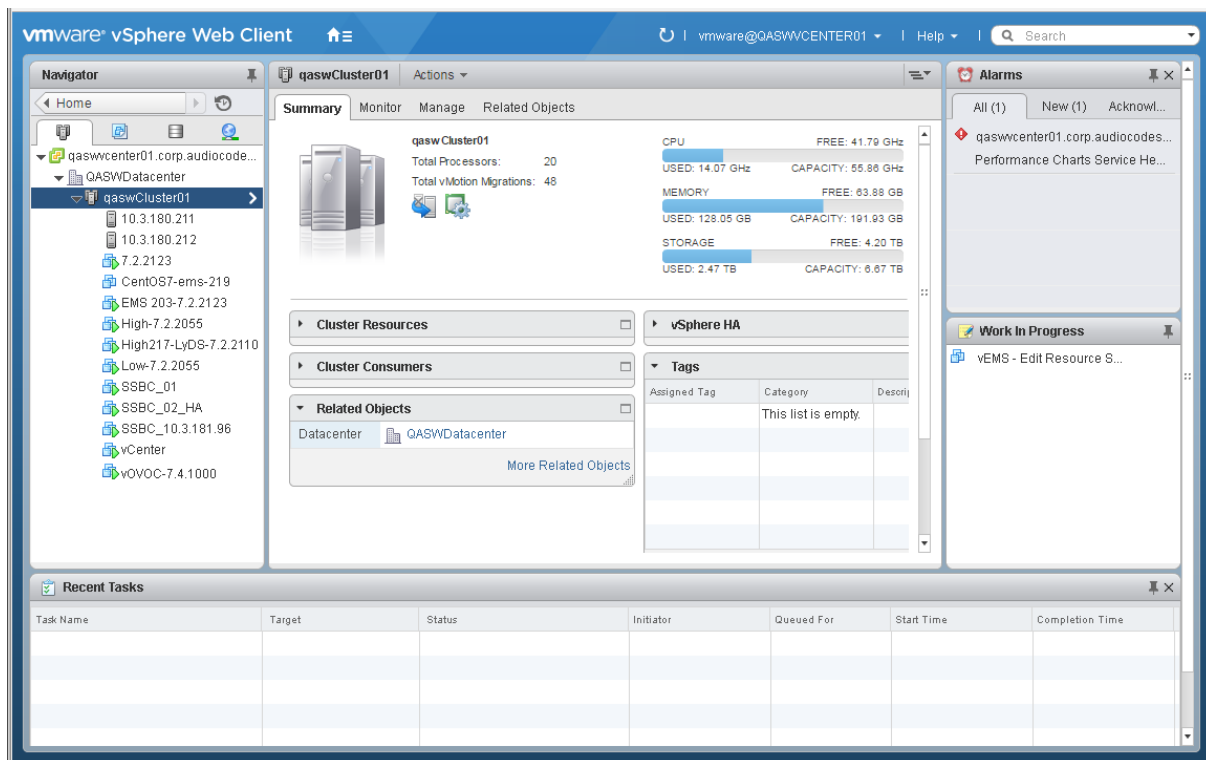
1. Transfer the OVA file containing the VMware Virtual Machine installation package from **DVD 5** to your PC (see Appendix D for instructions on how to transfer files).
2. Login to the VMware vSphere Web client.

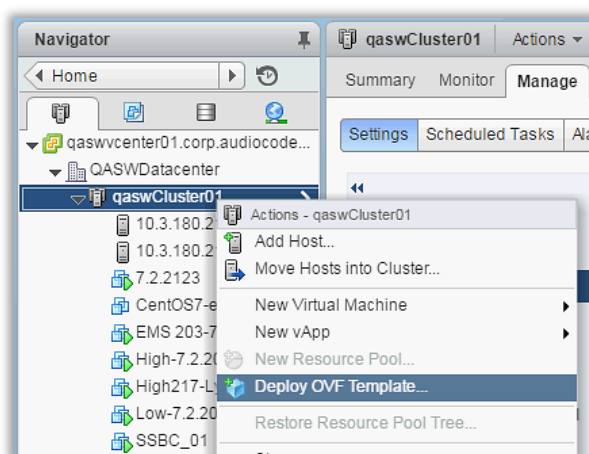
Figure 8-1: VMware vSphere Web Client



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

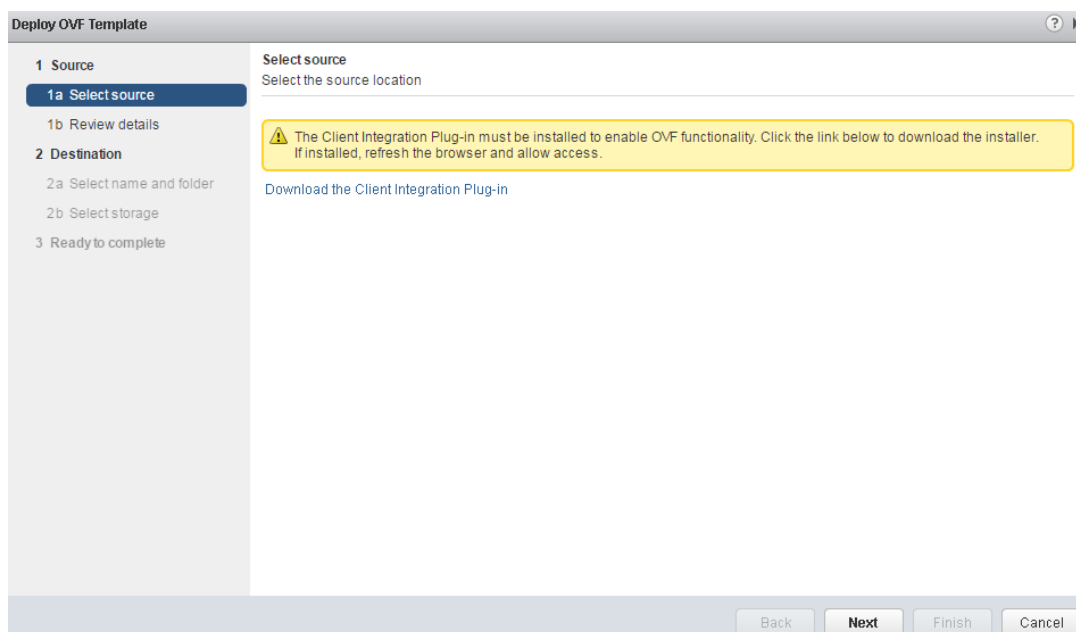
Figure 8-2: Hosts and Clusters



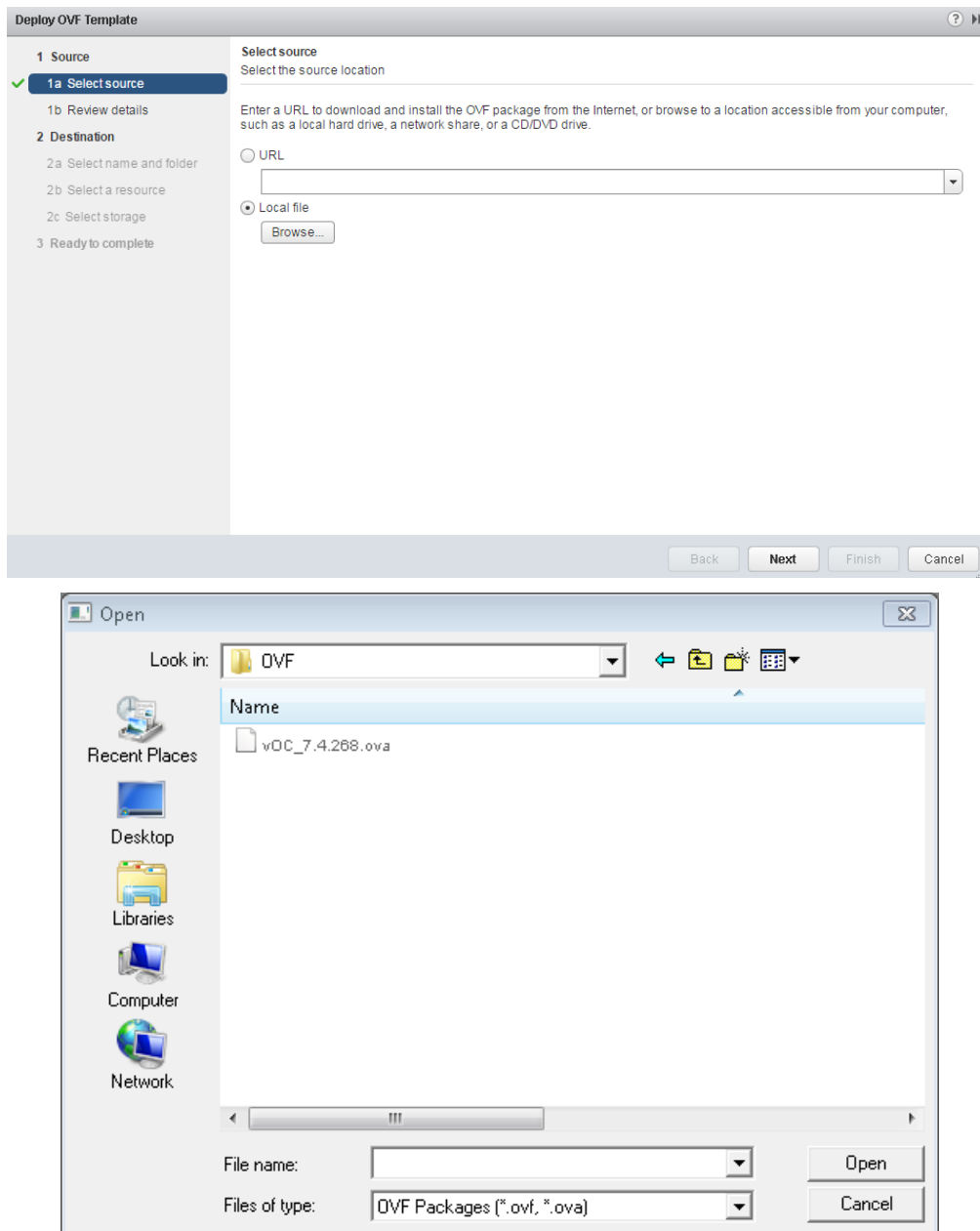
**Figure 8-3: Deploy OVF Template Option**

4. In the Navigator, select the cluster and from the right-click menu, choose **Deploy OVF Template**.

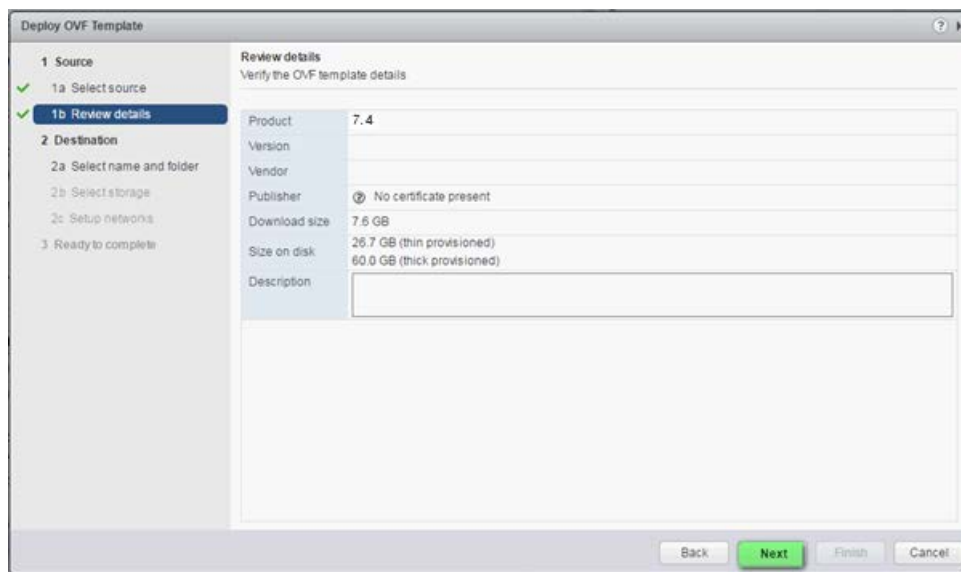
The following screen may be displayed if the Client Integration Plug-in is not installed on your PC. Click the **Download the Client Integration Plug-in** link to download this application to your PC and then install it.

**Figure 8-4: Client Integration Plug-in**

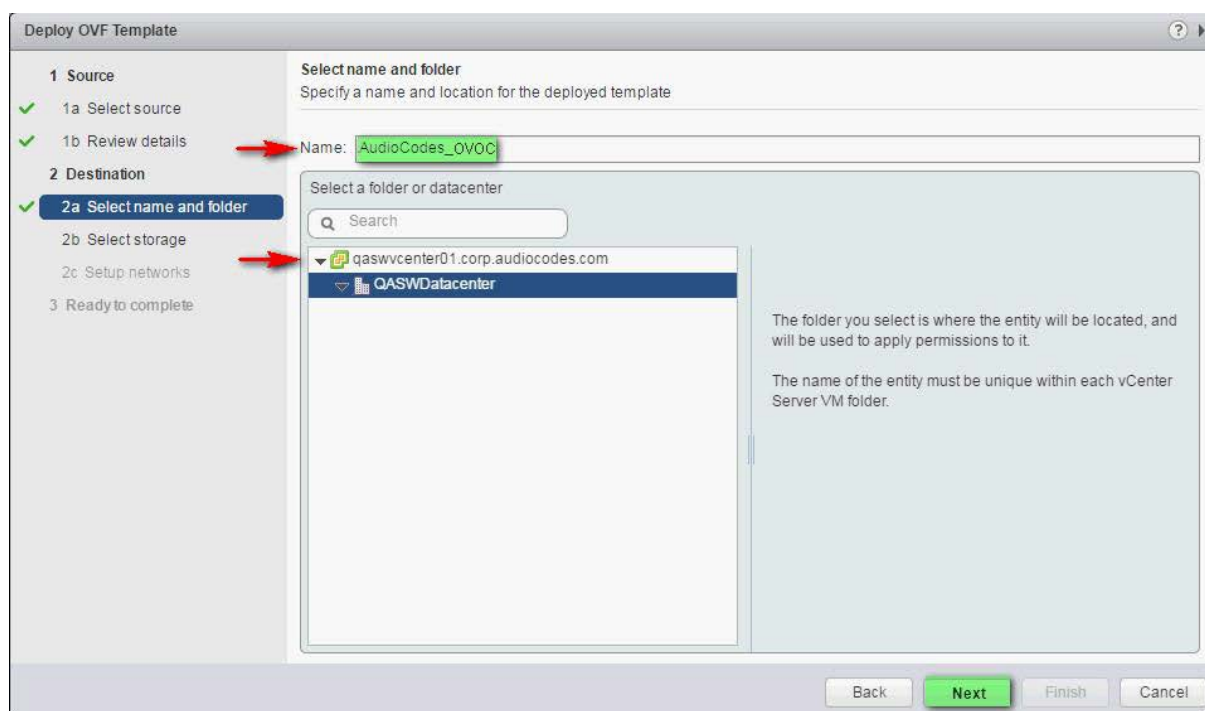
**Figure 8-5: Browse to OVF Package**



5. Browse to the OVF file with extension OVA that you saved to your PC, and click **Next**.

**Figure 8-6: OVF Template Details Screen**

6. In the OVF Template Details screen, click **Next**.

**Figure 8-7: Virtual Machine Name and Location Screen**

7. In the Name and Location screen, enter the desired virtual machine name and choose the inventory location (the Data Center to locate the machine), and then click **Next**.

**Figure 8-8: Destination Storage Screen**

Select storage  
Select location to store the files for the deployed template

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Storage DRS
Netapp04.lun2	3.00 TB	3.58 TB	1.55 TB	VMFS	
Netapp04.lun1	1.50 TB	1.70 TB	840.06 GB	VMFS	
datastore211	1.08 TB	310.22 GB	808.19 GB	VMFS	

Back Next Finish Cancel

8. In the Storage screen, do the following:
  - Select Virtual Disk Format- choose the desired provisioning option ('Thin Provisioning' is recommended),
  - Select the data store where wish to locate your machine, and click **Next**.

**Figure 8-9:: Setup Networking Screen**

Setup networks  
Configure the networks the deployed template should use

Source	Destination	Configuration
VM Network 4	VM Network	✓

IP protocol: IPv4 IP allocation: Static - Manual

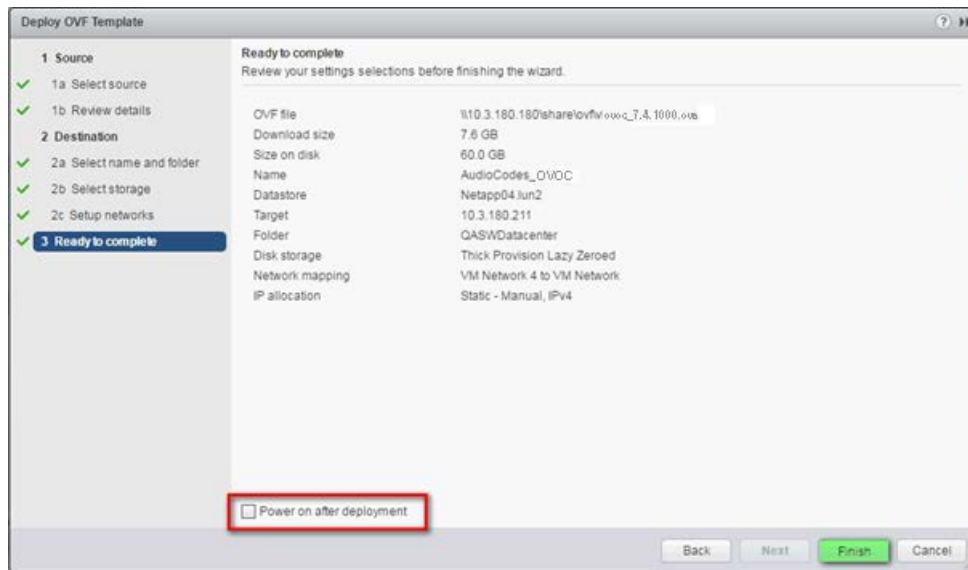
Source: VM Network 4 - Description  
The VM Network 4 network

Destination: VM Network - Protocol settings  
No configuration needed for this network

Back Next Finish Cancel

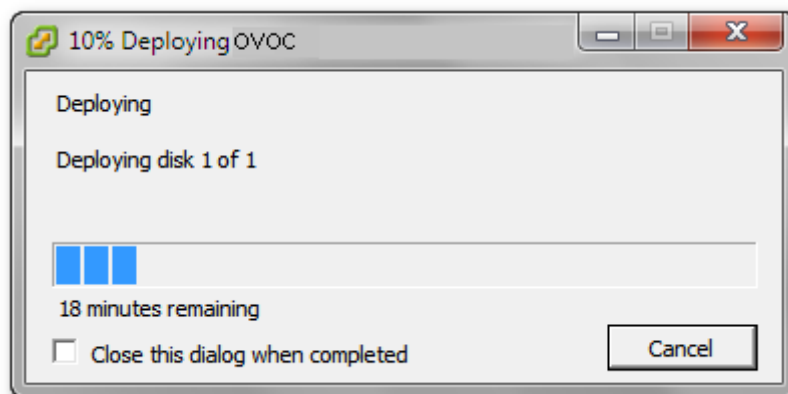
9. In the Network setup screen, select the network where the deployed template should apply, and click **Next**.

**Figure 8-10: Ready to Complete Screen**

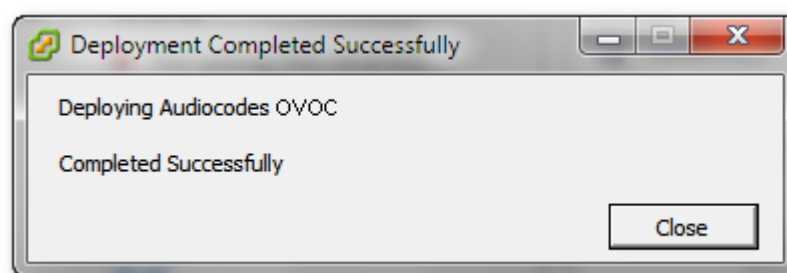


10. In the Ready to Complete screen, ensure the option 'Power on after deployment' is not selected, and click **Finish**.

**Figure 8-11: Deployment Progress Screen**



Recent Tasks			
Name	Target	Status	Requested Start Time
Deploy OVF template	Audiocodes OVOC	14%	21/05/2012 09:32:26



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	

11. Wait until deployment process has completed. This process may take approximately half an hour.



## 8.1.2 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 Chapter 3.

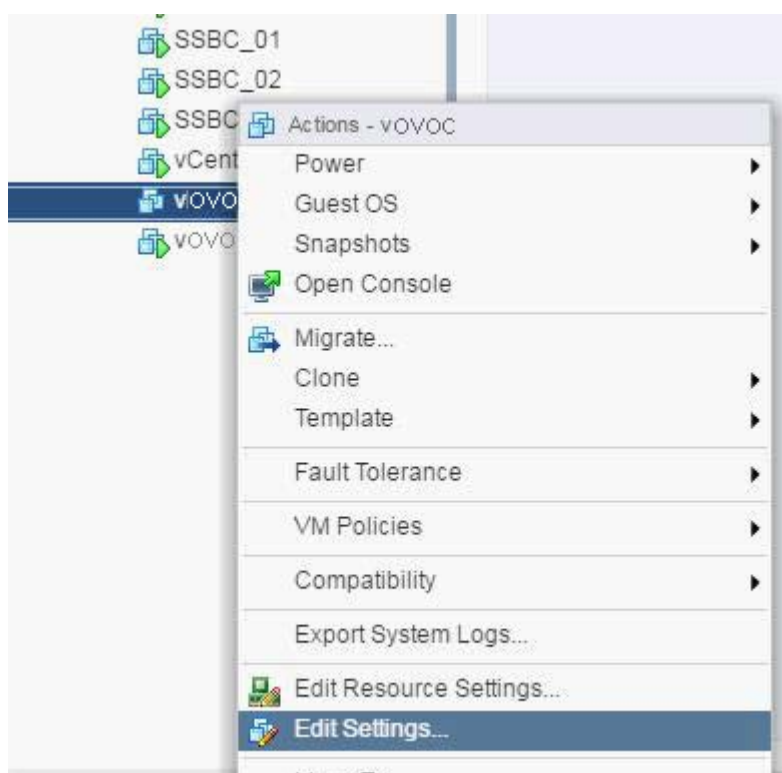
**Table 8-1: Virtual Machine Configuration**

Required Parameter	Value
Disk size	Fill-in-here
Memory size	Fill-in-here
CPU cores	Fill-in-here

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

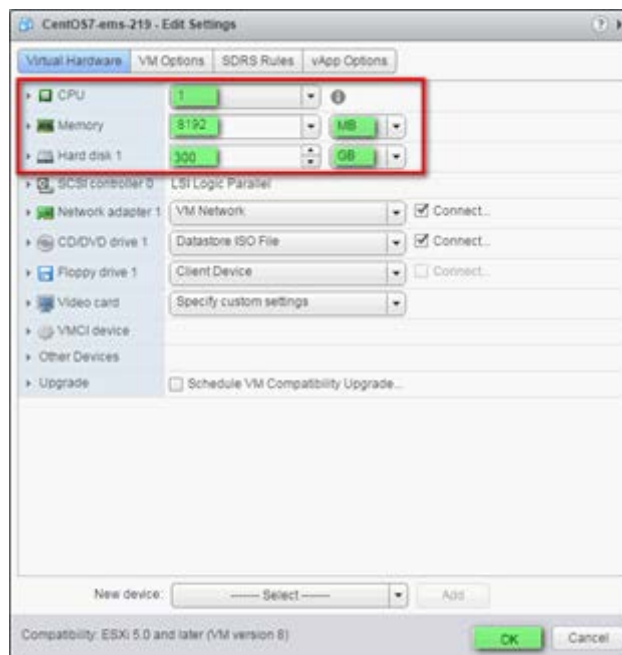
1. Before powering up the machine, go to the virtual machine **Edit Settings** option.

**Figure 8-12: 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. (See Chapter 3), and then click **OK**.

**Figure 8-13: CPU, Memory and Hard Disk Settings**






**Note:**

- 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 (see Section 8.1.4).

3. **Wait** until the machine reconfiguration process has completed.

**Figure 8-14: Recent Tasks**

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

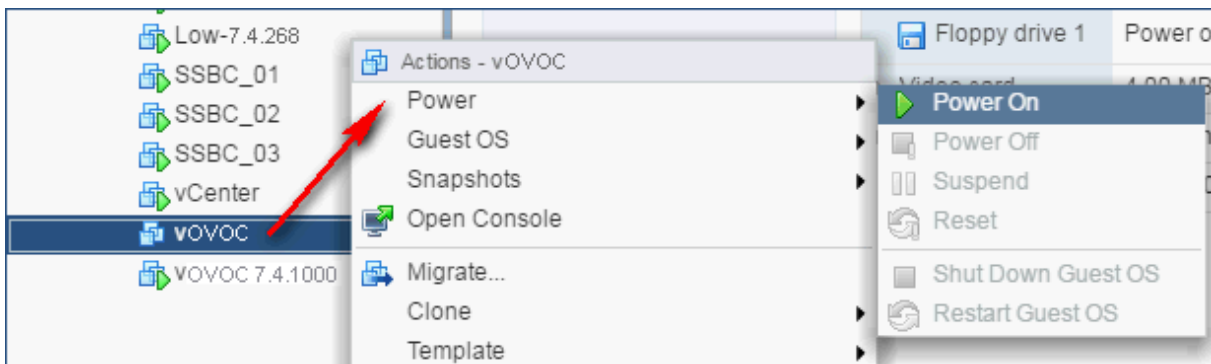
### 8.1.3 Connecting OVOC Server to Network

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

➤ **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 (see Chapter 3).

**Figure 8-15: 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 EMS Server Manager. To run the manager type 'EmsServerManager', and then press Enter.
6. Set the OVOC server network IP address as described in Section 18.1.
7. Perform configuration actions as required using the EMS Server Manager (see Chapter 13).

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

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

### 8.1.4.1 Site Requirements

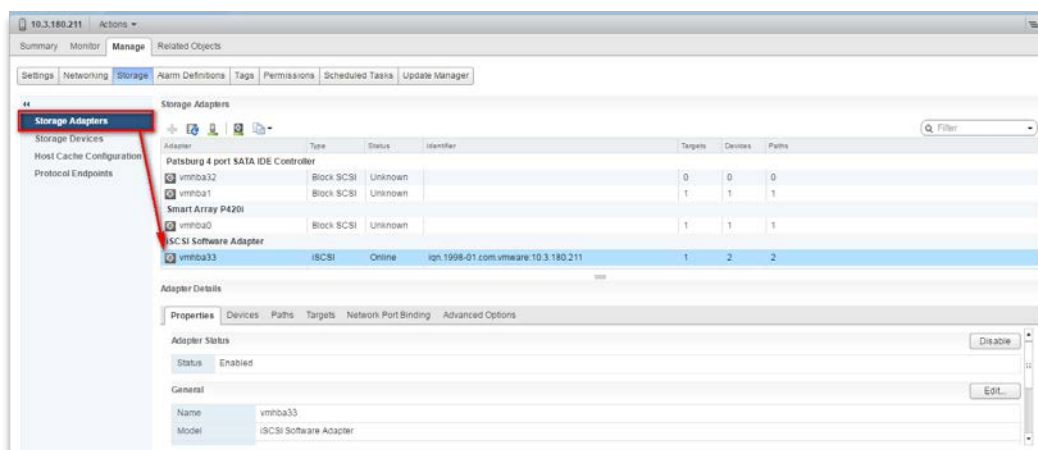
Ensure that your VM cluster site meets the following requirements:

- 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 (see figure below).

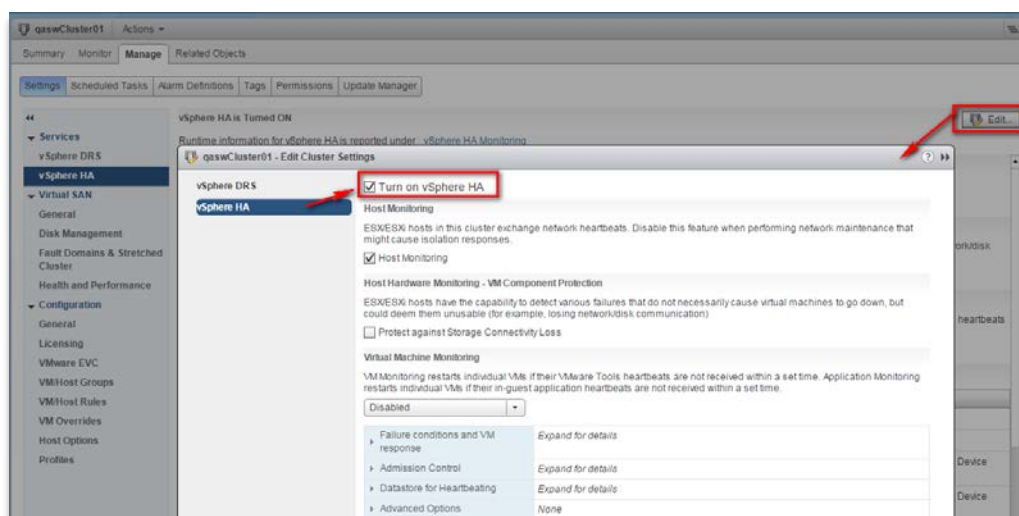
- Verify that Shared Storage is defined and mounted for all cluster members:

**Figure 8-16: Storage Adapters**



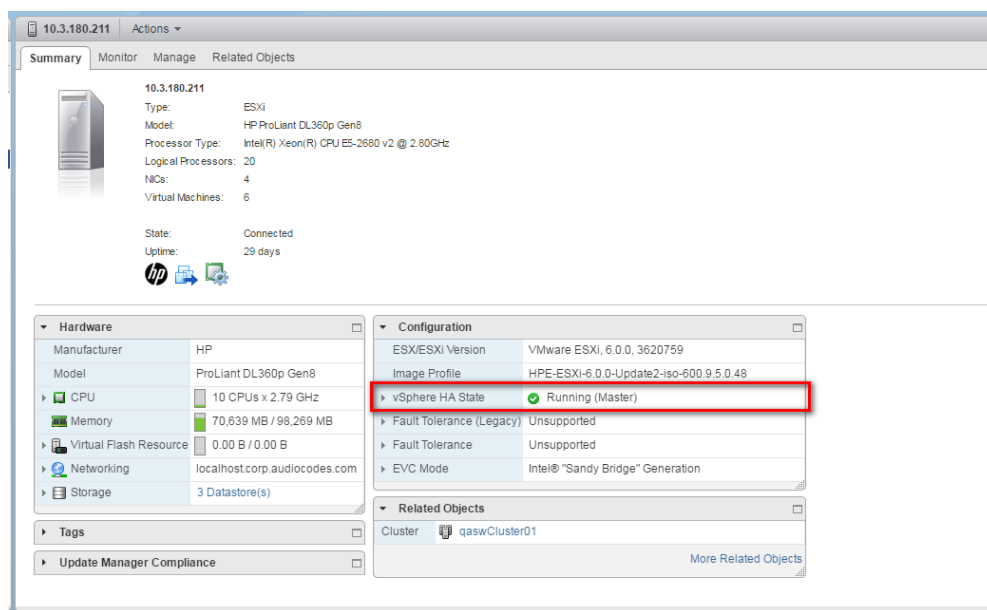
- Ensure that the 'Turn On vSphere HA' check box is selected:

**Figure 8-17: Turn On vSphere HA**



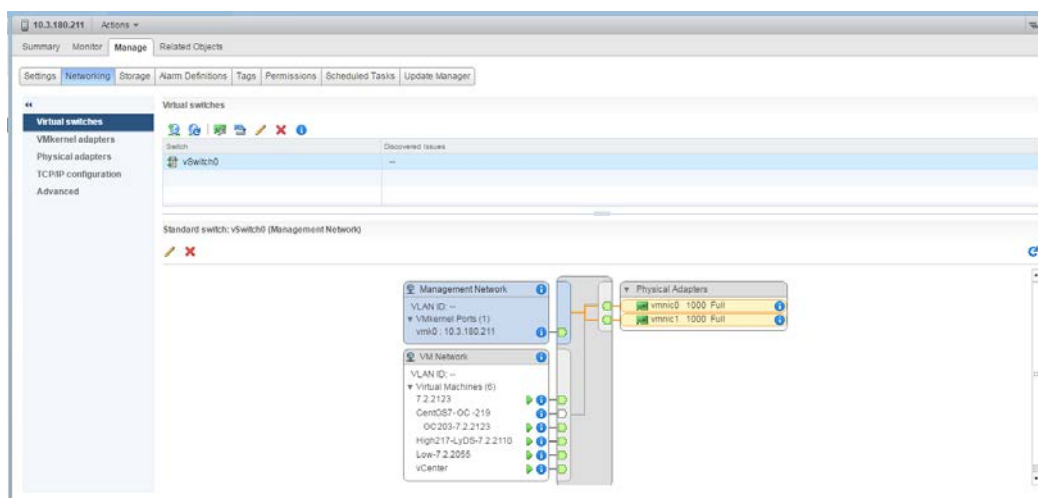
- Ensure that HA is activated on each cluster node:

**Figure 8-18: Activate HA on each Cluster Node**



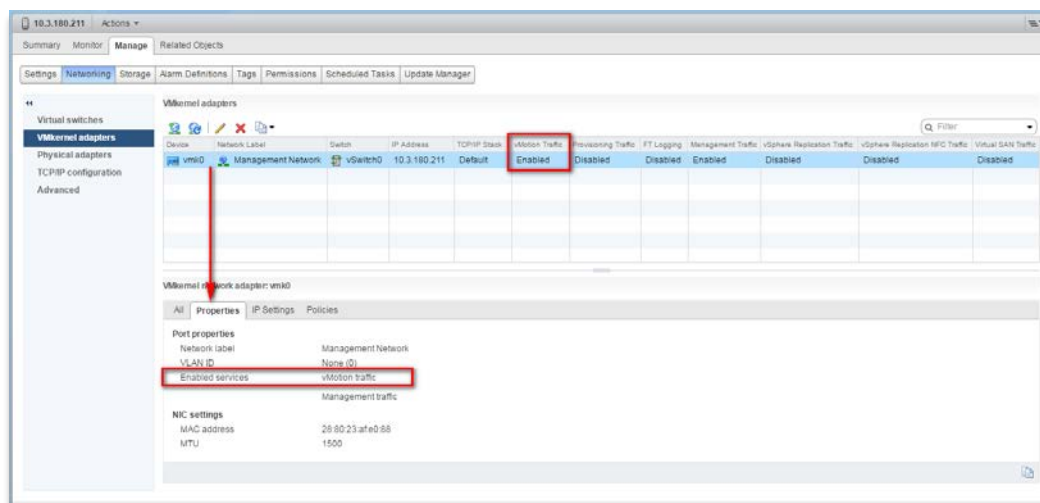
- Ensure that the networking configuration is identical on each cluster node:

**Figure 8-19: Networking**



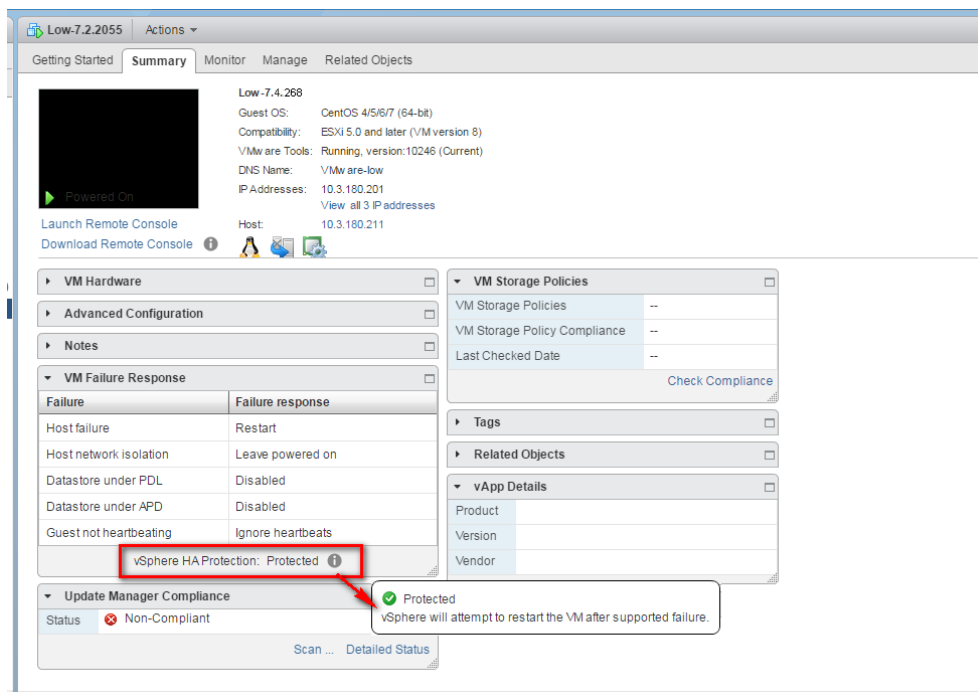
- Ensure that the vMotion is enabled on each cluster node. The recommended method is to use a separate virtual switch for vMotion network (this should be defined in all cluster nodes and interconnected):

Figure 8-20: 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 8-21: Protected VM





**Note:** If you wish to manually migrate the OVOC VMs to another cluster node, see Appendix B.

#### 8.1.4.2 Cluster Host Node Failure

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



**Note:** 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 running OVOC process is dropped. The migration process may take several minutes.

## 8.2 Installing the OVOC Server on Microsoft Hyper-V Platform

This section describes how to install 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.



**Note:** The AudioCodes OVOC supports the Failover Clustering feature in Windows Server 2012 R2 (see Chapter 3).

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

- Install the Virtual Machine (VM) (see Section 8.2.1).
- Configure the Virtual machine hardware settings (see Section 8.2.2).
- Change MAC addresses from 'Dynamic' to 'Static' (see Section 8.2.3).
- Connect OVOC server to network (see Section 8.2.4).
- Configure VMs in a Microsoft Hyper-V cluster (see Section 8.2.5)

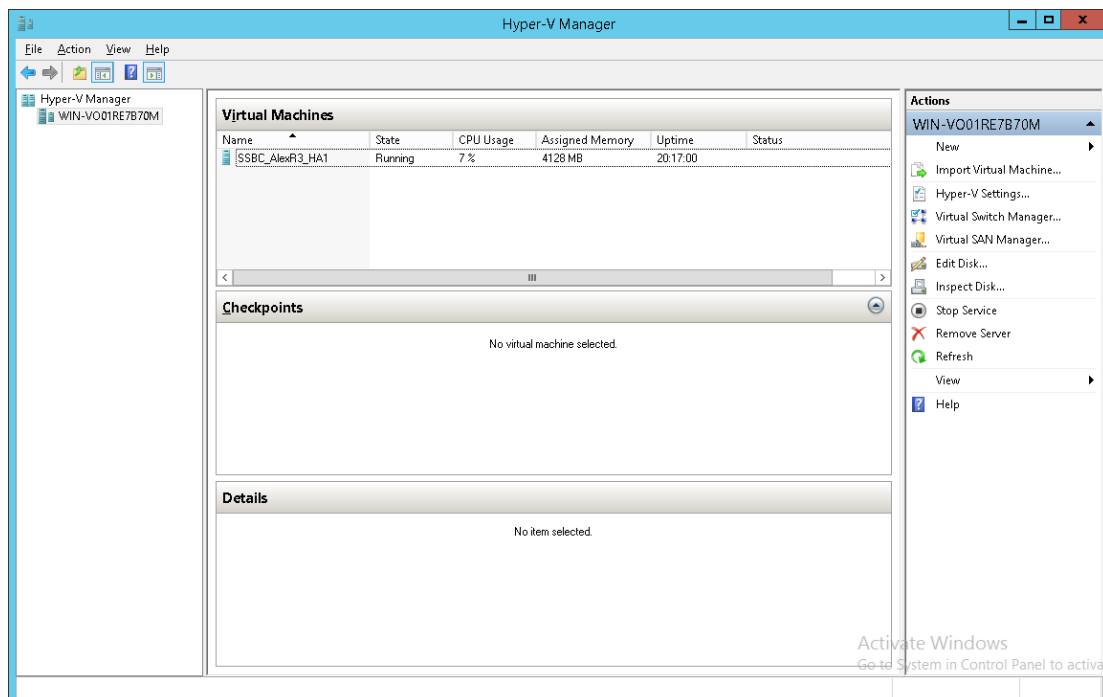
## 8.2.1 Installing the Microsoft Hyper-V Virtual Machine

The Microsoft Hyper-V Virtual Machine installation package is provided on **DVD 5** (see Section 4.2).

➤ **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 D for instructions on how to transfer files).
2. Open Hyper-V Manager by clicking **Start > Administrative Tools > Hyper-V Manager**; the following screen opens:

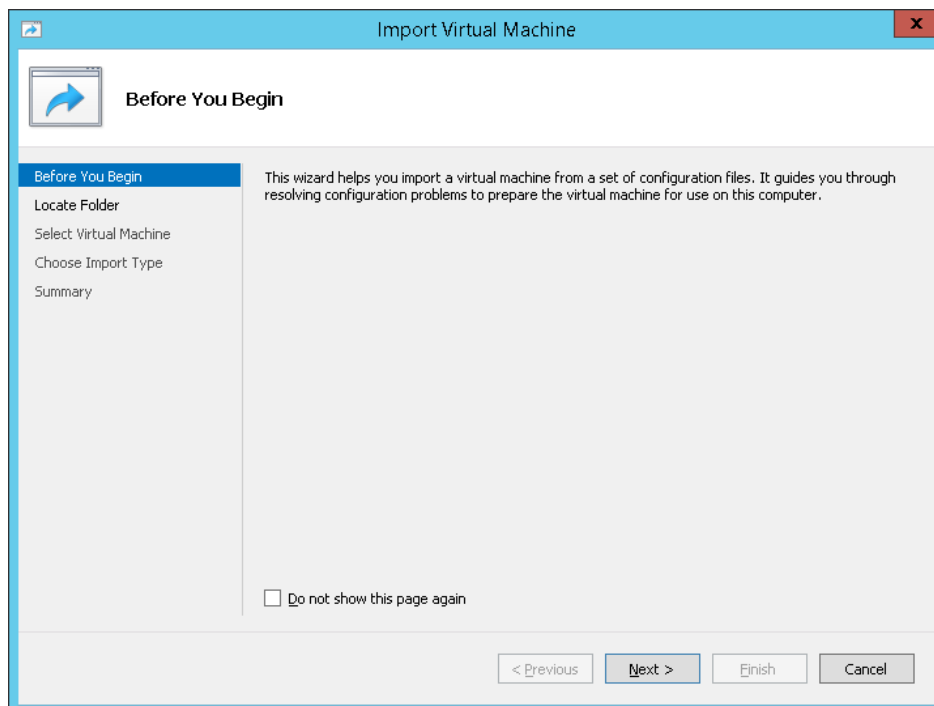
**Figure 8-22: Installing the OVOC server on Hyper-V – Hyper-V Manager**





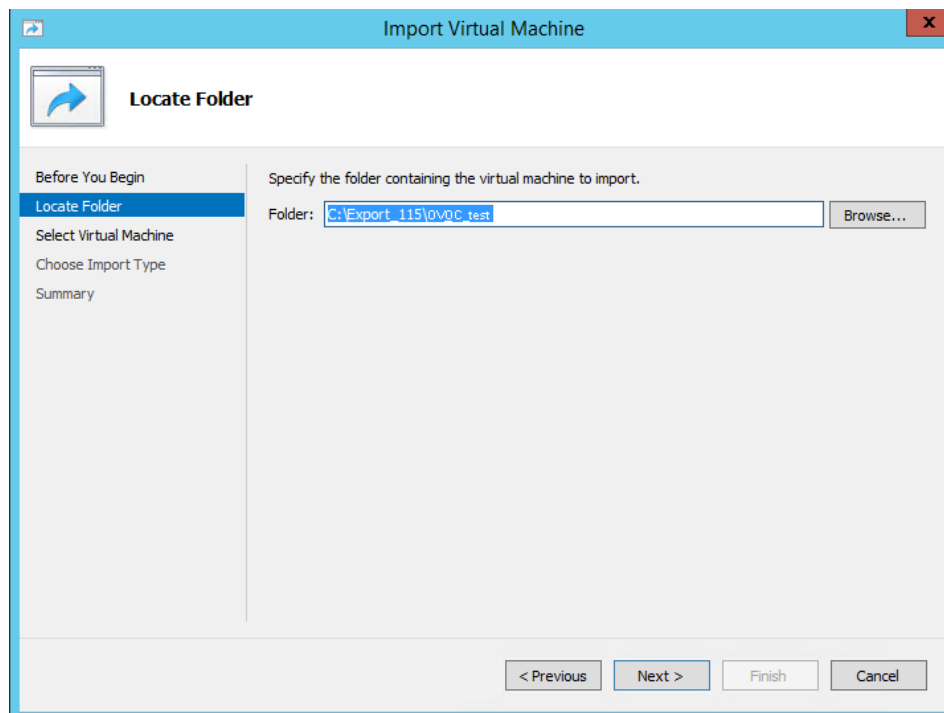
3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

**Figure 8-23: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard**



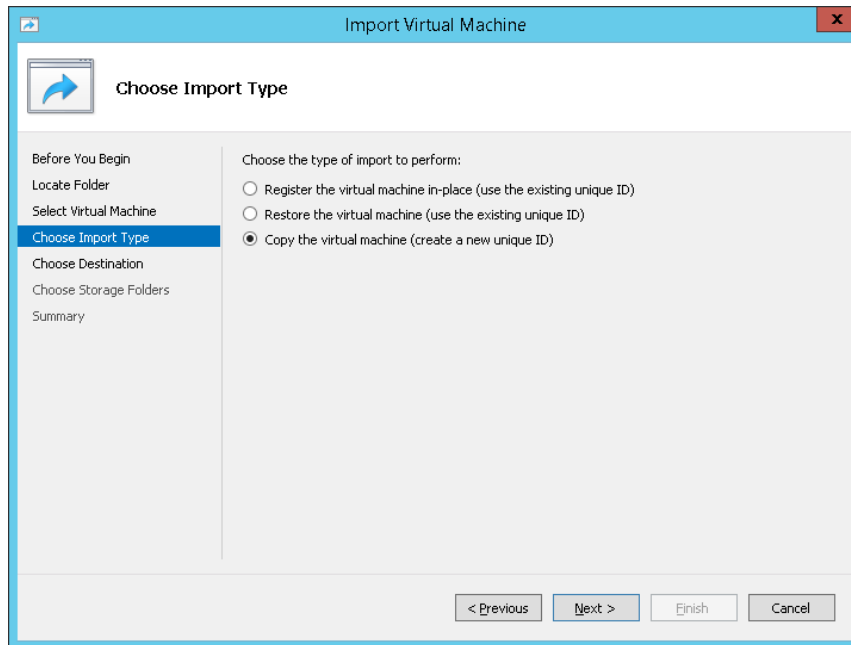
4. Click **Next**; the Locate Folder screen opens:

**Figure 8-24: Installing OVOC server on Hyper-V – Locate Folder**



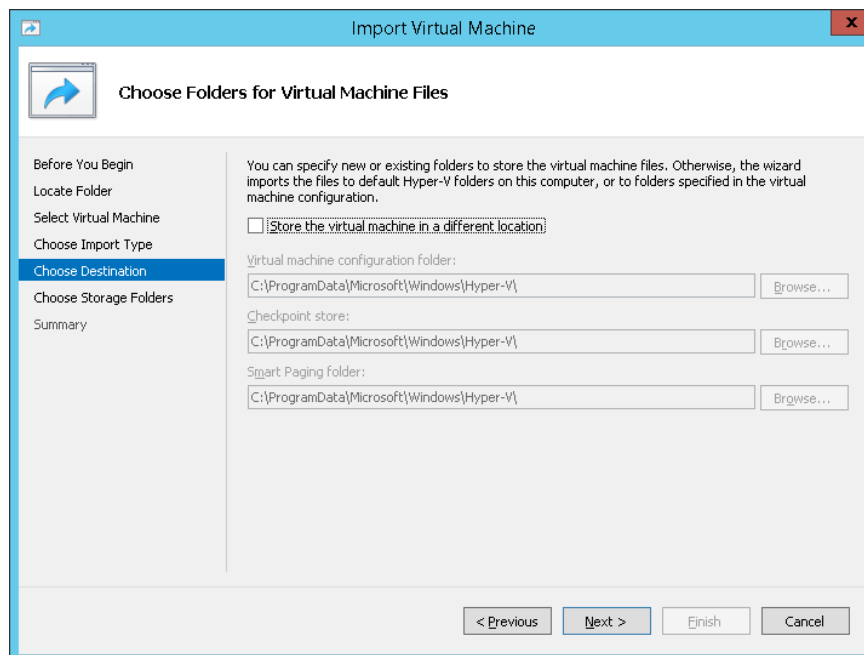
5. Enter the location of the VM installation folder (extracted from the zip file), and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

**Figure 8-25: Installing OVOC server on Hyper-V – Choose Import Type**



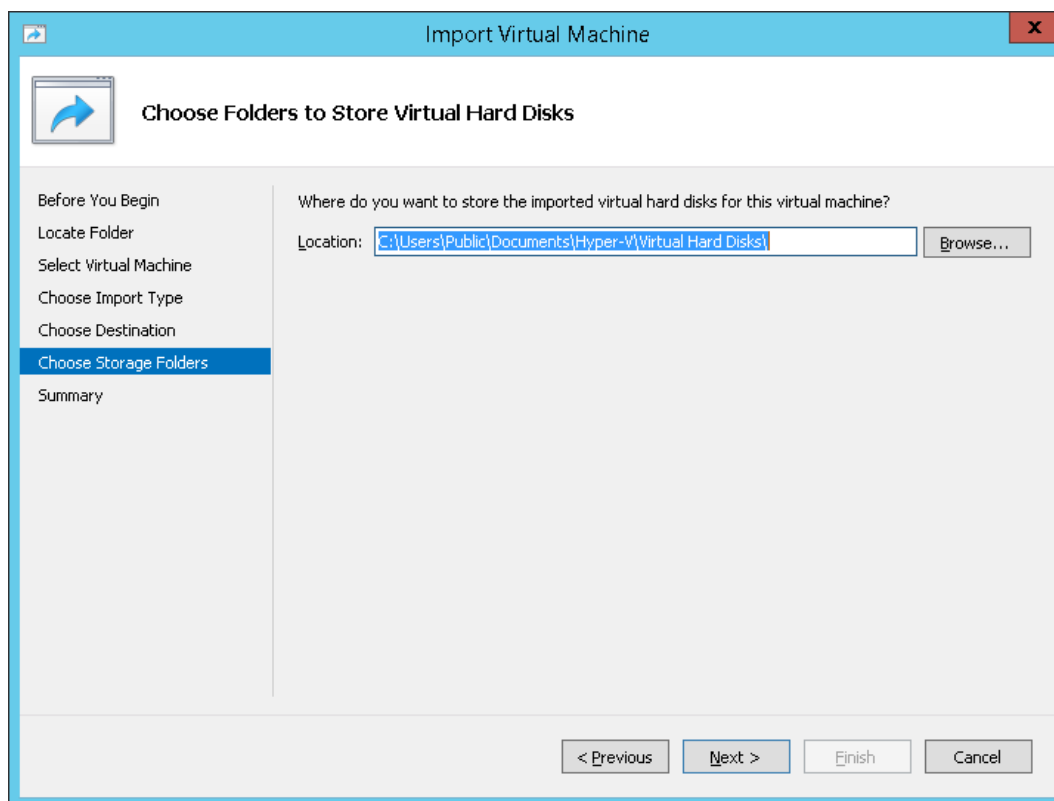
7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

**Figure 8-26: Installing OVOC server on Hyper-V – Choose Destination**



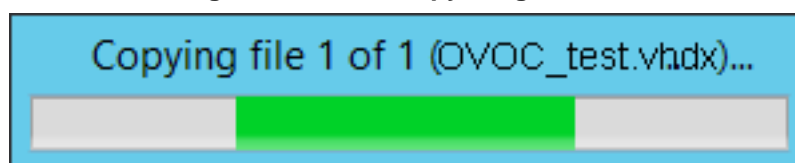
8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

**Figure 8-27: 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 8-28: File Copy Progress Bar**



This step may take approximately 30 minutes to complete.

11. Proceed to Section 8.2.2.

## 8.2.2 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 Chapter 3.

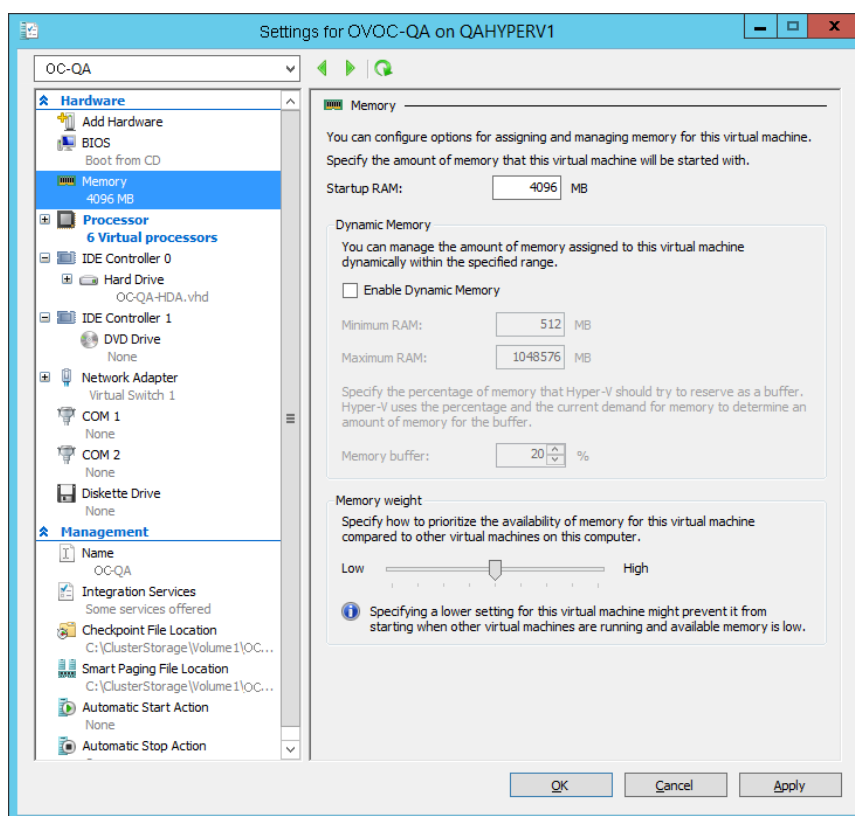
**Table 8-2: Virtual Machine Configuration**

Required Parameter	Value
Disk size	Fillhere
Memory size	Fill-in here
CPU cores	Fill-in here

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

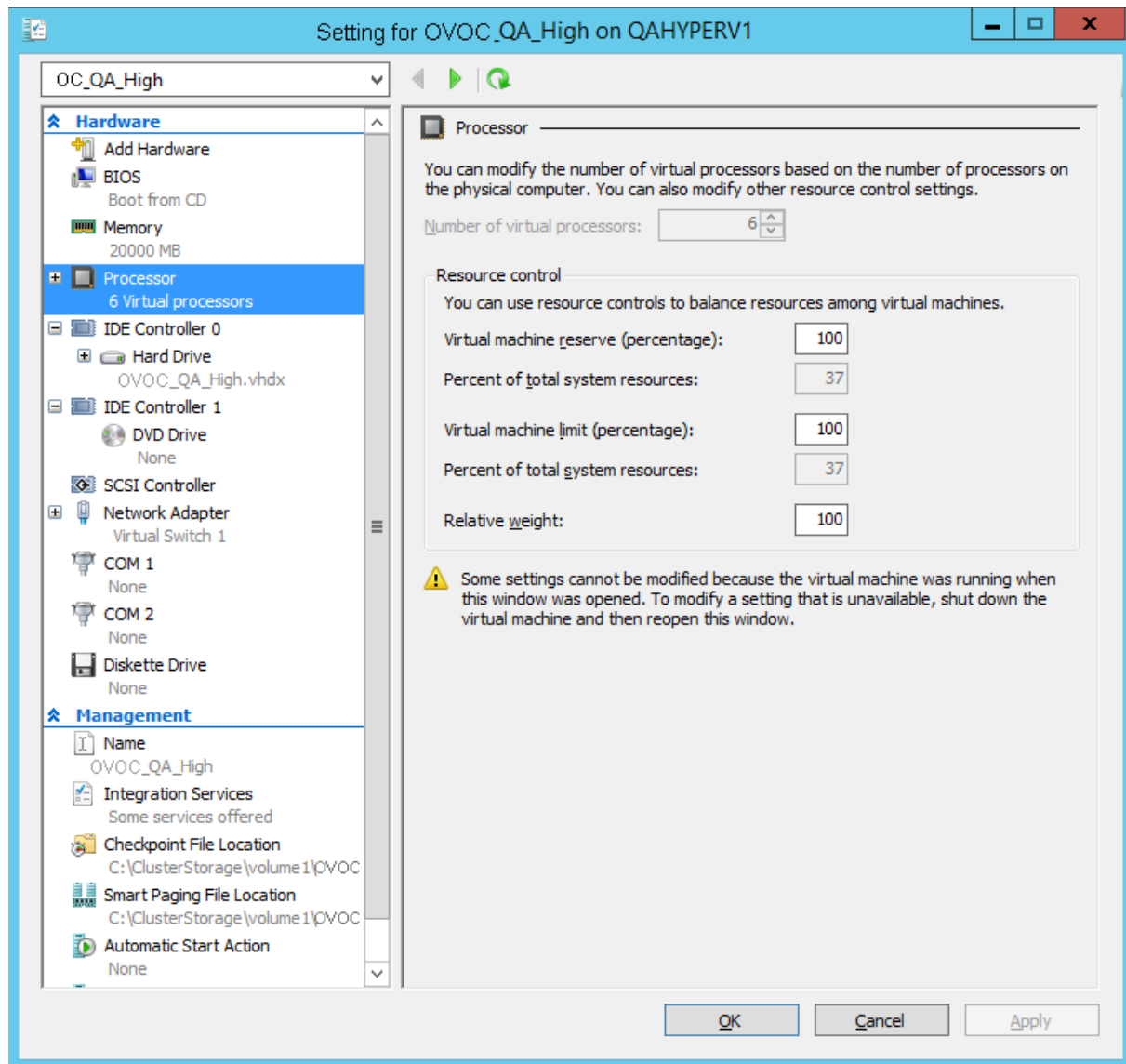
1. Locate the new OVOC server VM in the tree in the Hyper-V Manager, right-click it, and then select **Settings**; the Virtual Machine Settings screen opens:

**Figure 8-29: 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 8-30: 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**.



**Note:**

- 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 (see Section 8.2.5).

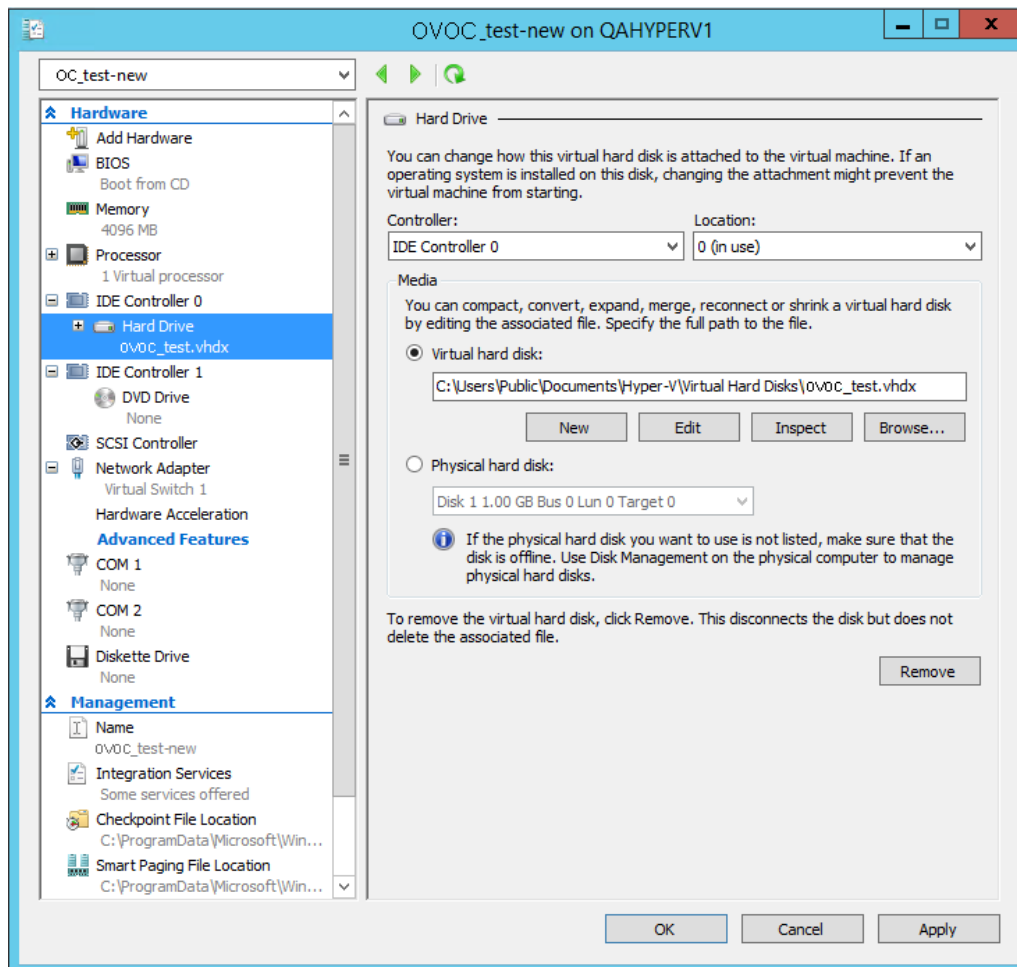
### 8.2.2.1 Expanding Disk Capacity

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:

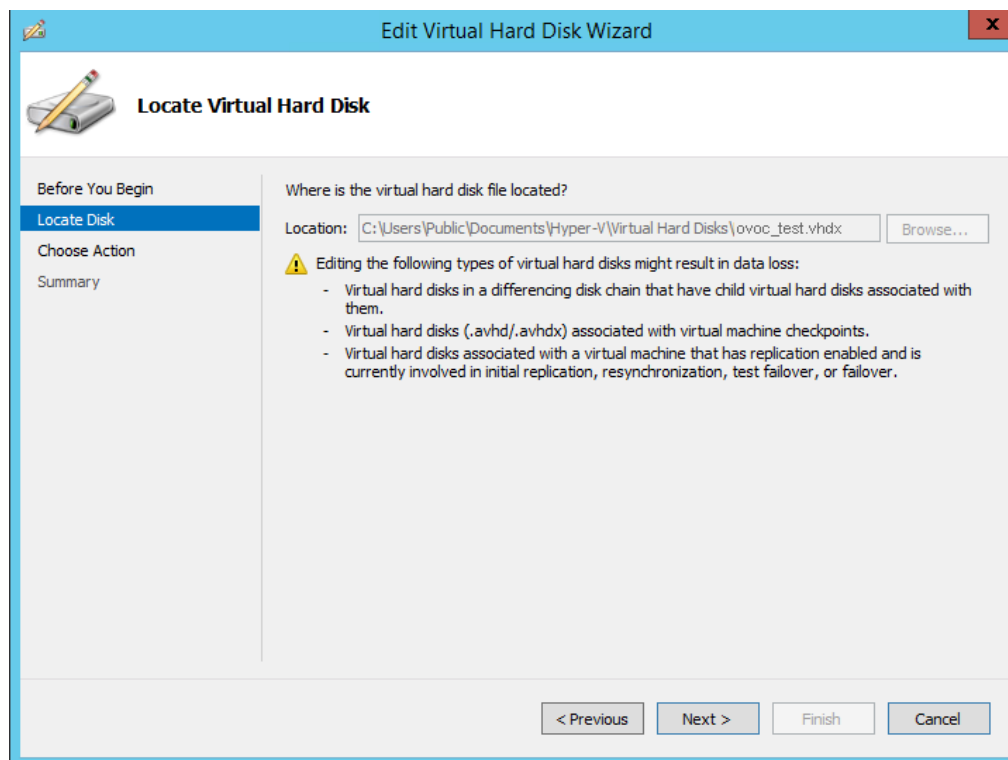
1. Make sure that the target OVOC server VM is not running - Off state.
2. Select the Hard Drive, and then click **Edit**.

**Figure 8-31: Expanding Disk Capacity**



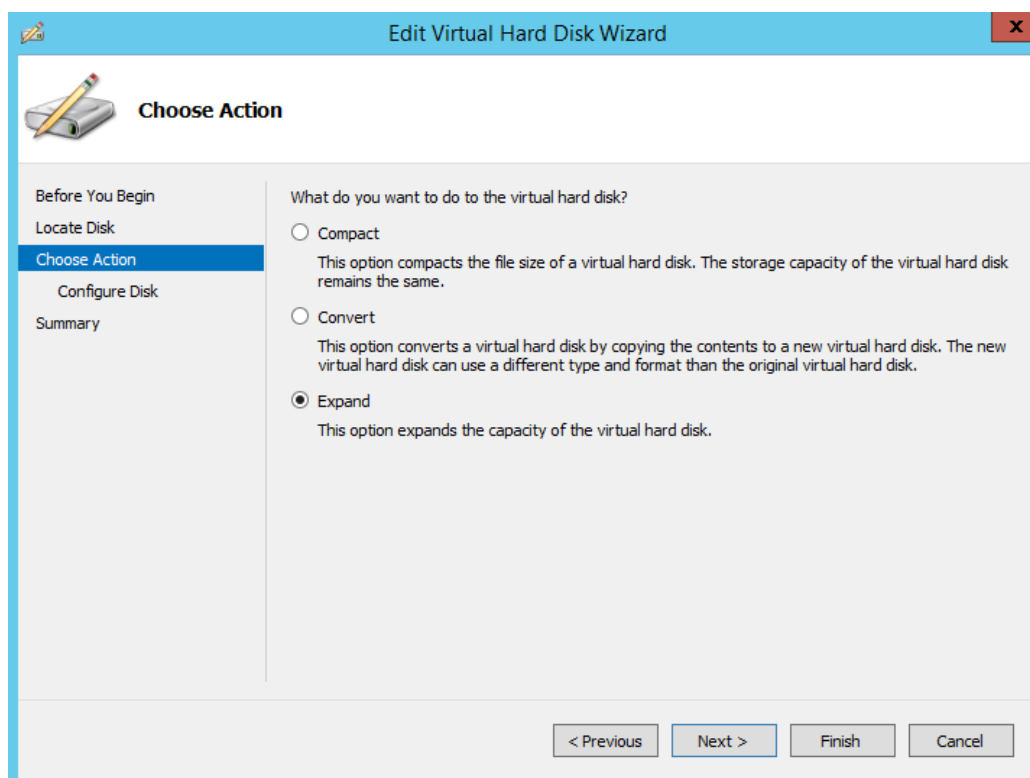
The Edit Virtual Disk Wizard is displayed as shown below.

**Figure 8-32: Edit Virtual Hard Disk Wizard**



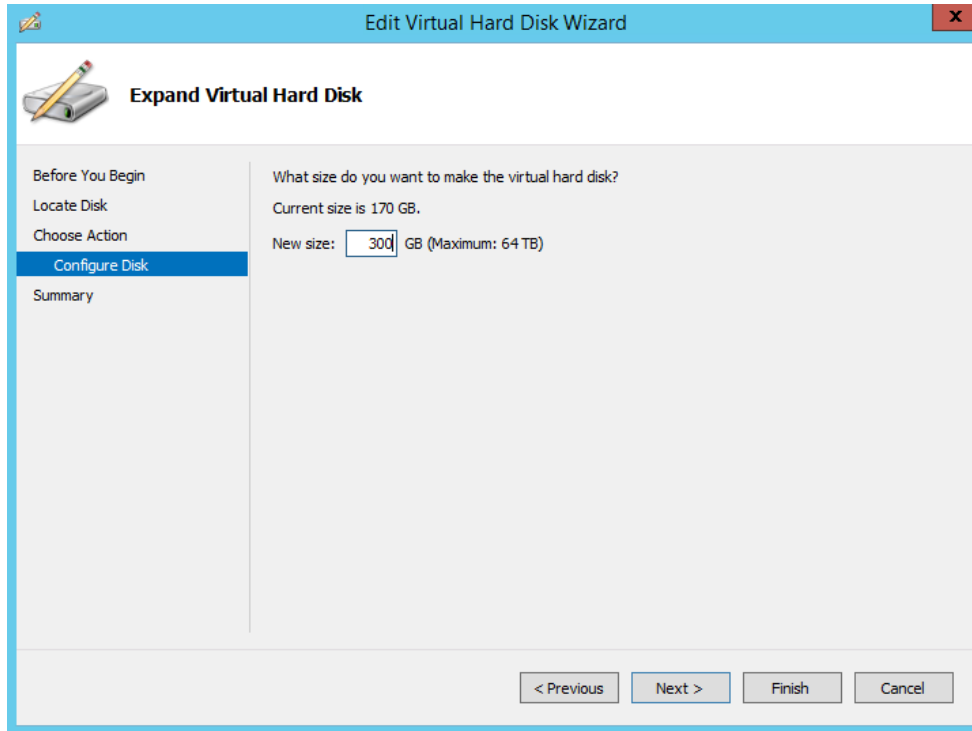
3. Click **Next**; the Choose Action screen is displayed:

**Figure 8-33: Edit Virtual Hard Disk Wizard-Choose Action**



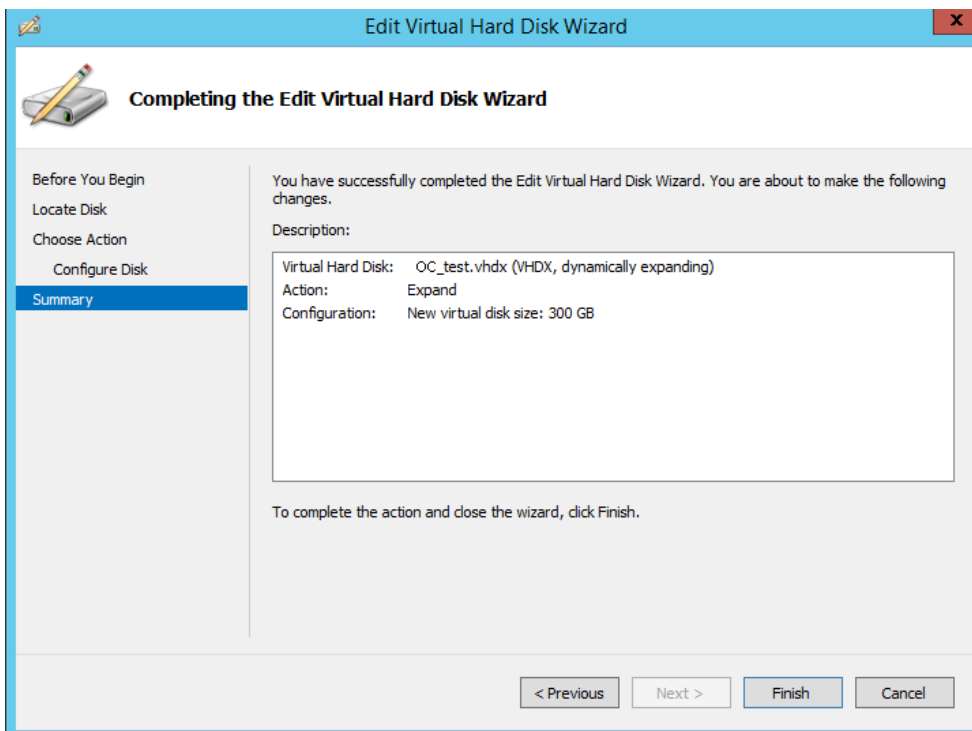
4. Select the **Expand** option, and then click **Next**; the Expand Virtual Hard Disk screen opens.

**Figure 8-34: 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 8-35: 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.

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

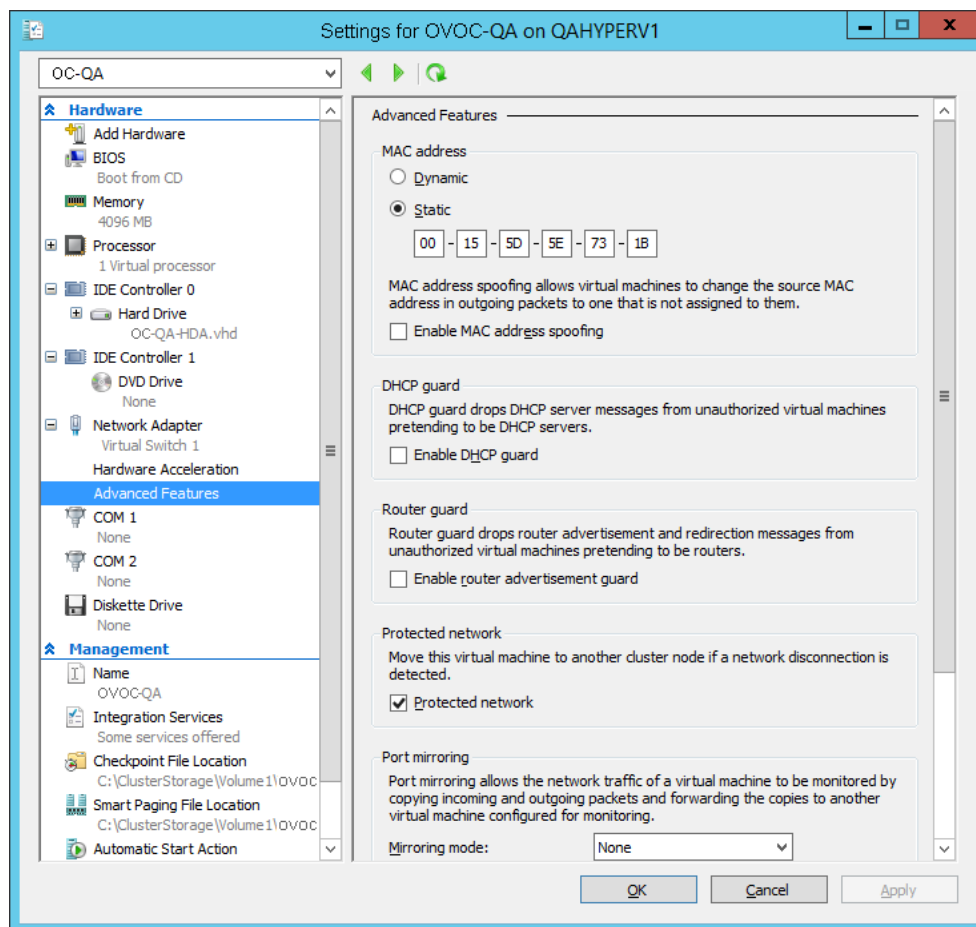
By default, the MAC addresses of the OVOC server Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances, for example, after moving the VM between Hyper-V hosts. Changing the MAC address may lead to an invalid license.

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 (see Section 17.6).
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 8-36: Advanced Features - Network Adapter – Static MAC Address**



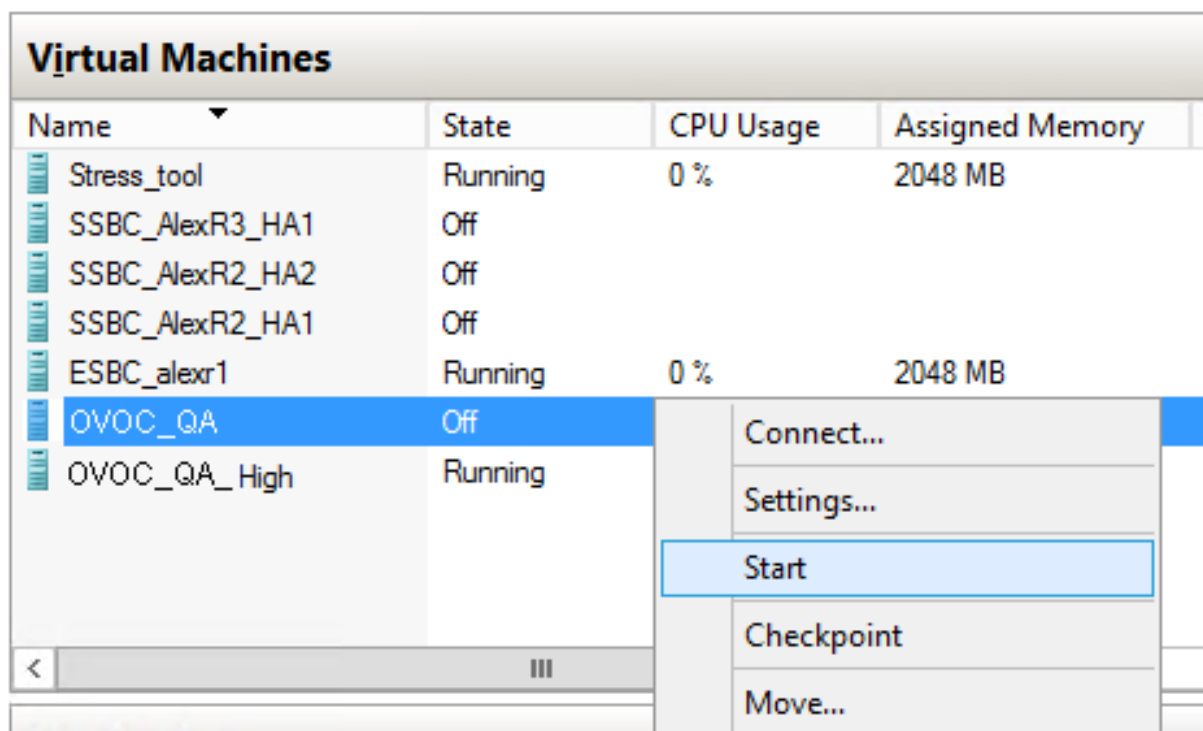
## 8.2.4 Connecting OVOC Server to Network

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.

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

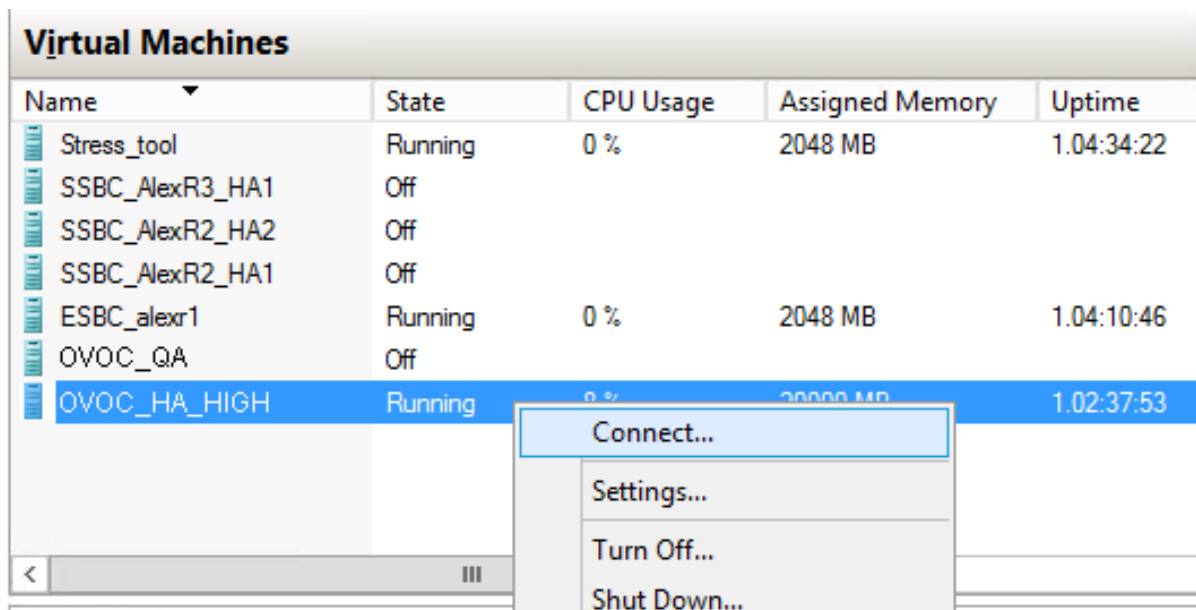
1. Start the OVOC server virtual machine, on the Hyper-V tree, right-click the OVOC server, and then in the drop-down menu, choose **Start**.

**Figure 8-37: 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 8-38: 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 EMS Server Manager utility by specifying the following command:  

```
# EmsServerManager
```
6. Set the OVOC server network IP address to suit your IP addressing scheme (see Section 18.1).
7. Perform other configuration actions as required using the EMS Server Manager (see Chapter 13).

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

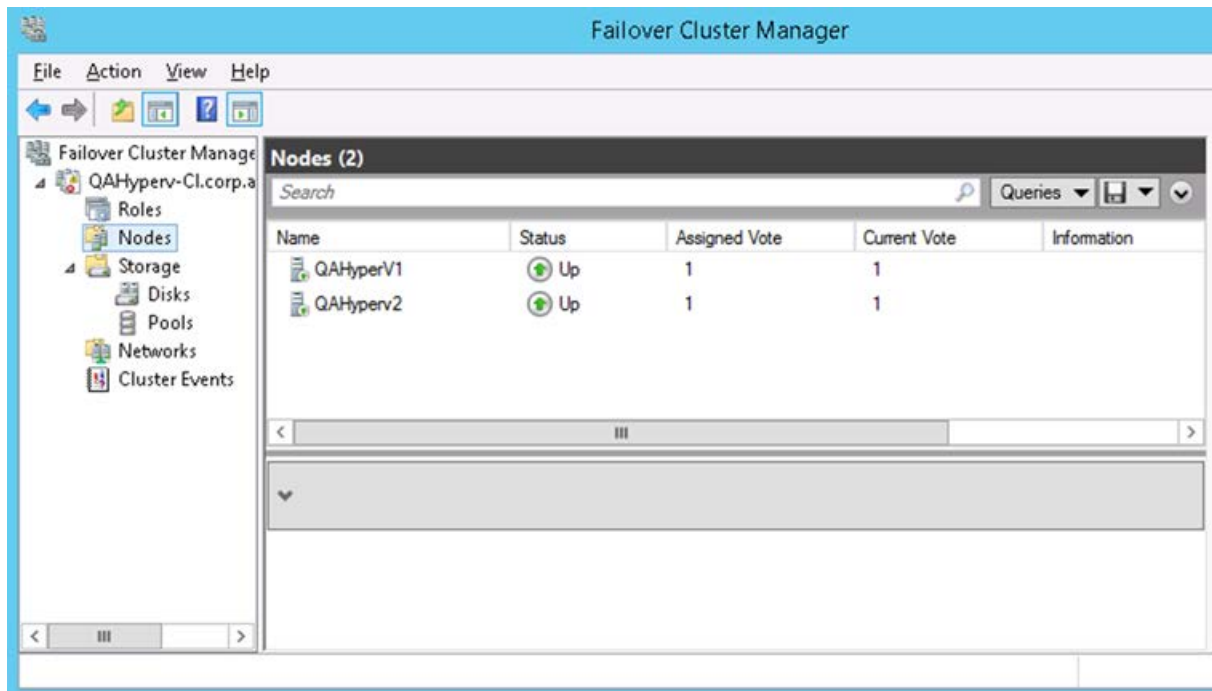
This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

### 8.2.5.1 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 8-39: Hyper-V-Failover Cluster Manager Nodes



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

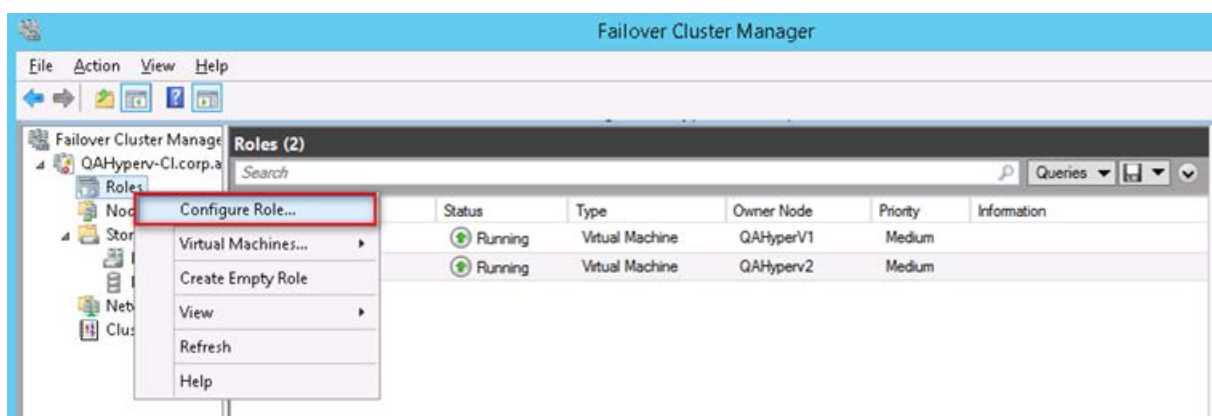
### 8.2.5.2 Add the OVOC VM in Failover Cluster Manager

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

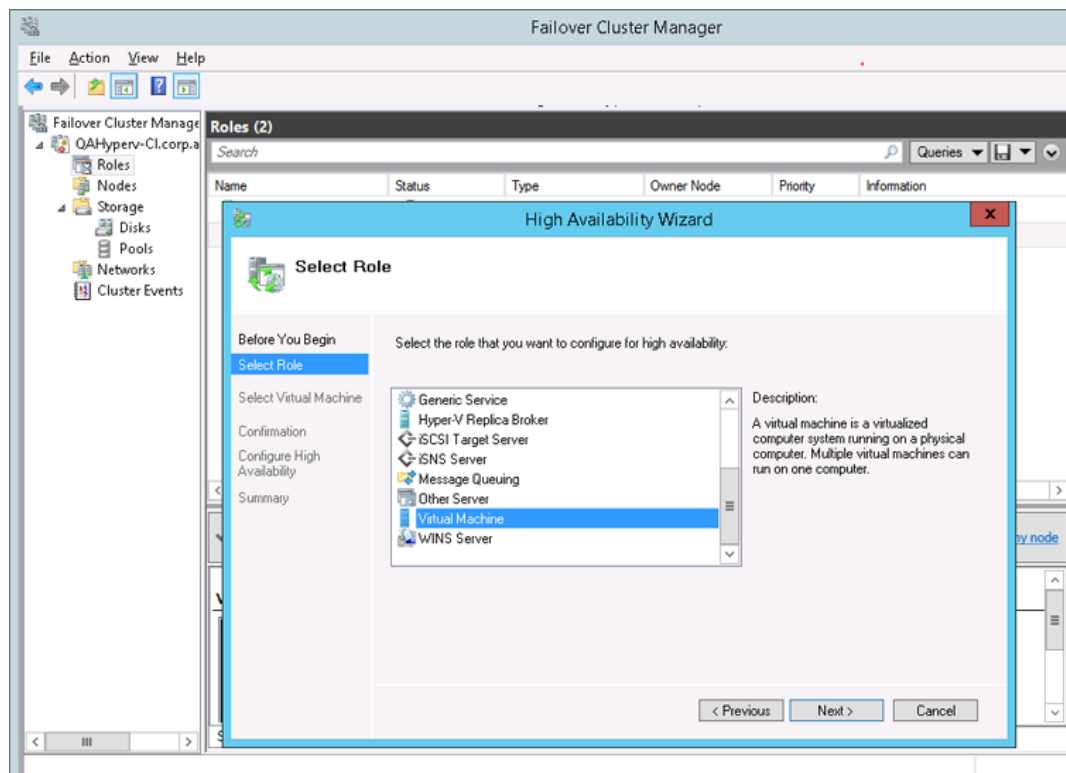
➤ To add the OVOC VM in Failover Cluster Manager:

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

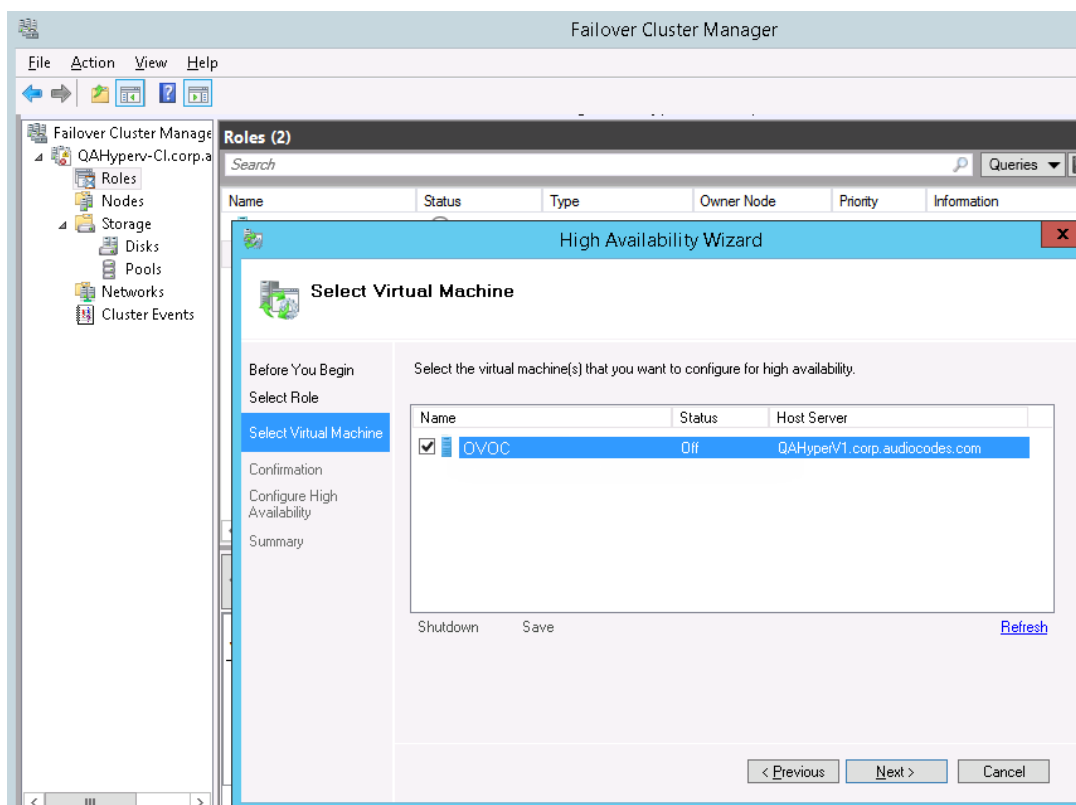
Figure 8-40: Configure Role



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

**Figure 8-41: Choose Virtual Machine**

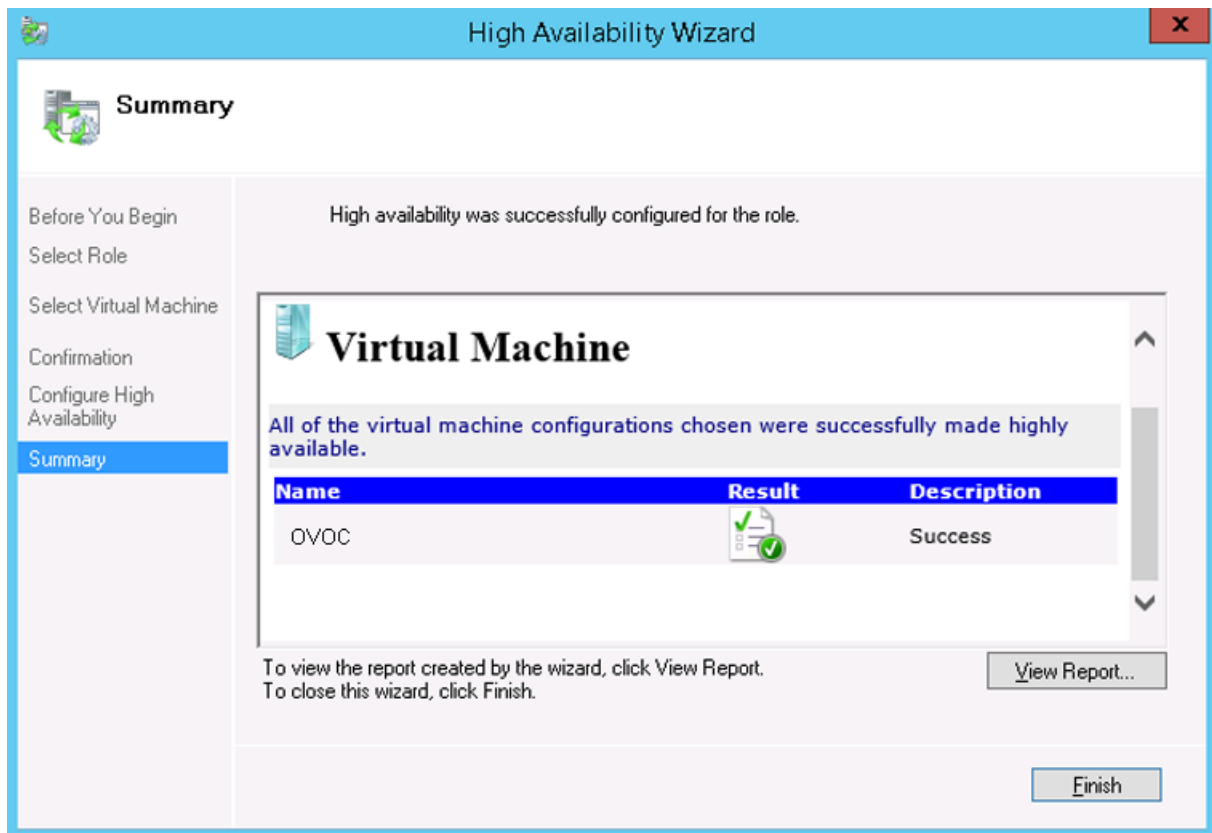
A list of available VMs are displayed; you should find the your new created OVOC VM:

**Figure 8-42: Confirm Virtual Machine**

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

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

**Figure 8-43: Virtual Machine Successfully Added**



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

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



**Note:** If you wish to manually move the OVOC VMs to another cluster node, see Appendix B.

### 8.2.5.3 Cluster Host Node Failure

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



**Note:** 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.

# Part III

## OVOC Server Upgrade

This part describes the upgrade of the OVOC server on dedicated hardware and on the VMware platform.





## 9 Upgrading the OVOC Server on Dedicated Hardware

This section describes the upgrade of the OVOC server on dedicated hardware.



### Important:

- Prior to performing the upgrade, it is highly recommended to perform a complete backup of the OVOC server (see Chapter 11).
- This upgrade is supported from Version 7.4 and later. If you are upgrading from Version 7.2.3000, you can optionally migrate topology to Version 7.4 (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center Version 7.4*).

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

### 9.1 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 on the Linux platform to version 7.4, only DVD3 is required. Verify in the EMS Manager 'General Info' screen that you have installed the latest Linux revision (see Chapter 3 on page 23). If you have an older OS revision, a clean installation must be performed using all three DVDs (see Chapter 6).



**Note:** 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 on the Linux platform:

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:

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

5. Run the installation script from its location:

```
./install
```

Figure 9-1: 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 (M
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 9-2: 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 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
ferred 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. 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 [8](#).



**Note:** After the OVOC server has rebooted, repeat steps [2](#) to [6](#).

Figure 9-3: OVOC Server Application Install with Patches

```

Done
>>> Copy Oracle Security Patch
...
>>> Remove Old Oracle Security Patch Files
...
>>> Applying Oracle Security Patch
...

-----
Installing Oracle CPU patch 9655014
-----

NOTE: patch installation may take up to 30 min, so be patient

Oracle patch 9655014 is already installed
>>> ===== ...
>>> Installation Completed, Oracle is Now Secured ...
>>> ===== ...
>>> Remove /tmp/EmsServerInstall ...
EMS-Server17# reboot

```

Figure 9-4: 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 (see Chapter 14.14) and verify login to OVOC Web client is successful.
13. Verify that the Date and Time are set correctly (see Section 19.3 to set the date and time).
14. Set the OVOC server network IP address as described in Section 18.1.
15. Configure other settings as required (see Chapter 13).



**Note:** 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.

## 9.2 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 (see Section 6.1.2).

### ➤ 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 "7.4.xxx" in the filename with the relevant version in two of the following commands.

```
mkdir /ins
cp ~acems/DVD3_OVOC_7.4.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_OVOC_7.4.xxx.iso
/tmp/cd
cd /tmp/cd/EmsServerInstall
```

6. Run the installation script from its location:

```
./install
```

Figure 9-5: 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. Proceed to step 6 in Section 9.1.

# 10 Upgrading OVOC on a Virtual Platform

The upgrade of the OVOC server involves the following steps:

- **Step 1:** Setup the Virtual Machine (see Section 10.1)
- **Step 2:** Run the upgrade script (see Section 10.2)
- **Step 3:** Connect the OVOC server to the network (see Section 10.3)

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



## Important:

- Prior to performing the upgrade, it is highly recommended to perform a complete backup of the OVOC server (see Chapter 11).
- This upgrade is supported from Version 7.4 and later. If you are upgrading from Version 7.2.3000, you can optionally migrate topology to Version 7.4 (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center Version 7.4*).

## 10.1 Step 1: Setup the Virtual Machine

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

### 10.1.1 VMware Platform

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.



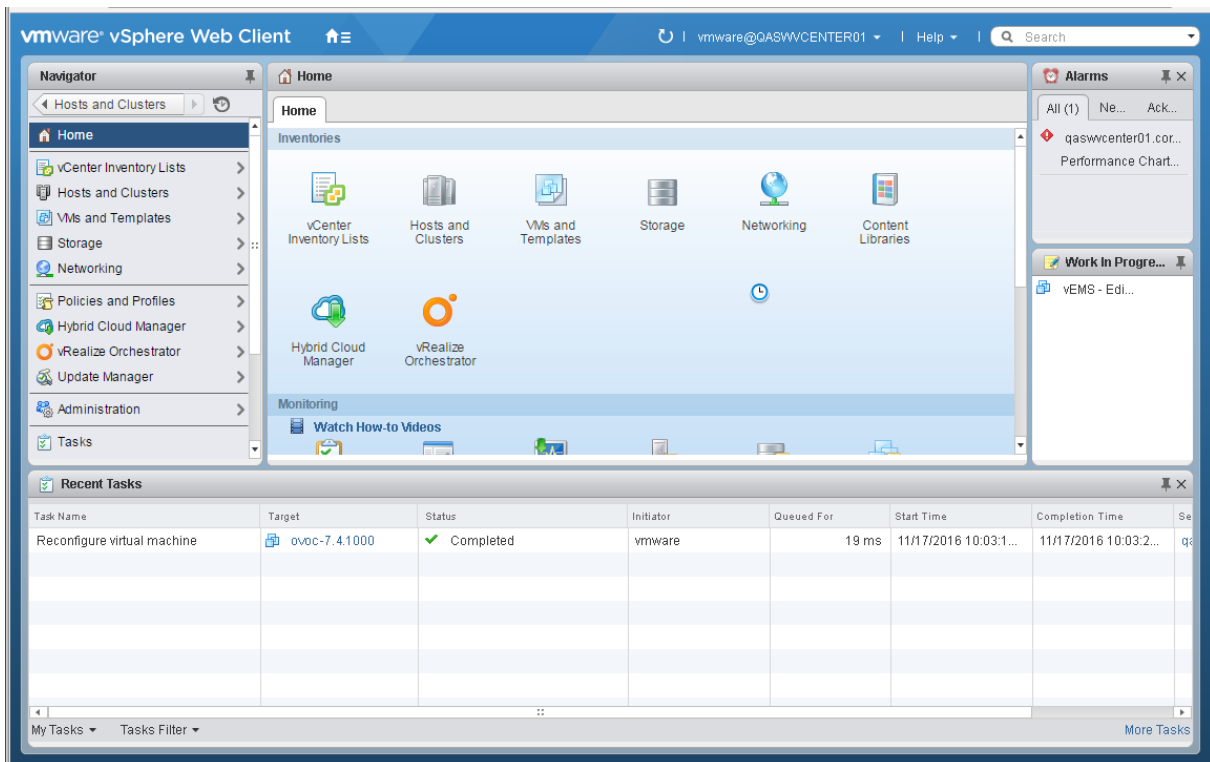
## Note:

- 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:

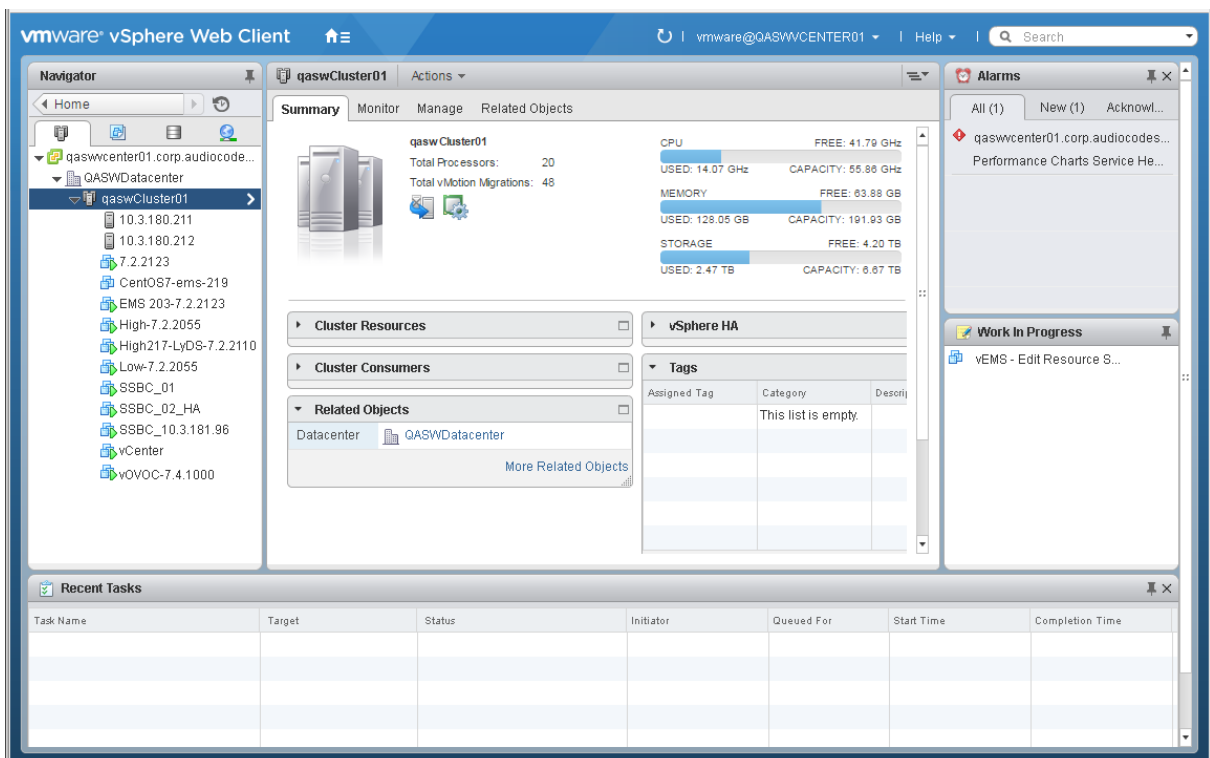
1. Transfer the OVA file containing the VMware Virtual Machine installation package from **DVD3-OVOC Server Application Installation** to your PC (see Appendix D for instructions on how to transfer files).
2. Login to the VMware vSphere Web client.

Figure 10-1: VMware vSphere Web Client



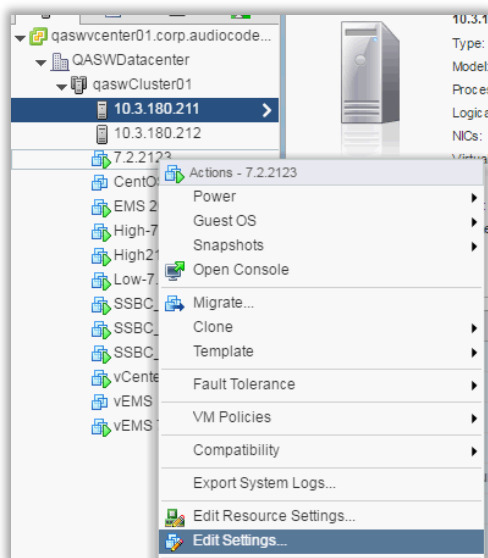
3. In the vCenter Navigator, select **Hosts and Clusters**. A list of Hosts and Clusters is displayed.

Figure 10-2: Hosts and Clusters



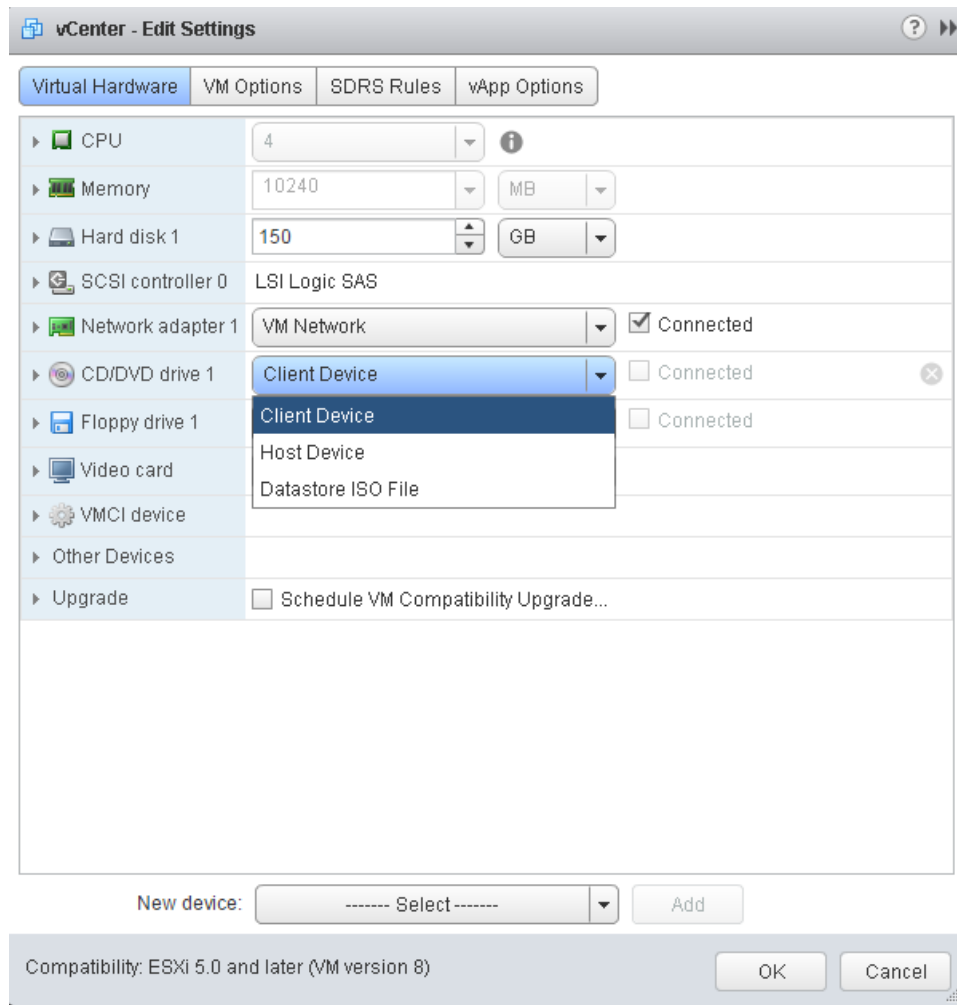
4. Right-click the AudioCodes OVOC node that you wish to upgrade and choose the **Edit Settings** option.

**Figure 10-3: Edit Settings Option**



The vCenter Edit Settings screen is displayed.

**Figure 10-4: 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 (see Section 10.1.1.1).
  - **Host Device:** This option enables you to run the upgrade from the CD/DVD drive of the VMware server host (see Section 10.1.1.2).
  - **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 (see Section 10.1.1.2).



### 10.1.1.1 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.



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

**Figure 10-5: Help Link to Launch Remote Console**

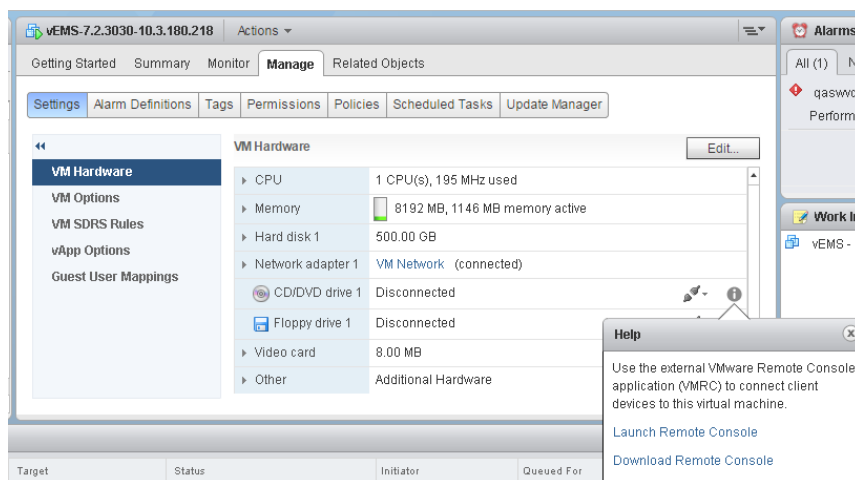
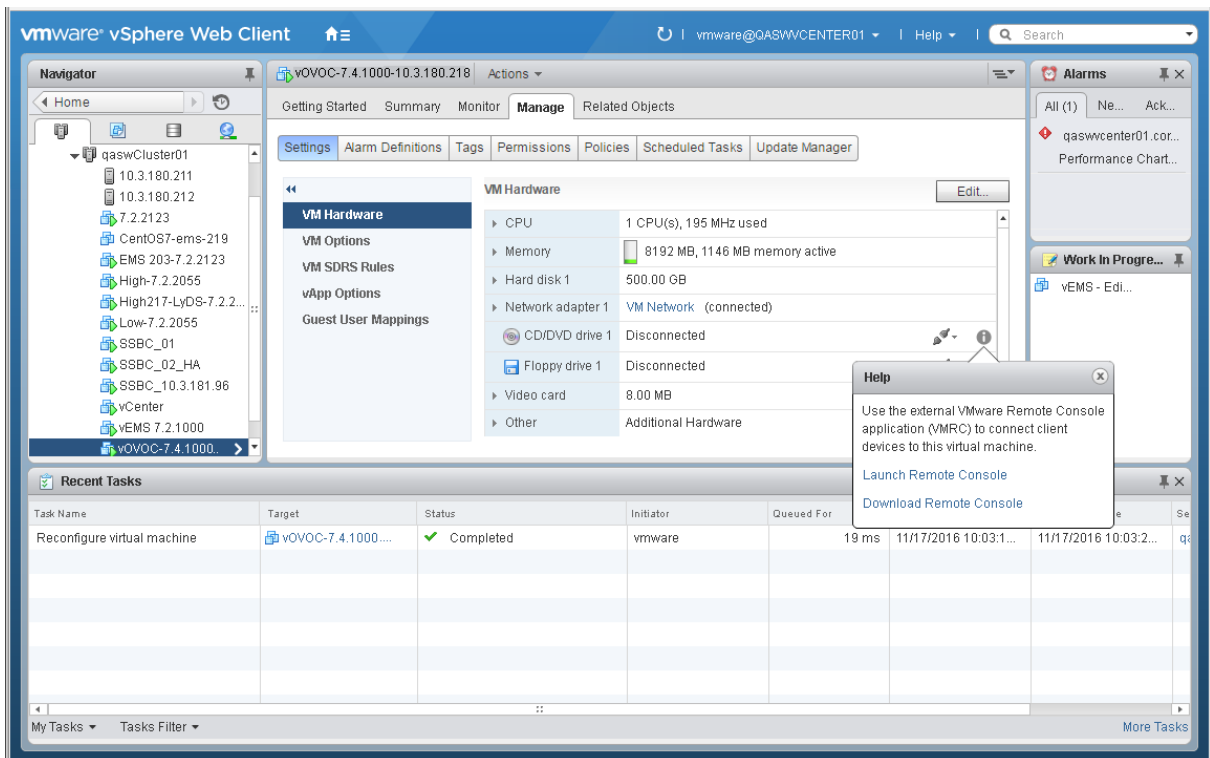
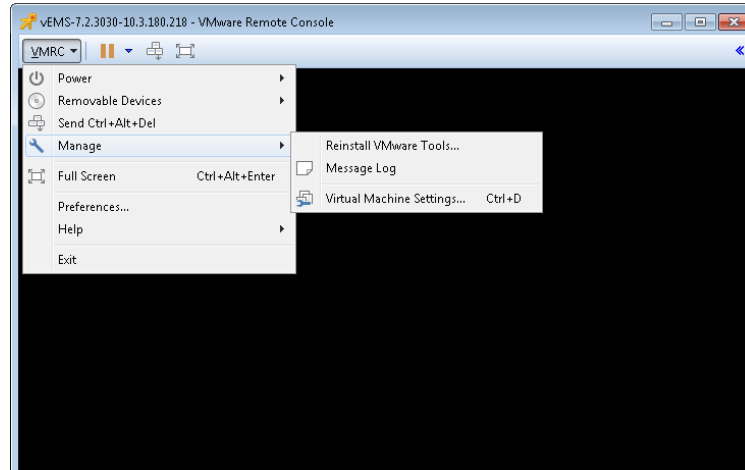


Figure 10-6: VMware Web Client



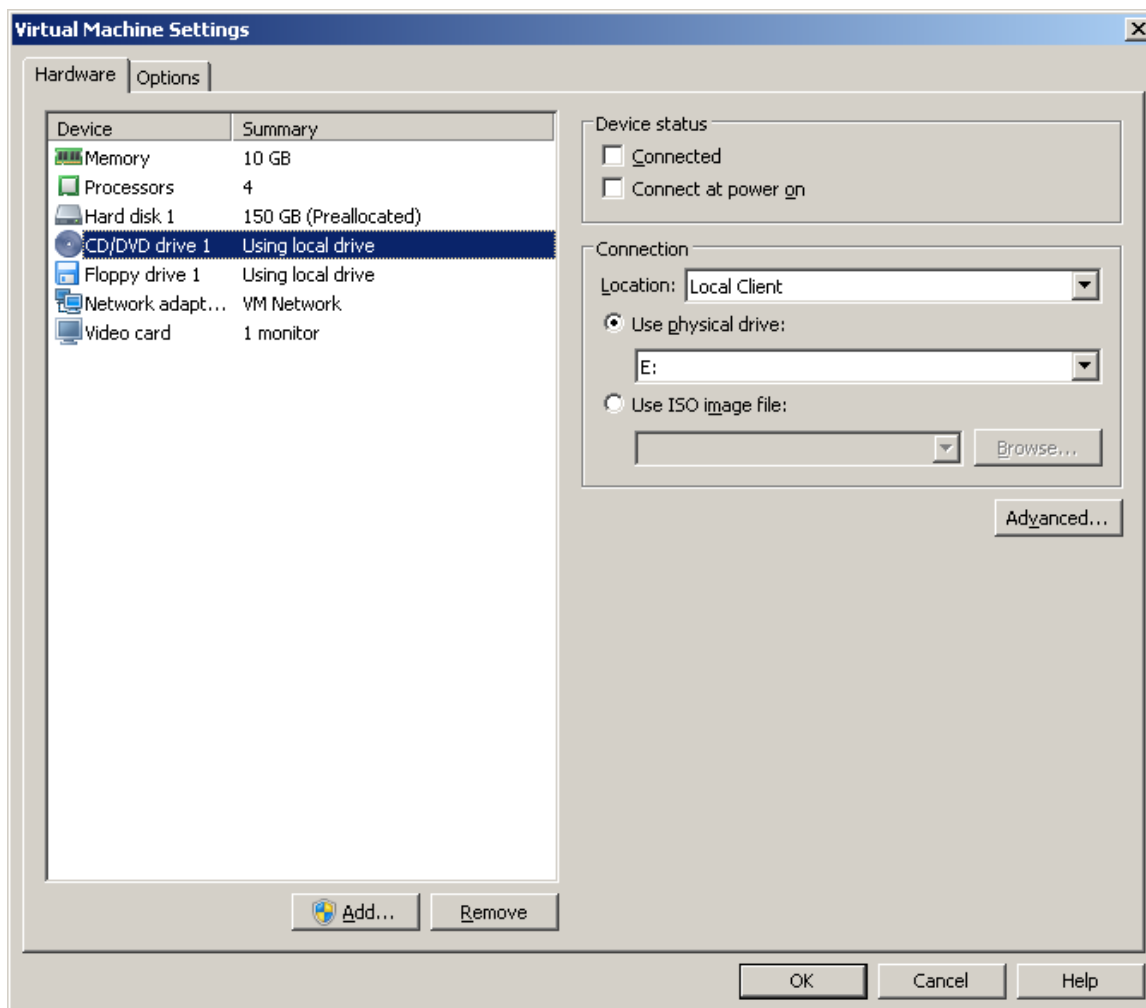
The remote console application is displayed.

Figure 10-7: Remote Console Application



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

**Figure 10-8: Virtual Machine Settings**



3. 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**.

### 10.1.1.2 Setting up Using VMware Server Host

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

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

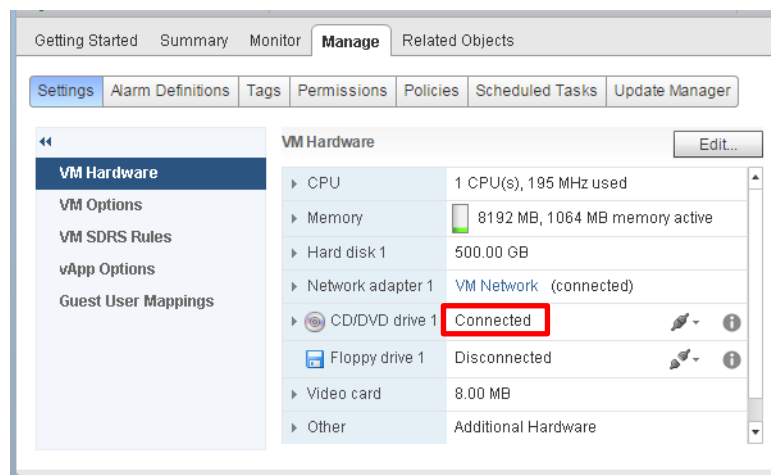
1. Select the **Manage** tab, right-click the Connect icon and select one of the following options:
  - Connect to host CD device
  - Connect to CD/DVD image on a datastore

**Figure 10-9: 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 10-10: CD/DVD Drive - Connected Status**



## 10.1.2 Microsoft Hyper-V Platform

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.

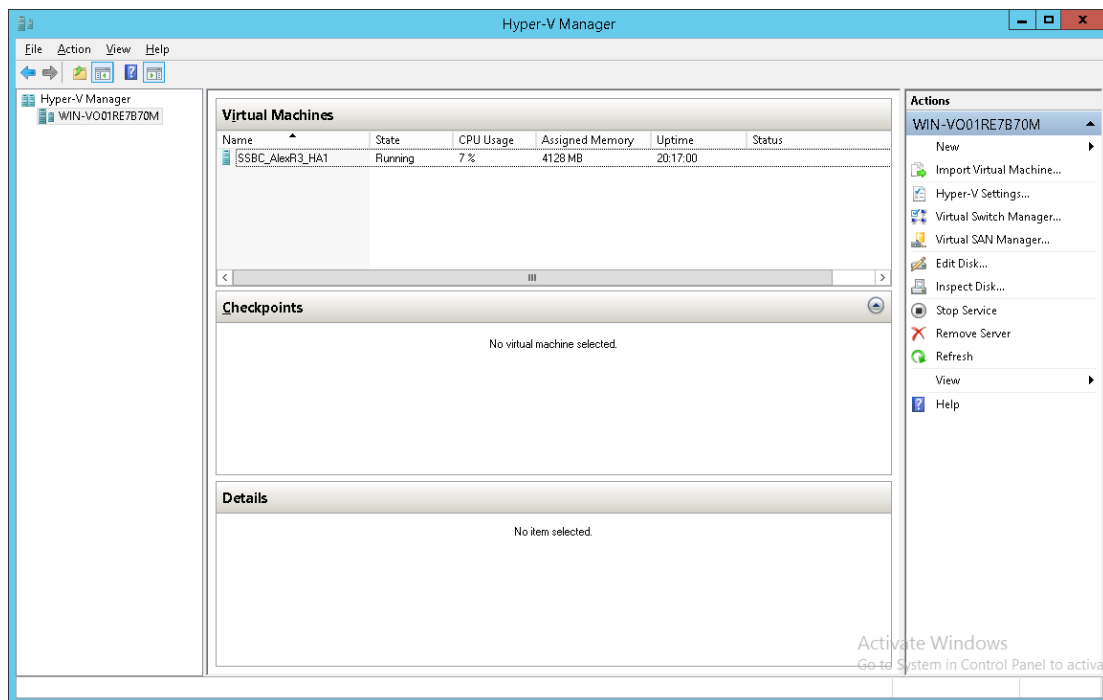
The upgrade of the OVOC server on Microsoft Hyper-V includes the following procedures:

- Upgrade the Virtual Machine (VM) (see Section 8.2.1).
- Configure the Virtual machine hardware settings (see Section 8.2.2).
- Change MAC addresses from 'Dynamic' to 'Static' (see Section 8.2.3).

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

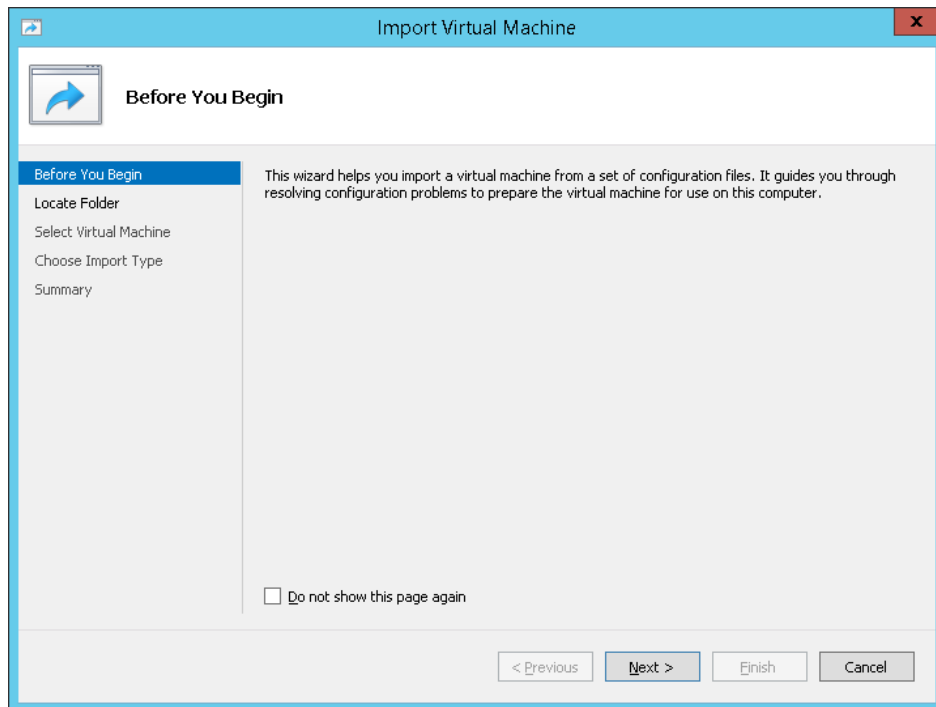
1. Transfer the ZIP file containing the Microsoft Hyper-V Virtual Machine installation package from the AudioCodes **DVD3-OVOC Server Application Installation** to your PC (see Appendix D for instructions on how to transfer files).
2. Open Hyper-V Manager by clicking **Start > Administrative Tools >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

**Figure 10-11: Installing the OVOC server on Hyper-V – Hyper-V Manager**



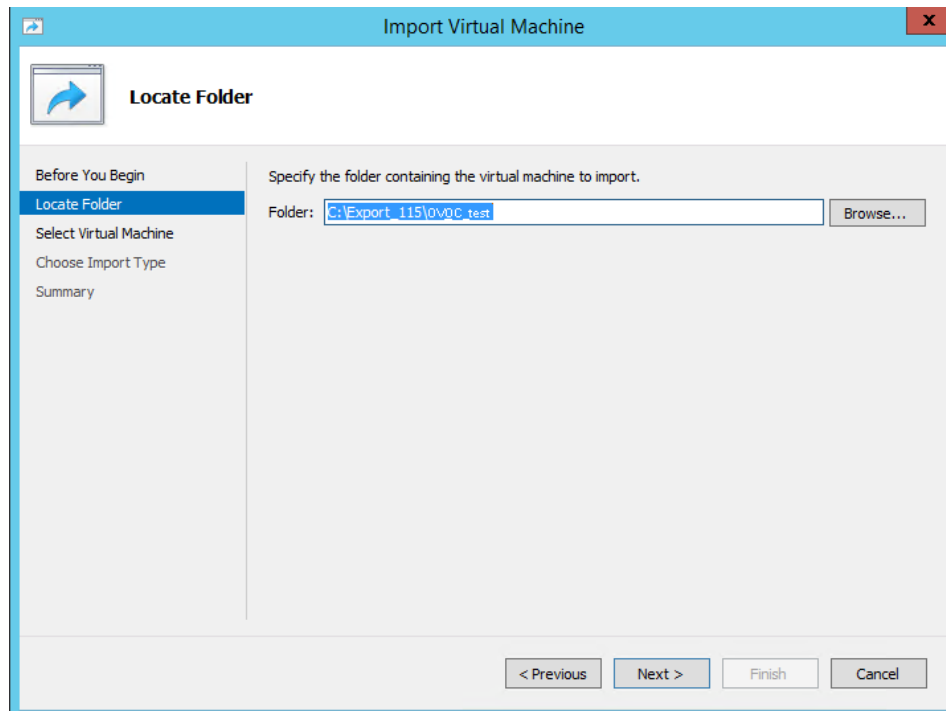
3. Start the Import Virtual Machine wizard: click the **Action** tab, and then select **Import Virtual Machine** from the menu; the Import Virtual Machine screen shown below opens:

**Figure 10-12: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard**



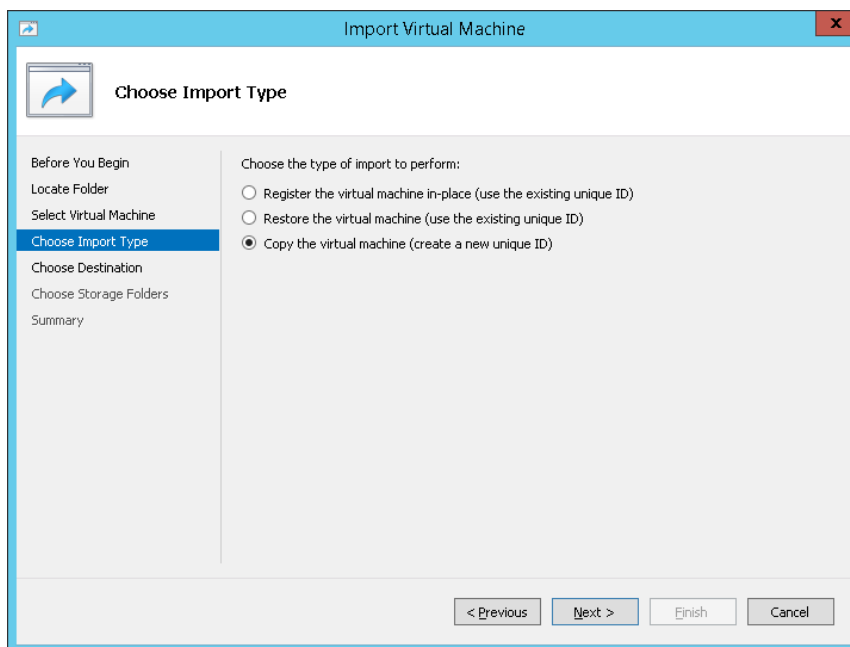
4. Click **Next**; the Locate Folder screen opens:

**Figure 10-13: Installing OVOC server on Hyper-V – Locate Folder**



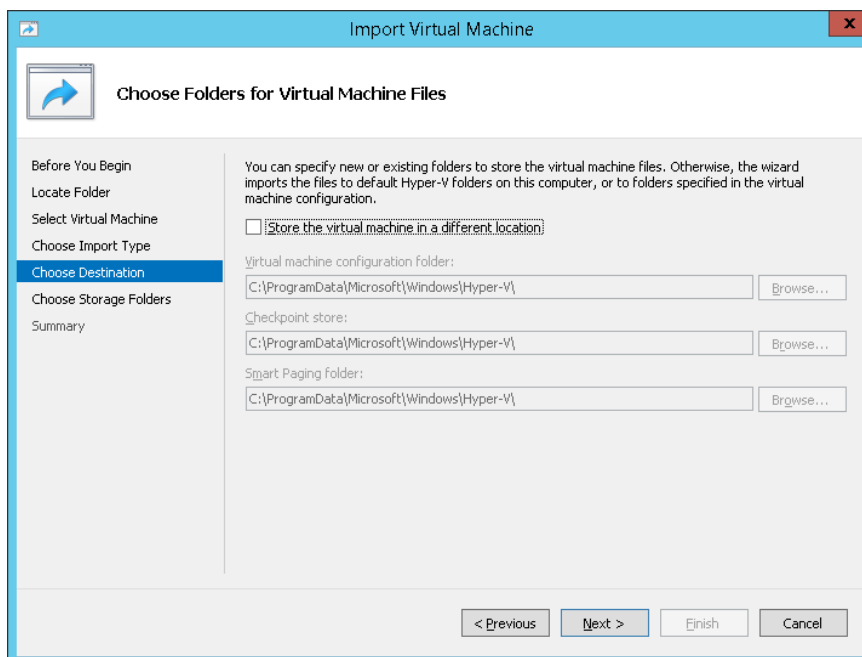
5. Enter the location of the VM installation folder, which was previously extracted, from the zip file as shown in the figure above, and then click **Next**; the Select Virtual Machine screen opens.
6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

**Figure 10-14: Installing OVOC server on Hyper-V – Choose Import Type**



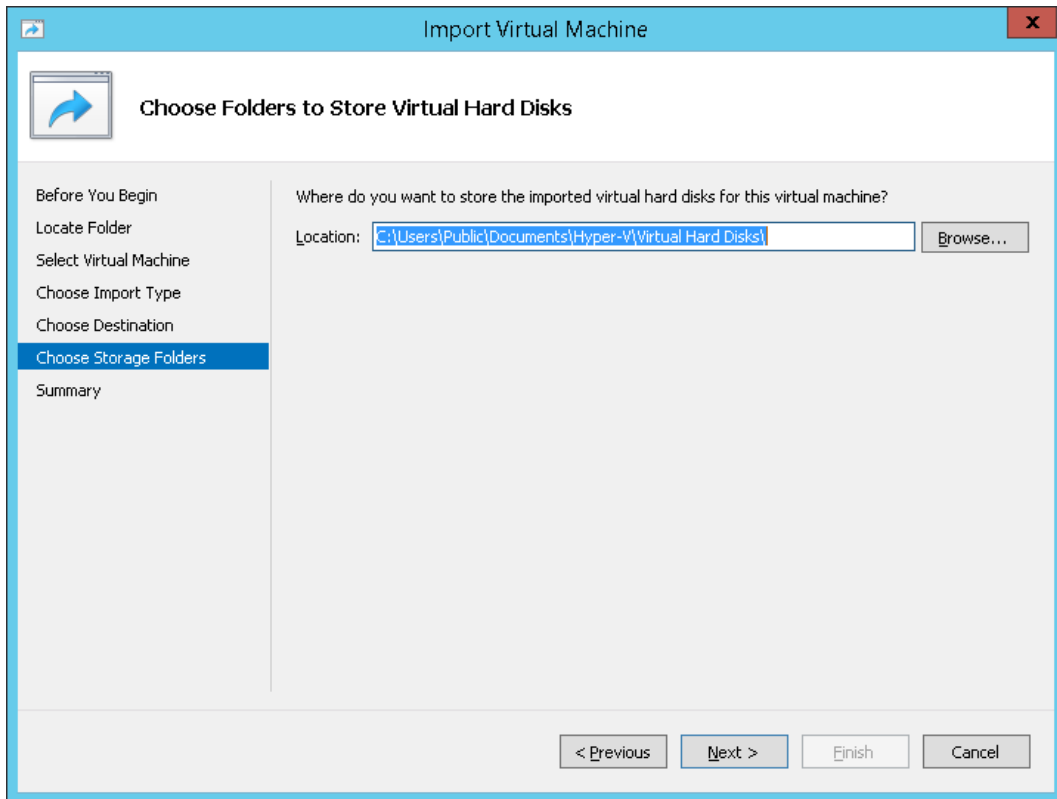
7. Select the option "Copy the virtual machine (create a new unique ID)", and then click **Next**; the Choose Folders for Virtual Machine Files screen opens:

**Figure 10-15: Installing OVOC server on Hyper-V – Choose Destination**



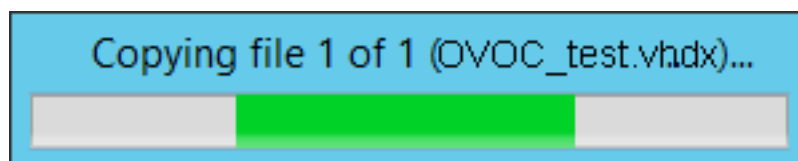
8. Select the location of the virtual hard disk, and then click **Next**; the Choose Storage Folders screen opens:

**Figure 10-16: 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 10-17: File Copy Progress Bar**



This step may take approximately 30 minutes to complete.



## 10.2 Step 2: Run the Upgrade Script

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



**Note:** 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 10-18: 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 10-19: 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 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 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. 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 8.



**Note:** After the OVOC server has rebooted, repeat steps 2 to 6.

Figure 10-20: OVOC Server Application Install with Patches

```

Done
>>> Copy Oracle Security Patch
...
>>> Remove Old Oracle Security Patch Files
...
>>> Applying Oracle Security Patch
...

-----
Installing Oracle CPU patch 9655014
-----

NOTE: patch installation may take up to 30 min, so be patient

Oracle patch 9655014 is already installed
>>> ===== ...
>>> Installation Completed, Oracle is Now Secured ...
>>> ===== ...
>>> Remove /tmp/EmsServerInstall ...
EMS-Server17# reboot

```

Figure 10-21: 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**.



**Note:** 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.

## 10.3 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.

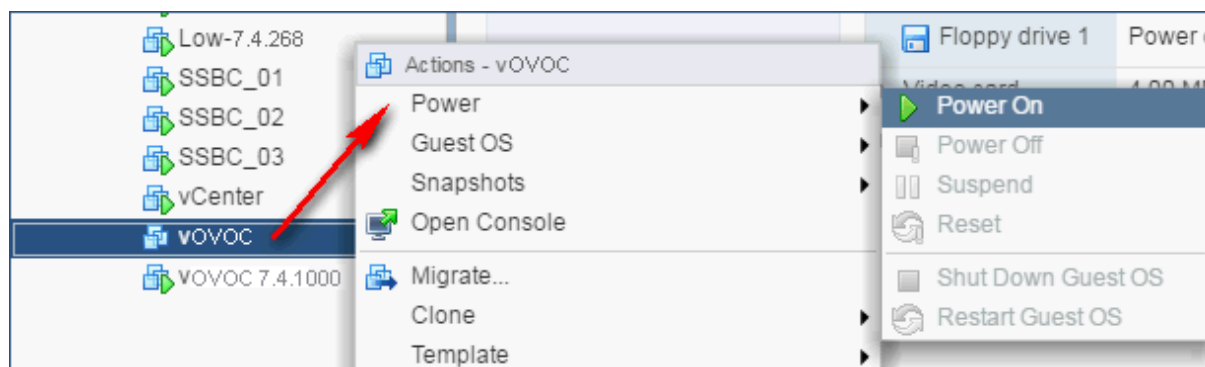
### 10.3.1 VMware Platform

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 (see Chapter 3).

Figure 10-22: 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 (see Chapter 14.14) and verify login to OVOC Web client is successful.
7. Verify that the Date and Time are set correctly (see Section 19.3 to set the date and time).
8. Set the OVOC server network IP address as described in Section 18.1.
9. Configure other settings as required (see Chapter 13).

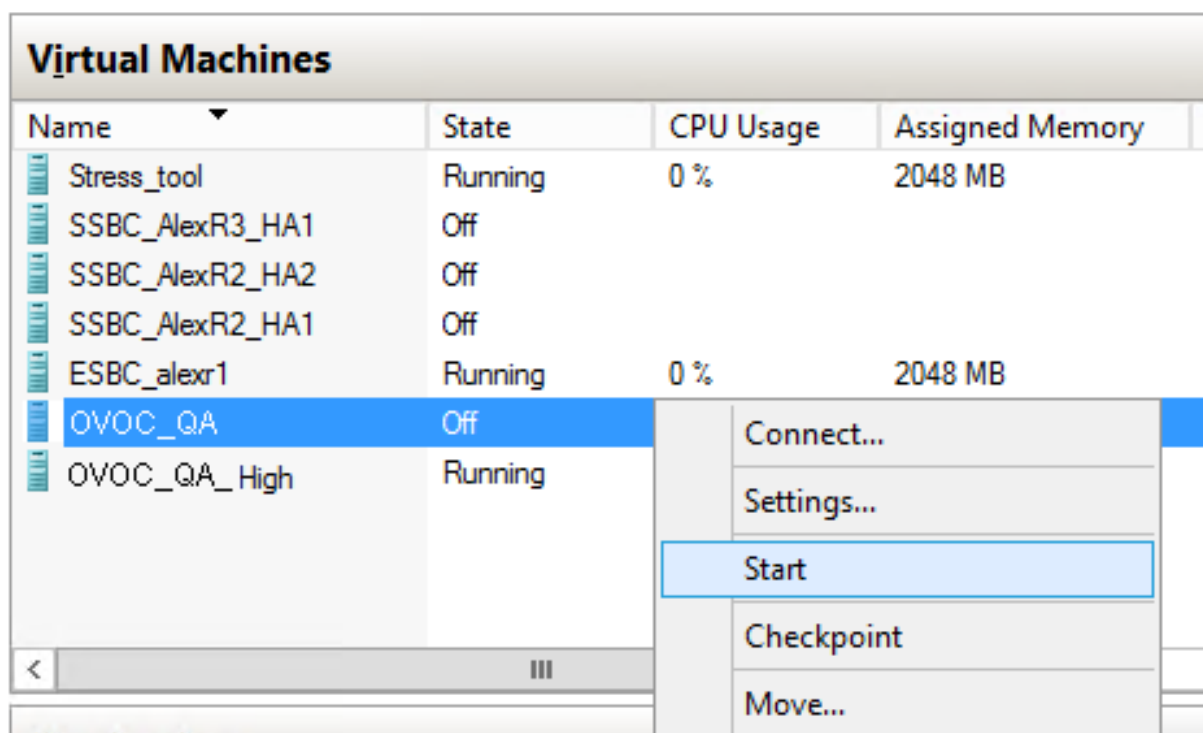
### 10.3.2 Hyper-V Platform

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 10-23: 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 10-24: Connect to OVOC Server Console

Virtual Machines				
Name	State	CPU Usage	Assigned Memory	Uptime
Stress_tool	Running	0 %	2048 MB	1.04:34:22
SSBC_AlexR3_HA1	Off			
SSBC_AlexR2_HA2	Off			
SSBC_AlexR2_HA1	Off			
ESBC_alexr1	Running	0 %	2048 MB	1.04:10:46
OVOC_QA	Off			
OVOC_HA_HIGH	Running	0 %	2048 MB	1.02:37:53
		<div> <div>Connect...</div> <div>Settings...</div> <div>Turn Off...</div> <div>Shut Down...</div> </div>		

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 (see Chapter 1414) and verify login to OVOC Web client is successful.
7. Verify that the Date and Time are set correctly (see Section 19.3 to set the date and time).
8. Set the OVOC server network IP address as described in Section 18.1.
9. Configure other settings as required (see Chapter 13).

# Part IV

## OVOC Server Machine Backup and Restore

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





# 11 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 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 Section 17.3.

- **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.



## Warning:

- 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 all files in /data/NBIF/EMSBackup/emsSServerBackup\_<time&date>\_<version>.tar file directory 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.

## 11.1 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.

**This page is intentionally left blank.**

## 12 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.

**Note:**

- 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 Chapter 13.
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 11 to /data/NBIF directory by SCP or SFTP client using the 'acems' user. Overwrite existing files if required.
6. In EMS Server Manager, go to the Application Maintenance menu and 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 (see Section 18.1).
9. If you installed custom certificates prior to the restore, you must reinstall these certificates (see Appendix C).

**This page is intentionally left blank.**

# 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 EMS Server Manager actions directly through the Linux OS shell. If you perform such actions, OVOC application functionality may be harmed.



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



# 13 Getting Started

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

## 13.1.1 Connecting to the EMS Server Manager

You can either run the EMS 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 EMS Server Manager menu is displayed:

**Figure 13-1: EMS Server Manager Menu**

```

OUOC Server 7.4.2050 Management
-----
Main Menu
-----
>1. Status
2. General Information
3. Collect Logs
4. Application Maintenance
5. Network Configuration
6. Date & Time
7. Security
8. Diagnostics
q. Exit
  
```



**Important:**

- 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 (see Chapter 14)
- **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. See Chapter 15.
- **Collect Logs** – Collates all important logs into a single compressed file (see Chapter 16 ):
  - General Info
  - Collect Logs



- **Application Maintenance** – Manages system maintenance actions (see Chapter 17):
  - Start / Stop the Application
  - Web Servers
  - Change Schedule Backup Time
  - Restore
  - High Availability
  - License
  - Shutdown the machine
  - Reboot the machine
- **Network Configuration** – Provides all basic, advanced network management and interface updates (see Chapter 18):
  - 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 (see Chapter 19):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations (see Chapter 20):
  - Add OVOC user
  - SSH
  - DB Password (OVOC and SEM processes will be stopped)
  - OS Users Passwords
  - Apache Security Settings:
    - ◆ TLS Version 1.0
    - ◆ TLS Version 1.1
    - ◆ TLS Contexts for Apache
    - ◆ HTTPS Authentication
    - ◆ Enable IP Phone 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 (see Chapter 21):
  - Server Syslog
  - Devices Syslog
  - Devices Debug

## 13.1.2 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".

## 14 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 14-1: Application Status**

```

-----Application-----|-----Status-----
Watchdog                  |UP
OVOC Server               |UP
SEM CPEs Server           |UP
SEM MS Lync Server        |UP
SEM Endpoints Server      |UP
CLM Server                |UP
Tomcat Server             |UP
Apache Server             |UP
Oracle DB                 |UP
Oracle Listener           |UP
SNMP Agent                |DOWN
NTP Daemon                |UP
-----
Press 'Enter' key to back to main menu...

```

The following table describes the application statuses.

**Table 14-1: 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.
Tomcat Server	Indicates the status of the Tomcat server, which manages the connection to the browser's statistics page.

Application	Status
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.
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.

## 15 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 EMS Server Manager root menu, choose **General Information**, and then press Enter; the following is displayed:

Figure 15-1: General Information

```

!vg-root      /          28G xfs      lvm running
!vg-swap      [SWAP]    23.5G swap    lvm running
!vg-data      /data     1.7T xfs      lvm running
!vg-meta      /meta     512M xfs      lvm running
!vg-opt       /opt      28G xfs      lvm running
!vg-oracle    /oracle   25G xfs      lvm running
!vg-var       /var      28G xfs      lvm running
!vg-home      /home     158G xfs      lvm running
sr0           1824M      rom running hp
!Data usage:
/dev/mapper/vg-data 1.7T 28G 1.7T 2% /data
-----
Versions
!OVOC Version   : 7.4.2891
!OS Version    : Linux 3.10.0-693.17.1.el7.x86_64 x86_64
!OS Revision    : CentOS 7 for EMS Server (Rev. 18)
!Java Version   : java full version "1.8.0_161-b12"
!Apache version: Apache/2.4.6 (CentOS) Server built: Oct 19 2017 20:39:16

!Server's NAT   : Not configured
!Server's Certificate : Default
<more>

```

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

Figure 15-2: General Information

```

Interface      : eno1
Host Name      : 000C-92
IP Address     : 172.17.140.92
Subnet Mask    : 255.255.255.0
Network Address : 172.17.140.0

Date & Time Information
!Date & Time   : [28/02/2018 10:11:04]
!Time Zone    : Europe/London (GMT, +0000)

Network Time Protocol
Server #1
Peer:         : static.109.226.
Sync source   : .INIT.
Stratum:      : 16
Type          : Unicast
Last response  : - seconds ago
Polling interval: 1024 seconds
Reach : 0
Delay : 0.000 ms.
Offset : 0.000 ms.
Jitter : 0.000 ms.

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

```

## 16 Collecting Logs

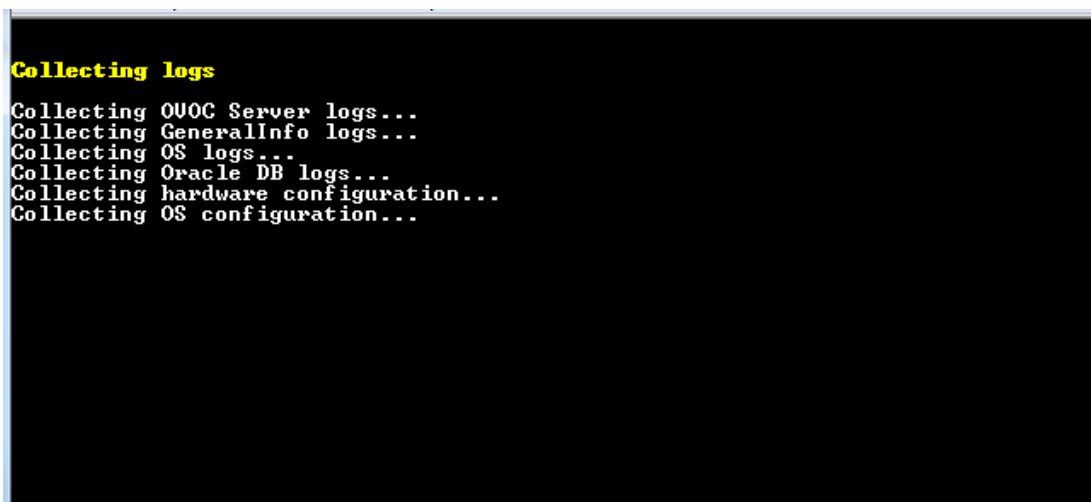
This option enables you to collect important log files. All log files are collected in a single file `log.tar` that is created under the user home directory. The following log files are collected:

- OVOC Server Application logs
- Server's Syslog Messages
- Oracle Database logs
- Tomcat logs
- Hardware information (including disk)
- 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 16-1: EMS Server Manager – Collect Logs**



```
Collecting logs
Collecting OVOC Server logs...
Collecting GeneralInfo logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
```

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 16-2: TAR File Location

```
Collecting logs
Collecting OVOC Server logs...
Collecting GeneralInfo 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 95%)
Logs can be found in /home/acems/logs.tar.zip
Press Enter to continue
```



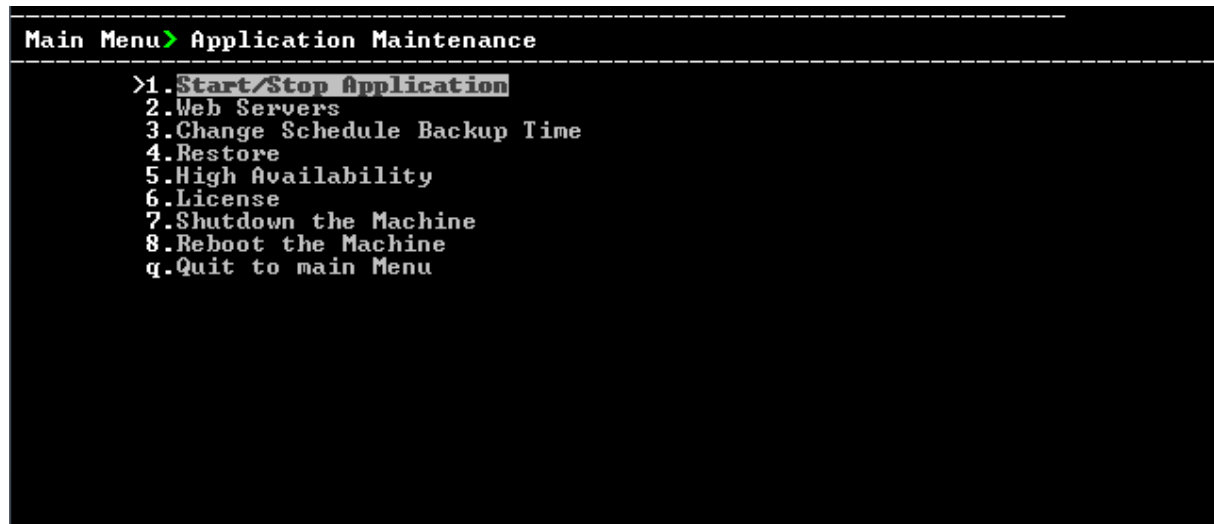
# 17 Application Maintenance

This section describes the application maintenance.

➤ **To configure application maintenance:**

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

**Figure 17-1: Application Maintenance**



This menu includes the following options:

- Start/Stop Application (see Section 17.1).
- Web Servers (see Section 17.2).
- Change Schedule Backup Time (see Section 17.3).
- Restore (see Section 17.4)
- License (see Section 17.5).
- Shutdown the Machine (see Section 17.6).
- Reboot the Machine (see Section 17.7).

## 17.1 Start /Stop the Application

This section describes how to start or stop the application.

➤ **To start/stop the application:**

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

Figure 17-2: Start or Stop the OVOC Server

```

OVOC Server 7.4.2050 Management
-----
Main Menu> Application Maintenance
-----
OVOC Server is started. Stop OVOC Server?
>1. Yes
  2.No
  
```

2. Select **Yes** to start the OVOC server or **No** to stop it.

## 17.2 Web Servers

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

Figure 17-3: – 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>
  h.Back
  q.Quit to main Menu
  
```

### 17.2.1 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.

## 17.2.2 HTTP/HTTPS Services

This section describes how to open and close the different HTTP/HTTPS services.

### ➤ To open/close HTTP Service (Port 80):

- In the Web Servers 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 IP Phone Manager Pro Web browser.

### ➤ To open/close IPPs FILES (Port 8080):

- In the Web Servers 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.

### ➤ To open/close IPPs HTTP (Port 8081):

- In the Web Servers 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.

### ➤ To open/close IPPs HTTPS (Port 8082):

- In the Web Servers 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).

## 17.3 Change Schedule Backup Time

This option enables you to reschedule the time that you wish to back up the OVOC server. (see Chapter 11)

## 17.4 Restore

This option enables you to restore the OVOC server to the latest backed up version (see Chapter 12).

## 17.5 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.

In order to obtain a valid license for your OVOC Server License you should activate your product through AudioCodes 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:**Product Key:** 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 (see Section 17.5.1 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' (see below).

The time zone is determined by the configured date and time in the Date & Time menu (see Section 19.2).

You will receive an e-mail with your product license file.



### Note:

- When you order AudioCodes devices (Mediant SBC and Mediant Gateway 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 Figure 17-4).

## 17.5.1 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, IP Phone Management 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 17-4: License Manager**

```

OVOC Server 7.4.2050 Management
-----
Main Menu> Application Maintenance> License
-----
License Configuration Manager:
Server Machine ID: D4547B4719EA
Product Key: 1111
License Status:  ENABLED
OVOC Advanced:  Yes
Floating License:  ENABLED
Expiration Date: 01-01-2019

License Pool
Managed Devices: 10
SBC Sessions: 100
SBC Registrations: 188
SBC Transcoding: 288
Main Menu> Application Maintenance> License
-----
CB PBX Users: 10
CB Analog Devices: 10
CB Voicemail Accounts: 10
-----

Endpoints
Managed Endpoints: 3.000
-----

Voice Quality
Total Devices: 1.000
Total Endpoints: 5.000
Total Sessions: 2.000
Total Users: 4.000
-----

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

```

**Table 17-5: License Pool Parameters**

License Pool	Description
Devices	The total number of devices (SBCs, gateways and MSBRs) that can be managed by the License Pool.

License Pool	Description
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>Voice Quality</b>	
Devices	The number of Voice Quality monitored devices (SBCs, gateways and MSBRs).
Endpoints	The number of Voice Quality monitored endpoints.
Sessions	The number of concurrent Voice Quality monitored call SBC sessions.
Users	The number of Skype for Business users supported by the OVOC call quality monitoring.
<b>Endpoints Management</b>	
Endpoints	The number of endpoints supported by the IP Phone Manager Pro application.

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

## 17.6 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.

## 17.7 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.

**This page is intentionally left blank.**



## 18 Network Configuration

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

➤ **To run the network configuration:**

- From the EMS Server Manager root menu, choose **Network Configuration**; the following is displayed:

**Figure 18-1: Network Configuration**

```
Main Menu> Network Configuration
-----
>1. Server IP Address      <The server will be rebooted>
2. Ethernet Interfaces    <The server will be rebooted>
3. Ethernet Redundancy    <The server will be rebooted>
4. DNS Client
5. NAT
6. Static Routes
7. SNMP Agent
8. SNMPv3 Engine ID
q. Quit to main Menu
```

This menu includes the following options:

- Server IP Address (the server will be rebooted) (see Section 18.1).
- Ethernet Interfaces (the server will be rebooted) (see Section 18.2).
- Ethernet Redundancy (the server will be rebooted) (see Section 18.3).
- DNS Client (see Section 18.4).
- NAT (see Section 18.5).
- Static Routes (see Section 18.6).
- SNMP Agent (see Section 18.7).

### 18.1 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.



**Note:** 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 18-2: EMS Server Manager – Change Server's IP Address**

```
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 18-3: IP Configuration Complete**

```
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.

## 18.2 Ethernet Interfaces

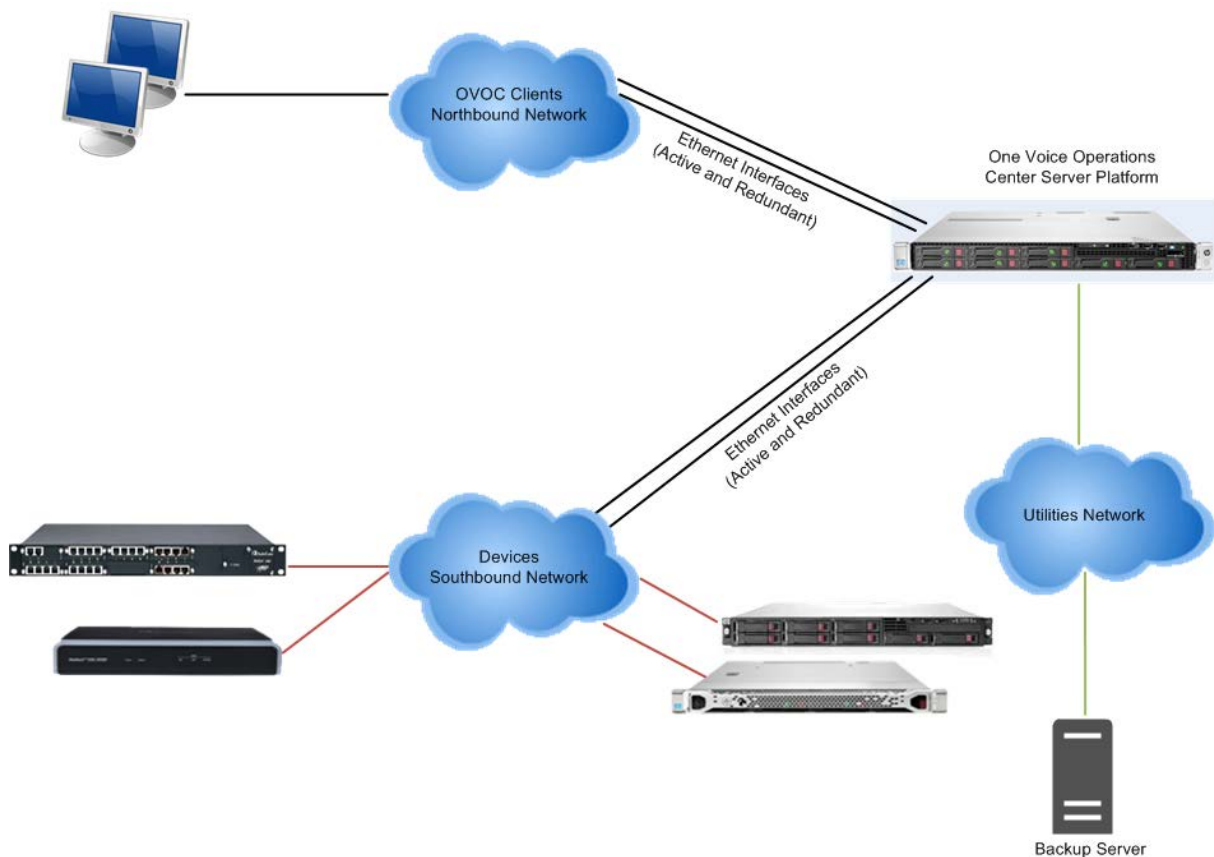
This section describes how to configure Ethernet interfaces.

### 18.2.1 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 18-4: 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, see [Section 18.6](#).

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 18-5: EMS Server Manager – Configure Ethernet Interfaces**

```

Main Menu> Network Configuration> Ethernet Interfaces
>1. Add Interface
  2. Remove Interface
  3. Modify Interface
  b. Back
  q. Quit to main Menu
  
```

2. Choose from one of the following options:
  - **Add Interface** – Adds a new interface to the OVOC server (see Section 18.2.2).
  - **Remove Interface** – Removes an existing interface from the OVOC server (see Section 18.2.3).
  - **Modify Interface** – Modifies an existing interface from the OVOC server (see Chapter 3).

## 18.2.2 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 18-9: 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) █
```

## 18.2.3 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.

## 18.2.4 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.

## 18.3 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.

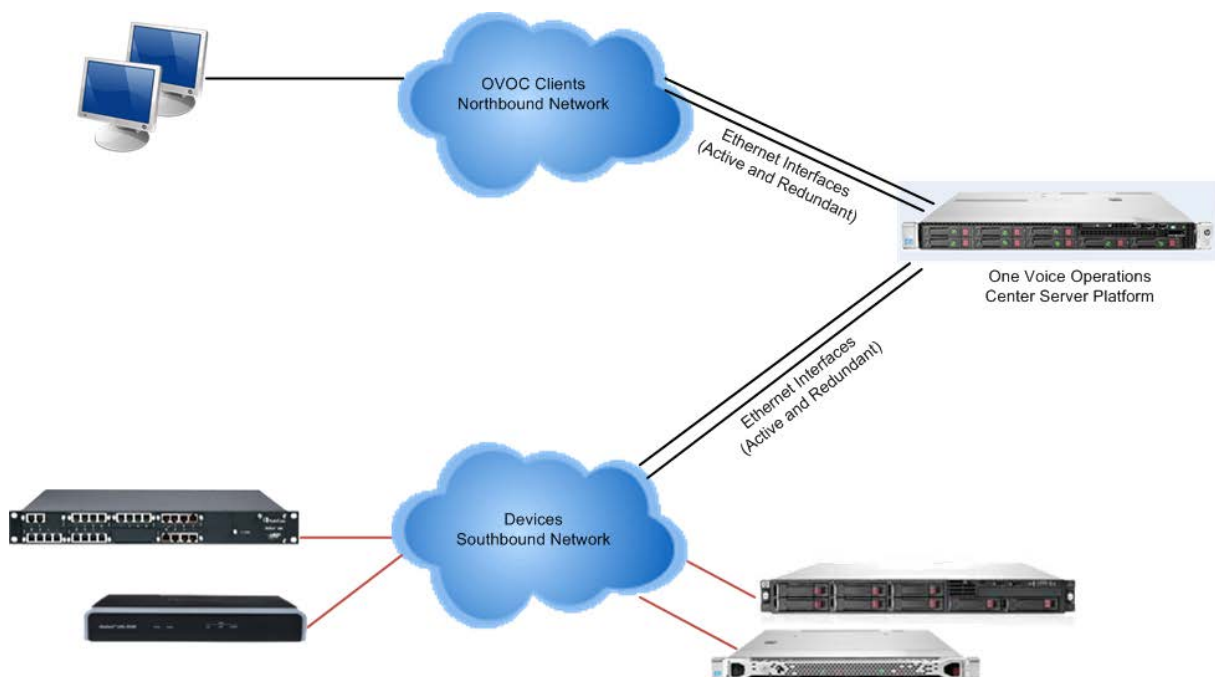
The OVOC server supports up to four Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them. For example, OVOC Clients [Northbound] and Gateways [Southbound]].

This option enables you to configure Ethernet ports redundancy.



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

**Figure 18-6: 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 18-7: 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 (see Section 18.3.1).
  - Remove Redundant Interface (see Section 18.3.2).
  - Modify Redundant Interface (see Section 18.3.3).

### 18.3.1 Add Redundant Interface

Remove a redundant interface under the following circumstances:

- You have configured an Ethernet interface (see Section 18.3.1).
- 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 18-8: Add Redundant Interface (Linux)**

```

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) █
    
```



### 18.3.2 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 18-9: 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
```

### 18.3.3 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 18-10: Modify Redundant Interface (Linux)**

```

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
  
```

## 18.4 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 18-11: 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.

## 18.5 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 a NAT address; type **y**.
3. Enter the NAT address, and then press Enter.
4. Type **y** to confirm the changes.
5. 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.

## 18.6 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 18-12: 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.

## 18.7 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 (see Section [18.7.1](#))
  - Configure the northbound destination for linux system traps forwarding (see Section [18.7.2](#)).
  - Configure the SNMPv3 Engine ID (see Section [18.7.3](#))

➤ **To configure SNMP Agent:**

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

Figure 18-13: SNMP Agent

```

OUOC Server 7.4.302 Management
-----
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 18-14: Configure SNMP Agent

```

OUOC Server 7.4.302 Management
-----
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
  
```

## 18.7.1 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 18-15: SNMP Agent Listening Port**



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

## 18.7.2 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.

### 18.7.3 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 18-16: 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 18-17: 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)
```



## 19 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 19-1: 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
- Timezone Settings
- Date & Time Settings

See Chapter 19.

### 19.1 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.



**Note:**

- 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 19-2: 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.

## 19.1.1 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.

## 19.1.2 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.

## 19.2 Timezone Settings

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



**Note:** 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.

## 19.3 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 19-3: Change System Time and Date Prompt**

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

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

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

**This page is intentionally left blank.**

## 20 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 EMS Server Manager root menu, choose **Security**, and then press Enter, the following is displayed:

**Figure 20-1: Security Settings**

```

OVOC Server 7.4.3077 Management
-----
Main Menu > Security
-----
>1.Add OVOC User
2.SSH
3.DB Password <OVOC Server will be stopped>
4.OS Users Passwords
5.Apache Security Settings
6.File Integrity Checker
7.Software Integrity Checker (AIDE) and Prelinking
8.USB Storage
9.Network options
10.Audit Agent Options
11.Disable Statistics Report Web page Secured Communication <OVOC Se
rver will be restarted>
12.Server Certificates Update
13.SEM - AudioCodes devices communication
q.Quit to main Menu
  
```

This menu includes the following options:

- Add OVOC User (see Section [20.1](#)).
- SSH (see Section [20.2](#)).
- DB Password (EMS and SEM applications will be stopped) (see Section [20.3](#)).
- OS Users Password (see Section [20.4](#))
- [20.10](#)File Integrity Checker (see Section [20.5](#))
- Software Integrity Checker (AIDE) and Pre-linking (see Section [20.6](#))
- USB Storage (see Section [20.7](#))
- Network options (see Section [20.8](#))
- Audit Agent Options (see Section [20.9](#))
- HTTPS/SSL/TLS (see Section [20.10](#))

## 20.1 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:** Note and retain these passwords for future access.

## 20.2 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 20-2: 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 (see Section [20.2.1](#)).
- Configure SSH Banner (see Section [20.2.2](#)).
- Configure SSH on Ethernet Interfaces (see Section [20.2.3](#)).
- Disable SSH Password Authentication (see Section [20.2.4](#)).
- Enable SSH Ignore User Known Hosts Parameter (see Section [20.2.5](#)).
- Configure SSH Allowed Hosts (see Section [20.2.6](#)).

### 20.2.1 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 20-3: SSH Log Level Manager

```

EMS Server 7.4.236 Management
-----
Main Menu> Security> SSH> Configure SSH Log Level
-----
LogLevel DEFAULT
Note: Changing LogLevel will restart SSH
>1. FATAL
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.

## 20.2.2 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 20-4: 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. Enable SSH Banner
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.

## 20.2.3 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 20-5: 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
b. Back
q. Quit to main Menu
  
```

This menu includes the following options:

- Add SSH to All Ethernet Interfaces (see Section 20.2.3.1).
- Add SSH to Ethernet Interface (see Section 20.2.3.2).
- Remove SSH from Ethernet Interface (see Section 20.2.3.3).

### 20.2.3.1 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.

### 20.2.3.2 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.

### 20.2.3.3 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.



**Note:** 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.

## 20.2.4 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 20-6: 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.



**Note:** 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.

## 20.2.5 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 20-7: 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.

## 20.2.6 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 20-8: 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 (see Section 20.2.6.1).
- Deny ALL Hosts (see Section 20.2.6.2).
- Add Host/Subnet to Allowed Hosts (see Section 20.2.6.3).
- Remove Host/Subnet from Allowed Hosts (see Section 20.2.6.4).

### 20.2.6.1 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.

### 20.2.6.2 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.



**Note:** 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.

### 20.2.6.3 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 20-9: Add Host/Subnet to Allowed Hosts**

```
-----
Main Menu> Security> SSH> Configure SSH Allowed Hosts> Add Host/Subnet to Allow
ed 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.



**Note:** 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 20-10: 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
    
```

#### 20.2.6.4 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:



**Note:** 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”.

## 20.3 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 20-11: 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:
```

3. Enter the new password, which should be at least 15 characters long, contain at least two digits, two lowercase and two uppercase characters, two underscores and should differ by one character from the previous passwords.



**Note:**

- 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.

4. After validation, a message is displayed indicating that the password was changed successfully.

## 20.4 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. Proceed to one of the following procedures:
  - General Password Settings (see Section 20.4.1).
  - Operating System User Security Extensions (see Section 20.4.2).

### 20.4.1 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.

```
Do you want to change general password settings? (y/n) y
```

2. The Minimum Acceptable Password Length prompt is displayed; type **10**, and then press Enter.

```
Minimum Acceptable Password Length [10]: 10
```

3. 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
```

4. The Maximum Login Retries prompt is displayed; type **3**, and then press Enter.

```
Maximum Login Retries [3]: 3
```

5. The Failed Login Locking Timeout prompt is displayed; type **900**, and then press Enter.

```
Failed Login Locking Timeout [900]: 900
```

6. 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
```



## 20.4.2 Operating System Users 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 in [Figure 20-12](#)).

➤ **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 20-12: 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 20-13: 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.

```



**Note:** 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.

## 20.5 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.

## 20.6 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 20-14: 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.

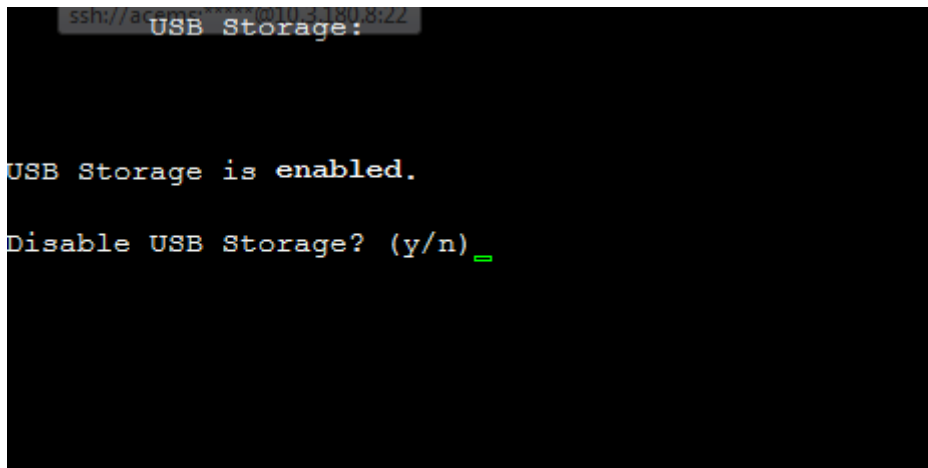
## 20.7 USB Storage

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 20-15: USB Storage



2. Enable or disable USB storage as required.

## 20.8 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 20-16: 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
```

2. Set the required network options.

## 20.9 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 20-17: Auditd Options**

```
Auditd Options:

Not using STIG recommendations for auditd

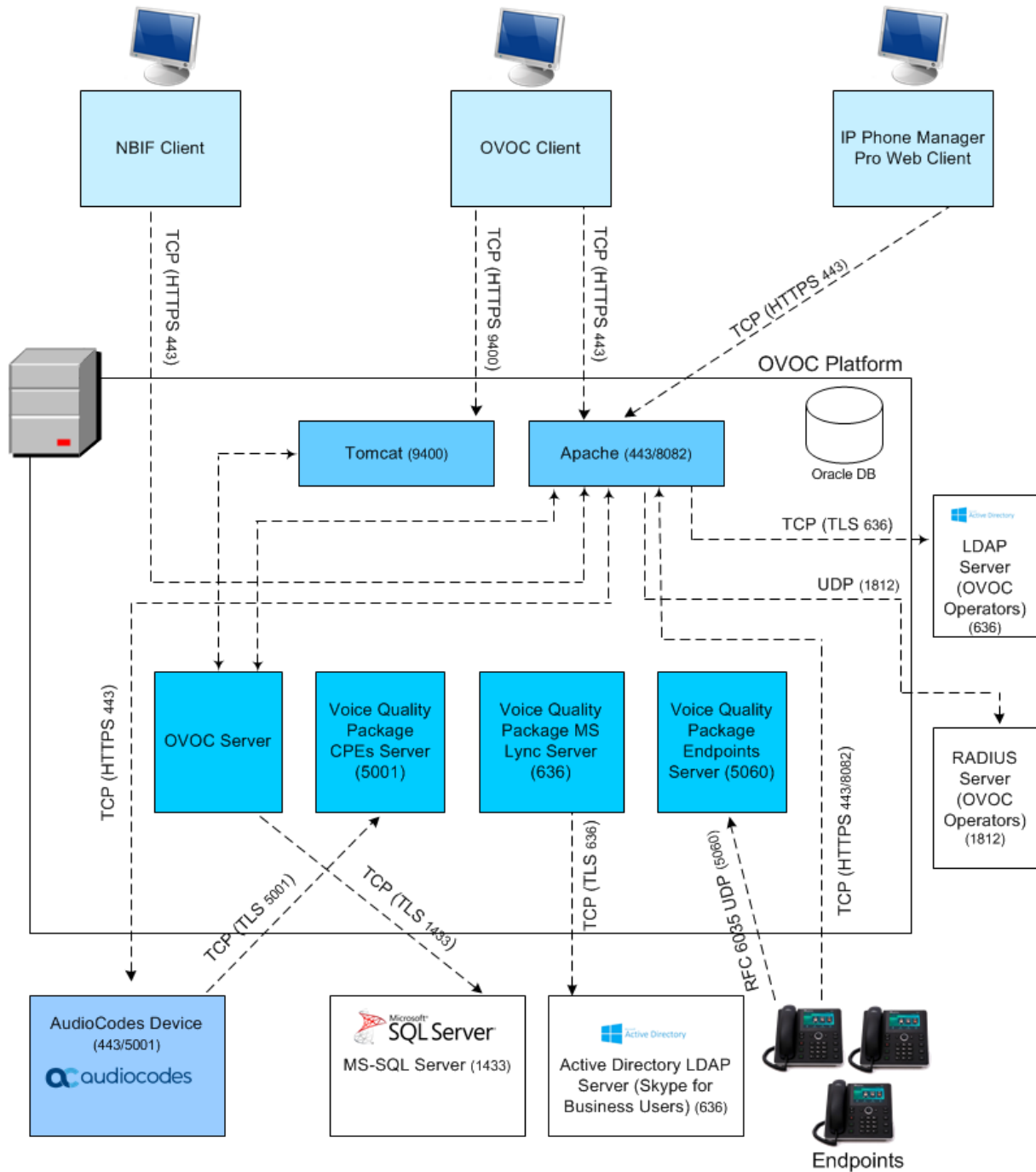
Change auditd settings according to STIG recommendations? (y/n) _
```

2. Enable or disable Auditd options as required.  
Audit records are saved in the following `/var/log/audit/` directory.

## 20.10 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. For most connections, the HTTPS/SSL/TLS protocols can be implemented; those connections where these protocols are not supported are indicated in red.

**Figure 20-18: OVOC Maximum Security Implementation**





**Note:** 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.

### 20.10.1 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.

### 20.10.2 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 [Figure 20-18](#) for an illustration of these connections.



**Note:** 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 C](#)).

➤ **To generate server certificates:**

1. From the Security menu, choose **Server Certificates Update**.

Figure 20-19: Server Certificate Updates

```

OUOC Server 7.4.2050 Management
-----
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 20-20: Generate Server Private Key

```

Main Menu> Security> Server Certificates Update> Generate Server Private Key
-----
Select Private Key size (in bits):
>1. 1024
2. 2048
3. 4096
b. Back
q. Quit to main Menu
  
```

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 20-21: Server Private Key Generated

```

Generating a Server Private Key:
This will override the existing private key and render the existing certificates
invalid until new certificates are imported.
Are you sure you want to generate a new private key? (N/y)y
Select Number Of bits for Private Key:
1. 1024
2. 2048
3. 4096
q. quit and return to menu
Select number: 1
Enter private key password:
Re-enter private key password:
Ready to generate server private key. Continue? (n/Y): y
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)

Done generating private key. Press Enter to go back to the menu

```

➤ **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 20-22: Generating a Server Certificate Signing Request (CSR)

```

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 sent it to the Certificate Authority (CA). For instructions on transferring files, see Appendix D.

Figure 20-23: Transfer CSR File to PC

```
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 D.



**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.

**Note:**

- If you have installed an HA system and wish to install Custom server certificates, the HA system must first be uninstalled, and then you must perform this procedure separately on both server machines (as stand-alone machines).
- 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 Appendix E for information on converting files):

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKlMbgbwDQYJKoZIhvcNAQEFBQAwFzEVMBMGAlUEAx
MM

RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTE1MDUwMzA4NTE0MFowKj
ET

...

Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEExNJol
10

L6V8lzUYOfHrEiq/6g==
-----END CERTIFICATE-----
```

➤ **Step 6: Verify the installed server certificate:**

- Select option 4.

The installed server certificate is displayed:

**Figure 20-24: Installed Server Certificate**

```
Installed Server Certificate:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2416025747 (0x9001a093)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: CN=EMS ROOT CA2
    Validity
      Not Before: Feb 20 19:15:13 2010 GMT
      Not After : Feb 20 19:15:13 2020 GMT
    Subject: O=AudioCodes, CN=EMS Server
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:d2:45:b7:4e:de:ba:0a:38:d9:fb:72:2a:c3:f2:
        15:4a:c9:e1:e1:e7:bf:3f:20:52:fd:3c:43:9a:43:
        7a:50:ad:a1:d5:b0:41:56:6c:7d:11:b4:23:6d:c8:
        9f:d1:2b:41:94:ee:e1:63:33:90:a9:73:b3:94:2a:
        f6:d6:27:31:27:df:64:d0:c2:8c:62:6d:35:d7:0e:
        26:09:5d:c0:71:e3:94:8e:60:b2:55:02:bd:ad:75:
        ef:3d:b2:94:8d:46:0d:c8:d5:be:b1:2f:4d:dd:bc:
--More--
```

➤ **Step 7: Verify the installed root certificate:**

- Select Option 5. The installed root certificate is displayed:

**Figure 20-25: Installed Root Certificate**

```
Installed Server Root Certificate Chain:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2416023367 (0x90019747)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: CN=EMS ROOT CA
    Validity
      Not Before: Feb 20 18:54:27 2010 GMT
      Not After : Feb 20 18:54:27 2020 GMT
    Subject: CN=EMS ROOT CA2
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:bc:dd:d6:eb:71:c8:79:de:f4:12:31:51:21:e6:
          7b:e9:3a:a3:9f:10:bc:4c:37:90:1d:da:4a:40:58:
          36:bb:43:f7:bb:c5:80:02:9e:66:21:7f:20:cc:48:
          c4:40:4a:ad:07:3b:48:3c:31:7a:db:9c:7c:a9:3e:
          76:f8:e9:d2:1a:40:c1:7d:db:16:18:67:66:34:13:
          50:74:08:ec:5b:3d:75:37:8a:d7:53:b2:59:a9:ff:
          a2:f2:23:2b:58:2c:b8:78:99:df:ca:3e:65:60:99:
  --More--
```

➤ **Step 8: Install device certificates and perform supplementary procedures**

- See Appendix C.

## 20.10.3 OVOC Voice Quality Package - AudioCodes Devices Communication

This option allows you to configure the transport type for the XML based OVOC Voice Quality Package communication from the AudioCodes devices to the . 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 20-26: SEM - AudioCodes Device Communication**

```
Main Menu> Security> SEM - AudioCodes devices communication
SEM - AudioCodes devices communication: TCP
>1. TCP <SEM Server will be restarted>
2. TLS <SEM Server will be restarted>
3. TLS/TCP <SEM Server will be restarted>
b.Back
q.Quit to main Menu
```

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).

## 20.10.4 Apache Security Settings

This menu allows you to configure the following Apache server security settings:

- TLS Version 1.0 (see Section 20.10.4.1)
- TLS Version 1.1 (see Section 20.10.4.2)
- Show Allowed SSL Cipher Suites (see Section 20.10.4.3)
- Edit SSL Cipher Suites Configuration String (see Section 20.10.4.4)
- Restore SSL Cipher Suites Configuration Default (see Section 20.10.4.5)
- HTTPS Authentication (see Section 20.10.4.6)
- Enable IP Phone Manager Pro and NBIF Web Pages Secured Communication (see Section 20.10.4.7)
- Change HTTP/S Authentication Password for NBIF Directory (see Section 20.10.4.8)

```

OVOC Server 7.4.3080 Management
-----
Main Menu> Security> Apache Security Settings
-----
!TLsv1.0: ENABLED
!TLsv1.1: ENABLED
!Cipher Suites Configuration String: ?EDH=?ADH=?DSS=?RC4-HIGH=?3DES=?aNU
LL
>1.Disable TLsv1.0 for Apache      <Apache will be restarted>
2.Disable TLsv1.1 for Apache      <Apache will be restarted>
3.Show allowed SSL Cipher Suites
4.Edit SSL Cipher Suites Configuration String <Apache will be restarted>
d)
5.Restore SSL Cipher Suites Configuration Default      <Apache will be
restarted>
6.HTTPS Authentication
7.Enable IP Phone Manager Pro and NBIF Web pages Secured Communication
<Apache will be restarted>
8.Change HTTP/S authentication password for NBIF directory      <Apache
will be restarted>
b.Back
q.Quit to main Menu

```

### 20.10.4.1 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 Apache Security Settings menu, select option **Enable TLSv1.0 for Apache**.

Note 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).

### 20.10.4.2 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 Apache Security Settings menu, select option **Enable TLSv1.1 for Apache**.

Note 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.

Default (enabled).

Apache server is restarted.

### 20.10.4.3 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 Apache 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 20-27: Show Allowed SSL Cipher Suites

```
> 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
Press ENTER to continue...
```

### 20.10.4.4 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 Apache Security Settings menu, select option **Edit SSL Cipher Suites Configuration String**.

Figure 20-28: Show SSL Cipher Suites Configuration

```

> 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.

#### 20.10.4.5 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 Apache Security Settings menu, select **Restore SSL Cipher Suites Configuration Default**.

#### 20.10.4.6 HTTPS Authentication

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 (see Section C.1.1.5).
- **One-way Authentication option:** the OVOC does not authenticate the device connection request using certificates; only the device authenticates the OVOC connection request.



**Note:** You can use the procedure described in Section 20.10.2 to load the certificate file to the OVOC server.

➤ To enable HTTPS authentication:

1. In the Security menu, choose the **HTTPS Authentication** option.

Figure 20-29: HTTPS Authentication



2. Choose one of the following options:
  - 1-Set Mutual Authentication
  - 2. Set One-Way Authentication

#### 20.10.4.7 Enable IP Phone Manager Pro and NBIF Web Pages Secured Communication

This menu option enables you to secure the connection between the IP Phone 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 IP Phone Manager Pro and NBIF Web pages connection:

- From the Security menu, choose **IP Phone Manager and NBIF Web pages Secured Communication**; the connection is secured.



### 20.10.4.8 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 Security 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 20-30: 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.

**This page is intentionally left blank.**

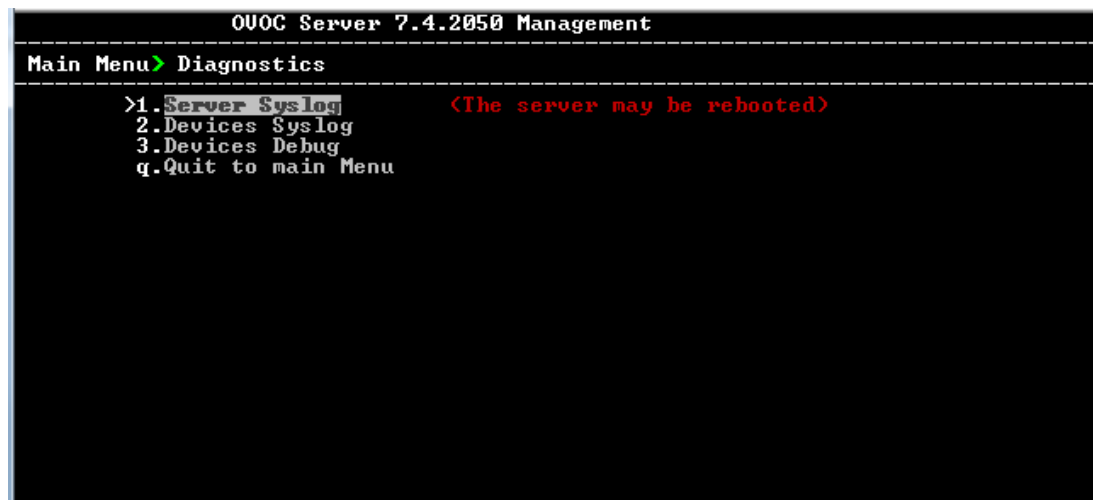
## 21 Diagnostics

This section describes the diagnostics procedures provided by the EMS Server Manager.

➤ **To run OVOC Server diagnostics:**

- From the EMS Server Manager Root menu, choose **Diagnostics**, and then press Enter, the following is displayed:

**Figure 21-1: Diagnostics**



This menu includes the following options:

- Server Syslog Configuration (see Section 21.1).
- Devices Syslog Configuration (see Section 21.2).
- Devices Debug Configuration (see Section 21.3).

### 21.1 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 21-2: Syslog Configuration

```

Syslog configuration
Send EMERG events to system console: n
Forward messages to external server: n

Send EMERG events to system console ? <y/n> y
Logging of many events on console when RS-232 console is used may cause severe p
erformance degradation (due to 9600 baud rate).
Are you sure ? <y/n>

```

Figure 21-3: 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.

## 21.2 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 EMS Server Manager is used to enable this feature.



**Note:** This feature is only relevant for CPE products. Syslog is captured according to the device's configured Syslog parameters. For more information, see the relevant device's *SIP 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**.

## 21.3 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.



**Note:** This feature is only relevant for CPE products. Debug recording packets are collected according to the device's configured Debug parameters. For more information, see the relevant device's *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 EMS 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.



**Note:** It is highly recommended to disable the 'TP Debug Recording' feature when you have completed recording because this feature heavily utilizes system resources.

**This page is intentionally left blank.**



# Part VI

## Configuring the Firewall

This part describes how to configure the OVOC firewall.



## 22 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 22-1: Firewall Configuration Rules**

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
<b>OVOC Clients and OVOC Server</b>					
<b>TCP/IP client ↔ OVOC server</b>	TCP	✓	22	SSH communication between OVOC server and TCP/IP client. Initiator: client PC	OVOC server side / Bi-directional.
<b>HTTPS/NBIF Clients ↔ OVOC server</b>	TCP	✓	443	HTTPS for OVOC/ NBIF clients. Initiator: Client	OVOC server side / Bi-directional.
<b>OVOC Server and Devices</b>					
<b>Device ↔ OVOC server (SNMP)</b>	UDP	✓	1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	✓	162	SNMP trap listening port on the OVOC.	OVOC server side / Receive only

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				Initiator: AudioCodes device	
	UDP	✓	161	SNMP Trap Manager port on the device that is used to send traps to the OVOC server. Initiator: OVOC server	MG side / Bi-directional
<b>Device ↔ OVOC Server (NTP Server)</b>	UDP (NTP server)	✗	123	NTP server synchronization. Initiator: MG (and OVOC Server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-directional
<b>Device ↔ OVOC Server</b>	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

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
<b>Device↔ OVOC Server Floating License Management</b>	TCP (HTTPS)	✓	443	HTTPS connection for files transfer (upload and download) and REST communication for device Floating License Management. Initiator: Device	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
<b>Endpoints (IP Phones)</b>					
<b>OVOC Server ↔ IP Phone Manager Pro</b>	TCP (HTTP)	✖	80	HTTP connection between the OVOC server and the IP Phone 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 (HTTPS)	✓	443	HTTPS connection between the OVOC server and the IP Phone Manager Pro Web browser. Initiator: Client browser	OVOC server side / Bi-Directional.
				HTTPS connection used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoints	

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
<b>OVOC Server ↔ Endpoints (IP Phones)</b>	TCP (HTTP)	x	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)	x	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

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	TCP (HTTPS)	✓	8082	<p>HTTPS REST updates connection (encryption only without SSL authentication). 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 443 to 8082 in the phone's configuration file.</p> <p>Initiator: Endpoint</p>	OVOC server side / Bi-directional



Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
<b>OVOC Voice Quality Package Server and Devices</b>					
<b>Media Gateways ↔ Voice Quality Package</b>	TCP	×	5000	XML based SEM communication carrying CDR and SIP call dialog messages. Initiator: Media Gateway	OVOC server side / Bi-directional
	TCP (TLS)	✓	5001	XML based Tomcat TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device	OVOC server side / Bi-directional
<b>Statistics Reports</b>					
<b>Statistics Reports client page ↔ Tomcat server</b>	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

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
<b>Skype for Business MS-SQL Server</b>					
<b>OVOC Voice Quality Package server ↔ Skype for Business MS-SQL Server</b>	TCP	✓	1433	Connection between the OVOC server and the MS-SQL Skype for Business Server. This port should be configured with SSL. Initiator: OVOC server	Skype for Business SQL server side / Bi-directional
<b>LDAP Active Directory Server</b>					
<b>OVOC Voice Quality Package server ↔ Active Directory LDAP server (Skype for Business user authentication)</b>	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
<b>OVOC server ↔ Active Directory LDAP server (OVOC user authentication)</b>	TCP	✗	389	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users). Initiator: OVOC server	Active Directory server side/ Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	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
<b>RADIUS Server</b>					
<b>OVOC server ↔ RADIUS server</b>	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
<b>AudioCodes Cloud License Manager (CLM)</b>					
<b>OVOC server ↔ Cloud License Manager (CLM)</b>	TCP	✓	443	HTTPS for OVOC/ Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi-directional
<b>OVOC HA (not supported in this release)</b>					
<b>Primary OVOC Server ↔ Secondary OVOC Server (HA Setup)</b>	TCP	✗	7788	Database replication between the servers. Initiator: Both servers	Both OVOC servers / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	UDP	×	694	Heartbeat packets between the servers. Initiator: Both servers	
<b>Mail and Syslog Servers</b>					
<b>OVOC server ↔ Mail Server</b>	TCP	×	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional
<b>OVOC server ↔ Syslog Server</b>	TCP	×	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side / Bi-directional
<b>RFC 6035</b>					
<b>OVOC Voice Quality Package server ↔ Endpoints</b>	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

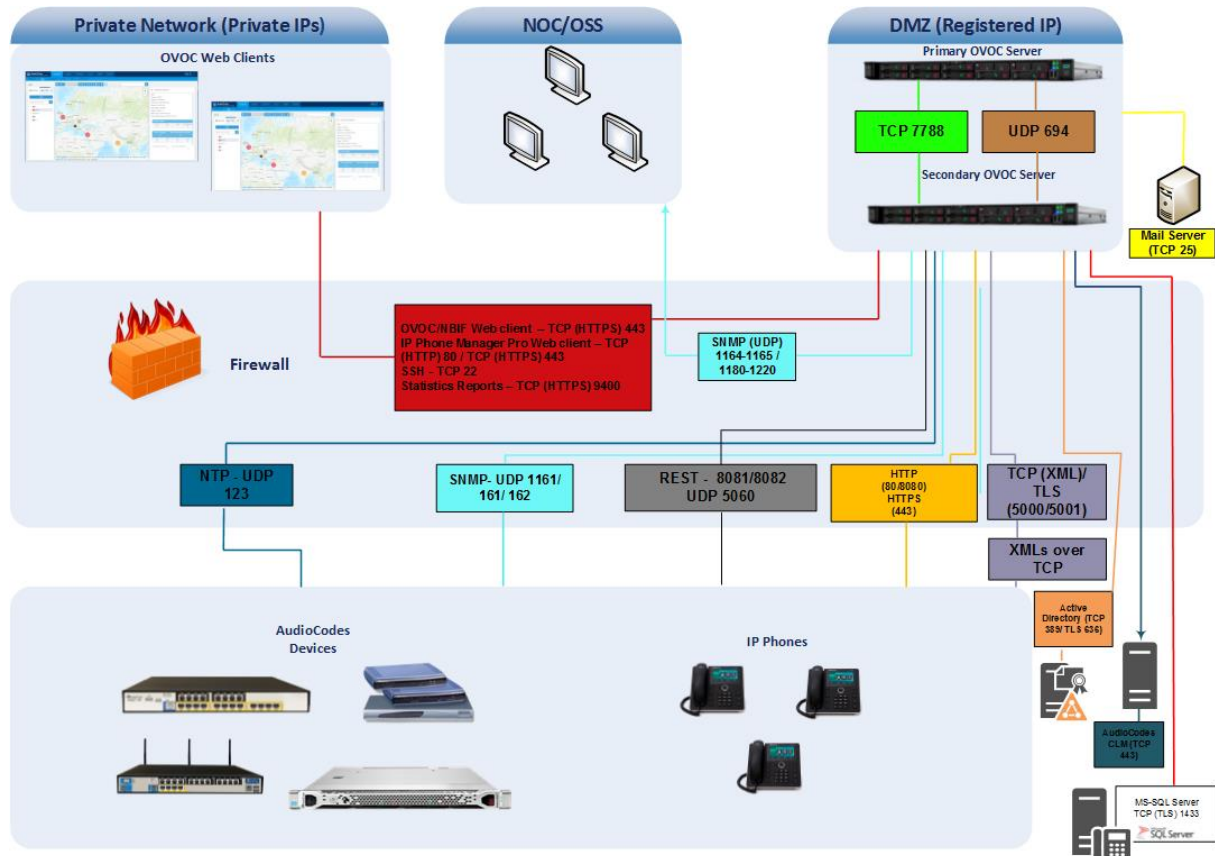
Table 22-2: OAM Flows: NOC/OSS → OVOC

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 22-3: 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 22-1: Firewall Configuration Schema



**Note:** The above figure displays images of devices. For the full list of supported products, see Chapter 2.

# Part VII

## Appendix

This part describes additional OVOC server procedures.





# A

## Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen8 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.



**Note:** This procedure erases any residual data on the designated disk drives.

### A.1 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.

### A.2 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 A-1: Hardware Preparation**



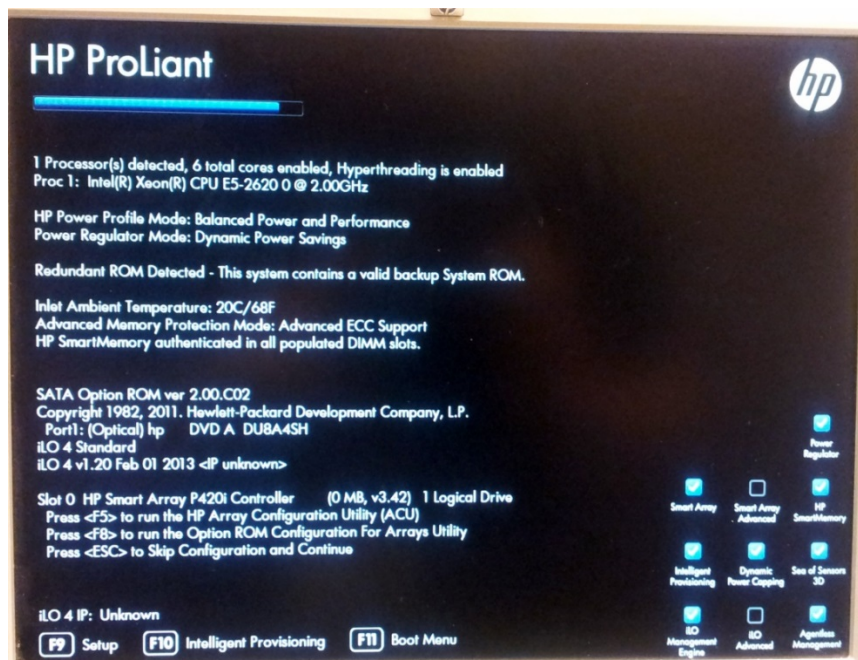
## A.3 Configuring RAID-0

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:

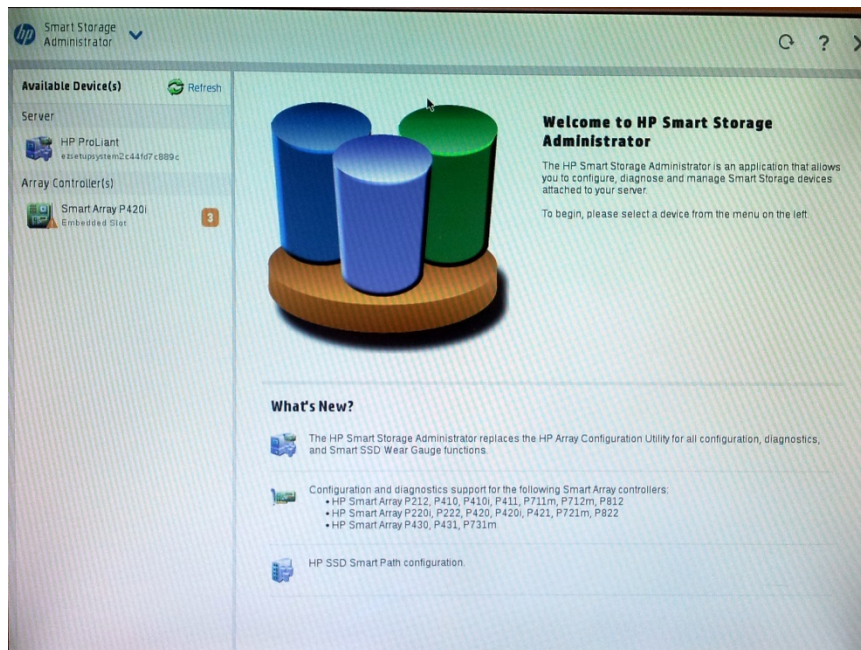
Figure A-2: HP Array Configuration Utility (ACU)



3. Press <F5> to run the HP Array Configuration Utility (ACU).
4. Wait for the ACU to finish loading.

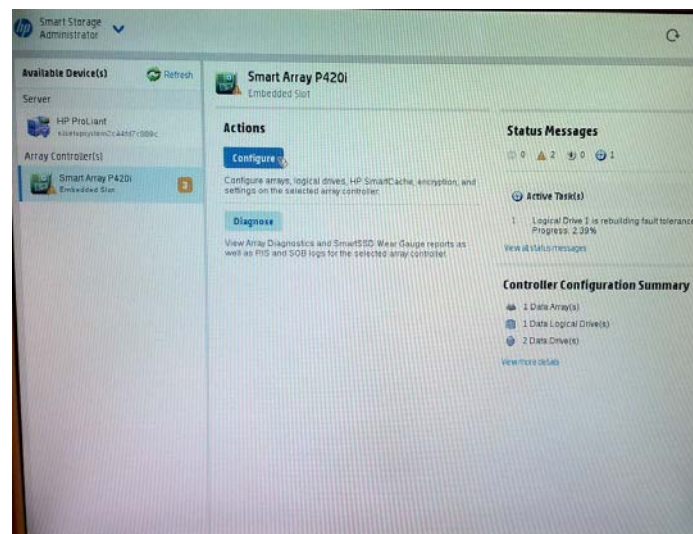
When the ACU is ready, the following screen is displayed:

**Figure A-3: RAID-Latest Firmware Versions**



5. In the left-hand pane, select **Smart Array P420i**; an Actions menu is displayed:

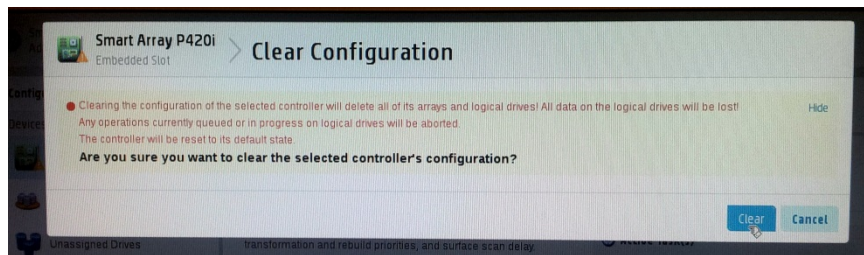
**Figure A-4: Actions Menu**





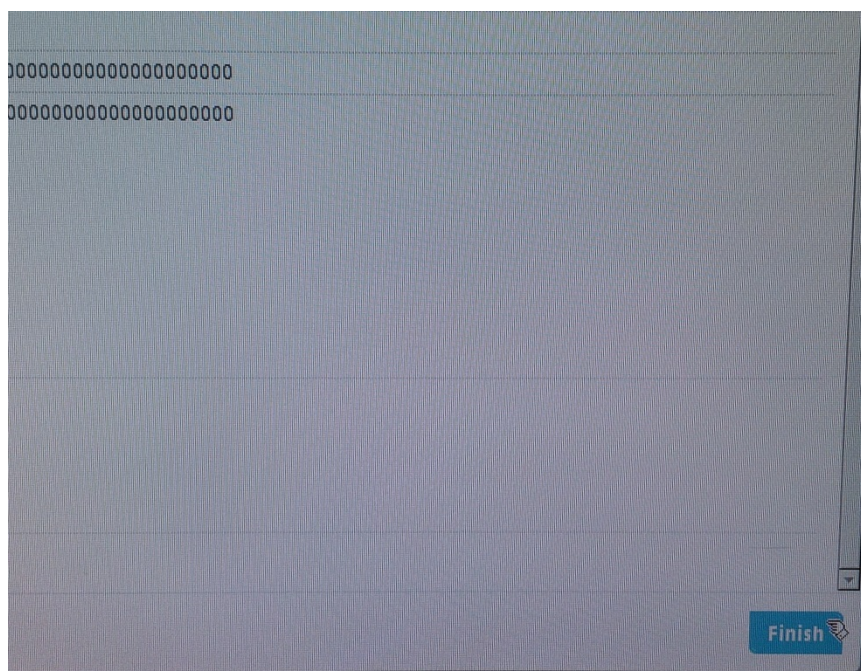
6. Click **Configure**, and then click **Clear Configuration** to clear any previous configuration; the following confirmation is displayed:

**Figure A-5: Clear Configuration**



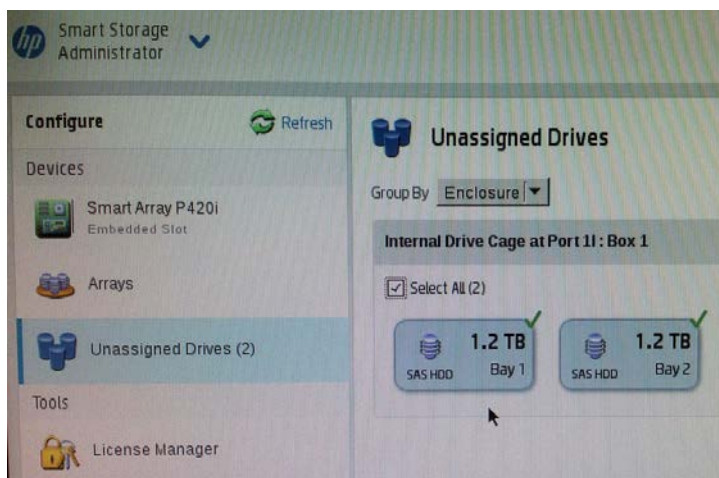
7. Click **Clear** to confirm; a summary display appears:

**Figure A-6: Summary Screen**



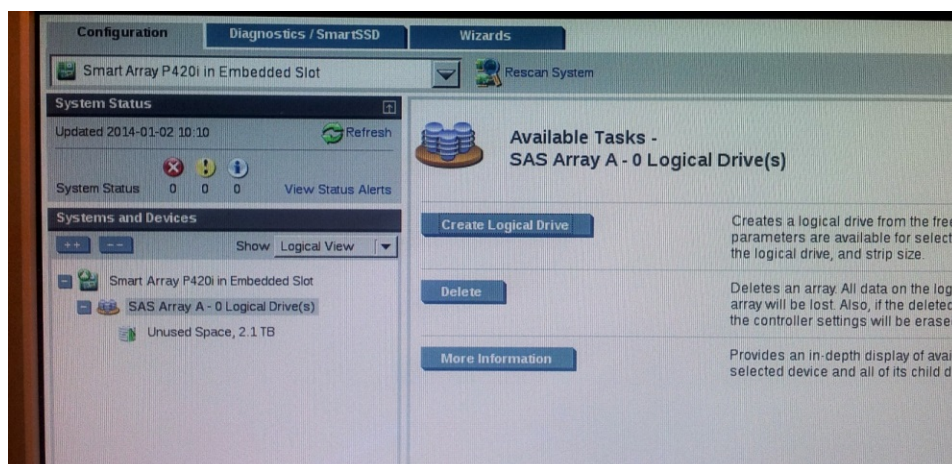
8. Click **Finish** to return to the main menu. The following screen is displayed:

**Figure A-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 A-8: Logical Drive**

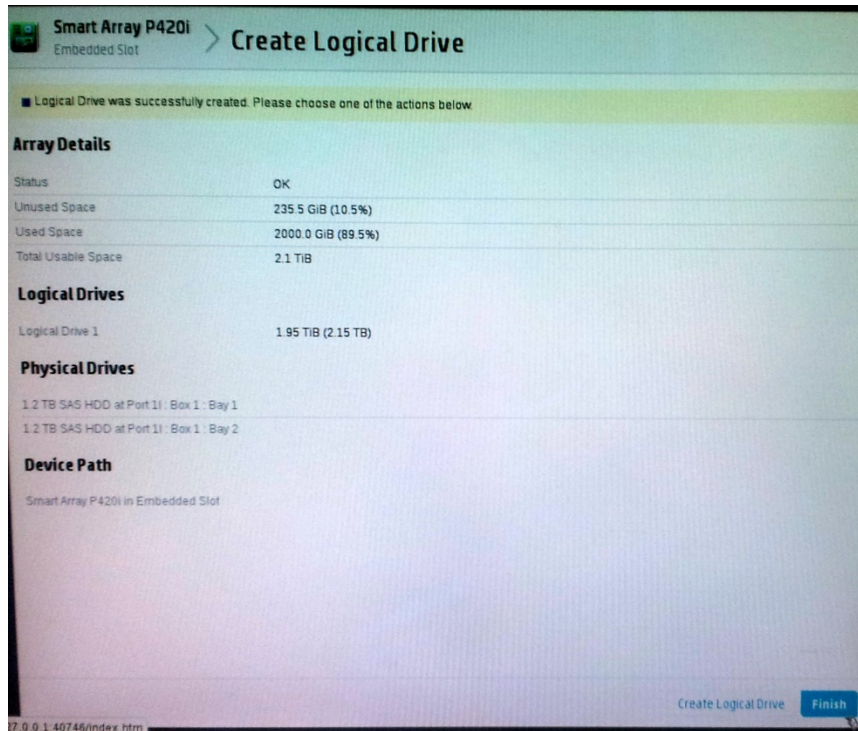


After the array is created, a logical drive should be created.

13. Click **Create Logical Drive**.

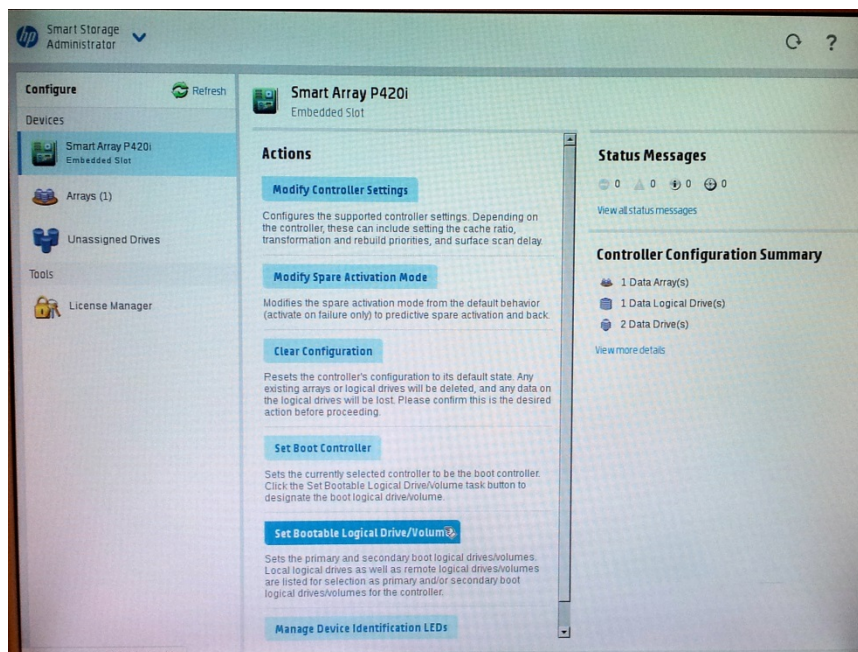
A summary screen is displayed:

**Figure A-9: Summary Screen**



14. Click **Finish**.

**Figure A-10: Set Bootable Logical Drive/Volume**

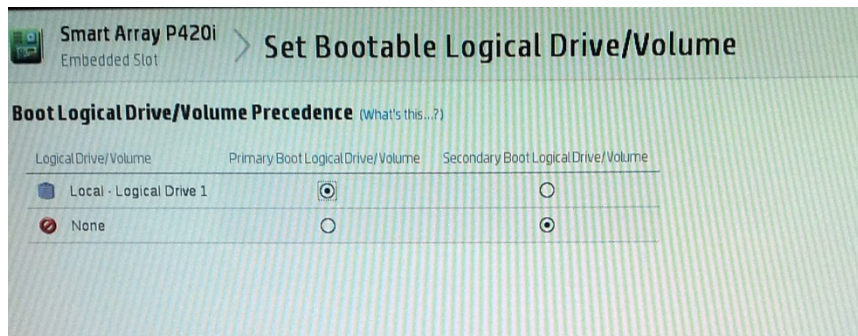




The new logical volume needs to be set as a bootable volume.

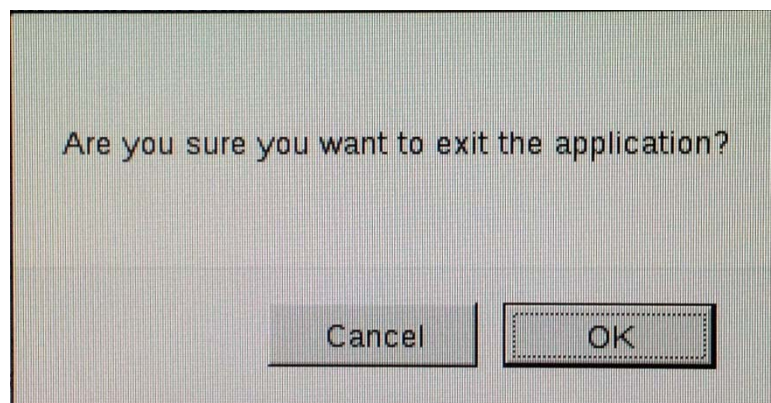
15. In the left-hand pane, select **Smart Array P420i**, and then click **Set Bootable Logical Drive/Volume**; the following screen is displayed:

**Figure A-11: Set Bootable Logical Drive/Volume**



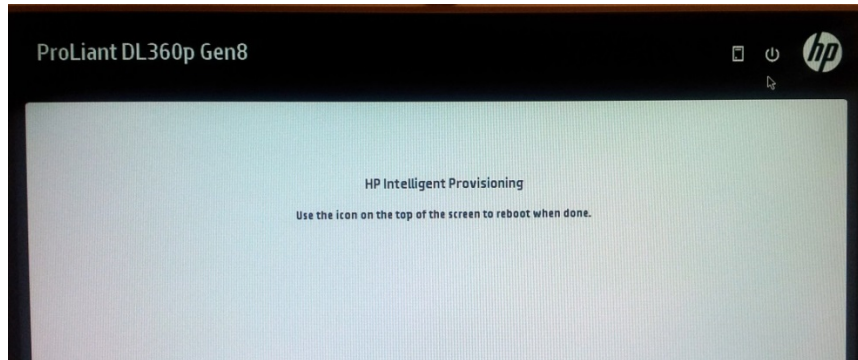
16. Select the "Local - Logical Drive 1" as **Primary Boot Logical Drive/Volume**, and then click **Save**.  
A summary window is displayed.
17. Click **Finish**.
18. Exit the ACU by clicking the **X** sign on the top right-hand side of the screen, and then confirm the following dialog:

**Figure A-12: Exit Application**



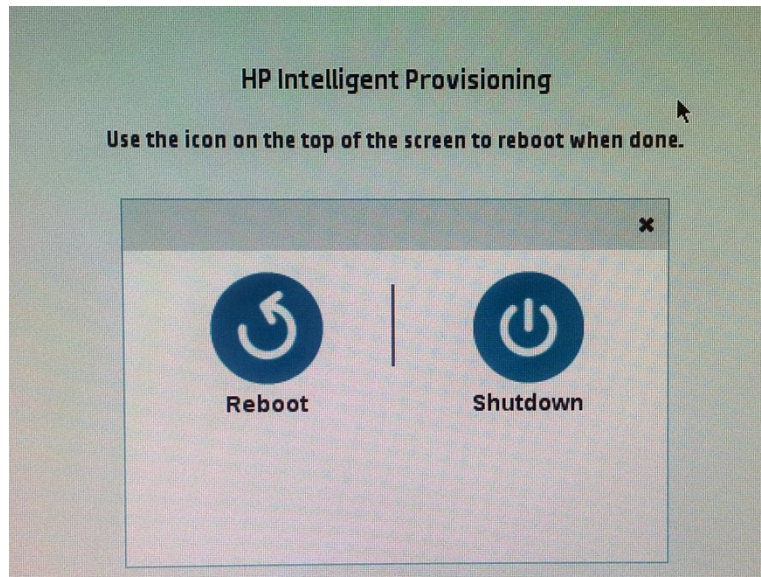
19. Click **Exit ACU** at the bottom left-hand corner of the screen; the following screen is displayed:

**Figure A-13: Power Button**



20. Click the **Power** icon in the upper right-hand corner of the screen. The following screen is displayed:

**Figure A-14: Reboot Button**



21. Click **Reboot** to reboot the server.  
The Disk Array configuration is now complete.
22. Install the OVOC server installation (see Chapter 6).



## B Managing Clusters

This appendix describes how to manually migrate or move OVOC VMs to another cluster node.

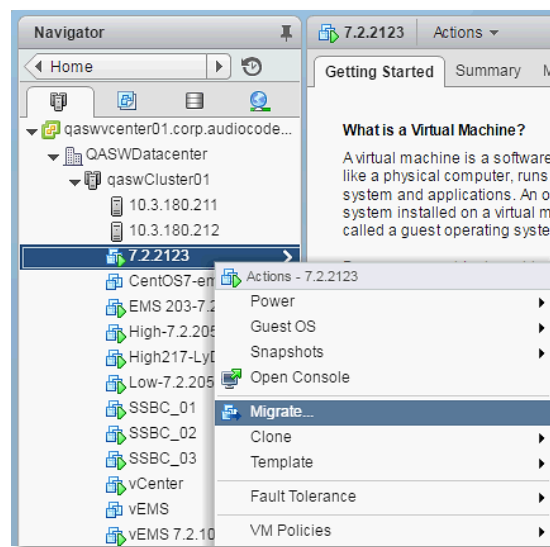
### B.1 Migrating OVOC Virtual Machines in a VMware Cluster

This section describes how to migrate your OVOC Virtual Machine from one ESXi host to another.

➤ **To migrate your OVOC VM:**

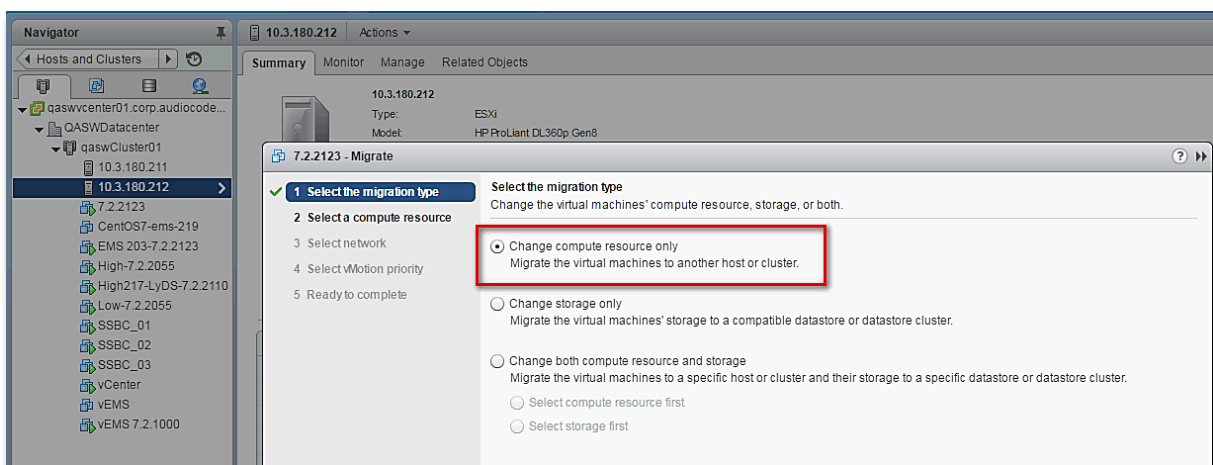
1. Select the OVOC VM that you wish to migrate and then choose the **Migrate** option:

**Figure B-1: Migration**



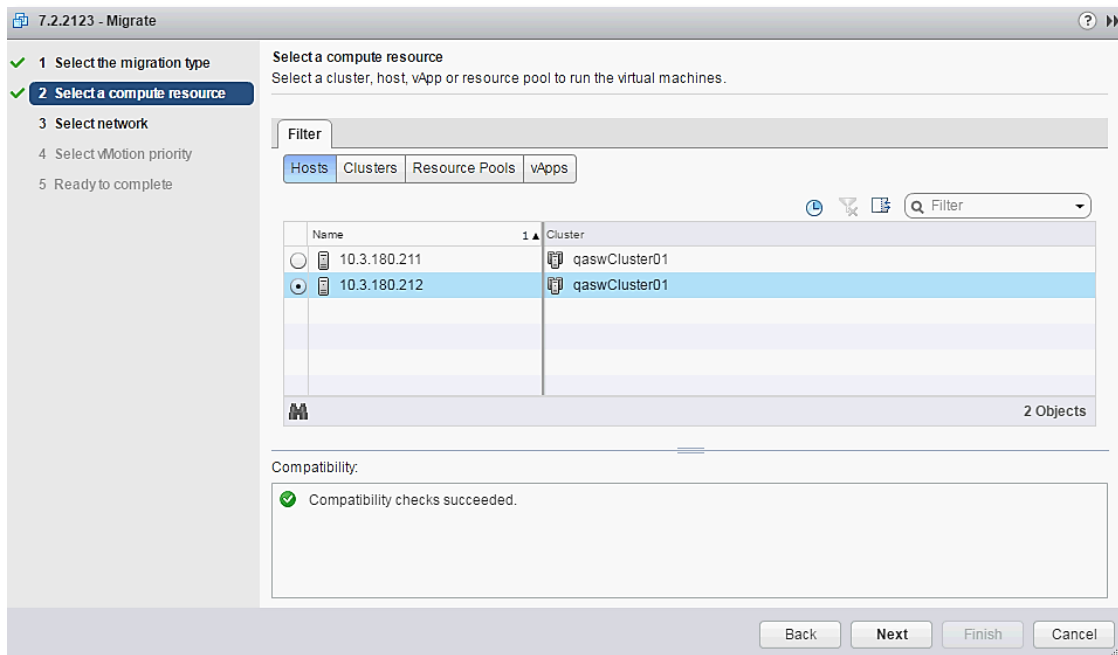
4. Change a cluster host for migration:

**Figure B-2: Change Host**



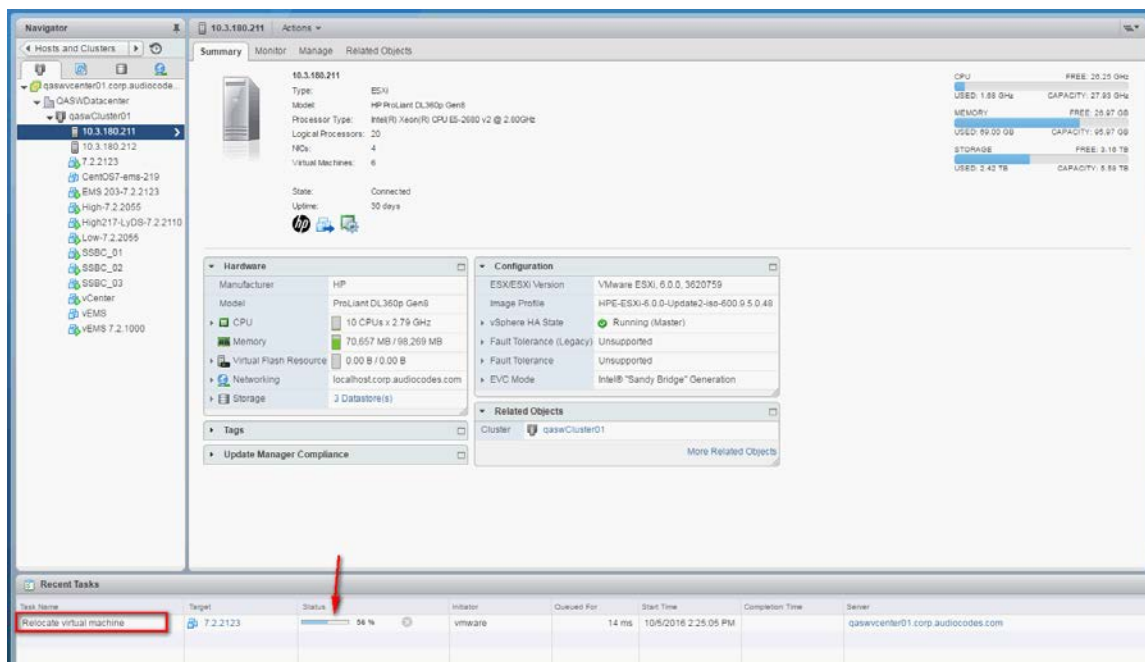
5. Choose the target host for migration:

**Figure B-3: Target Host for Migration**



The migration process commences:

**Figure B-4: Migration Process Started**



After the migration has completed, the OVOC application will run seamlessly on the VM on the new cluster's host.

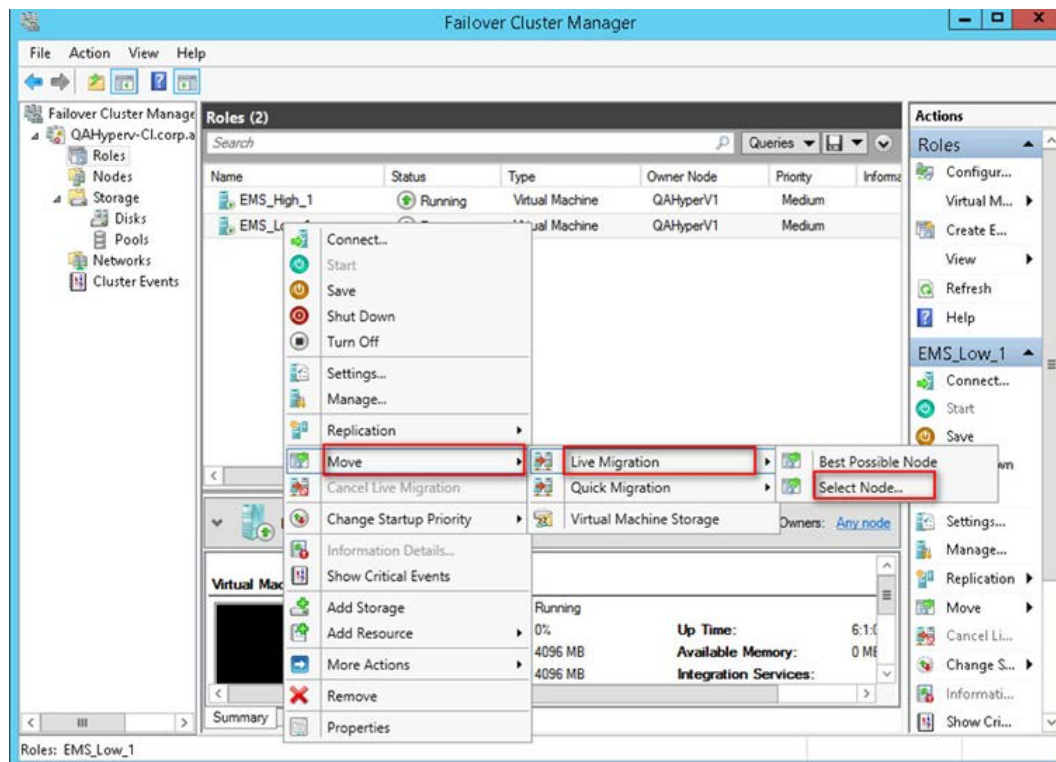
## B.2 Moving OVOC VMs in a Hyper-V Cluster

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:

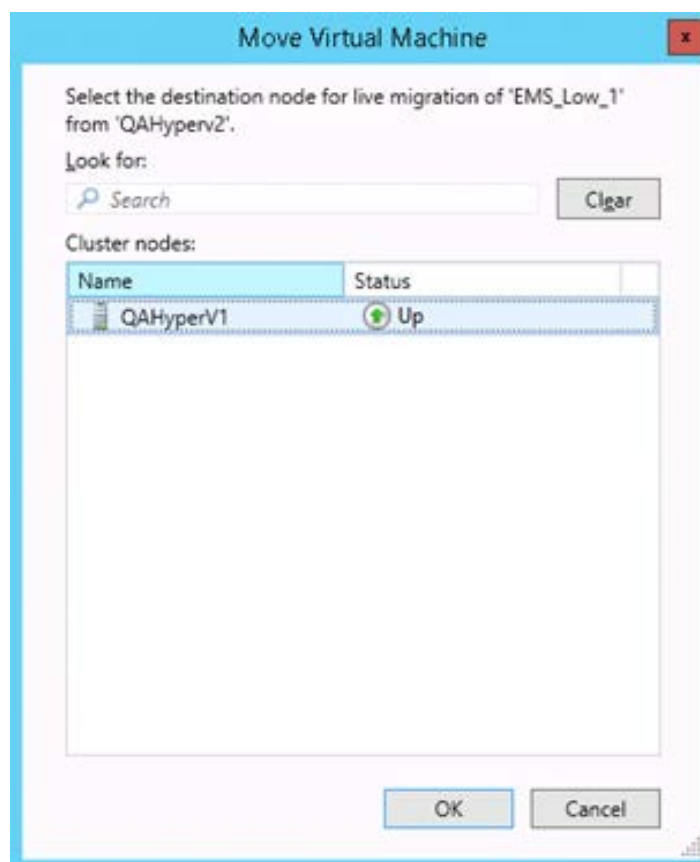
1. Select the Virtual Machine, right-click and from the menu, choose **Move > Live Migration > Select Node**.

Figure B-5: Hyper-V Live Migration



The following screen is displayed:

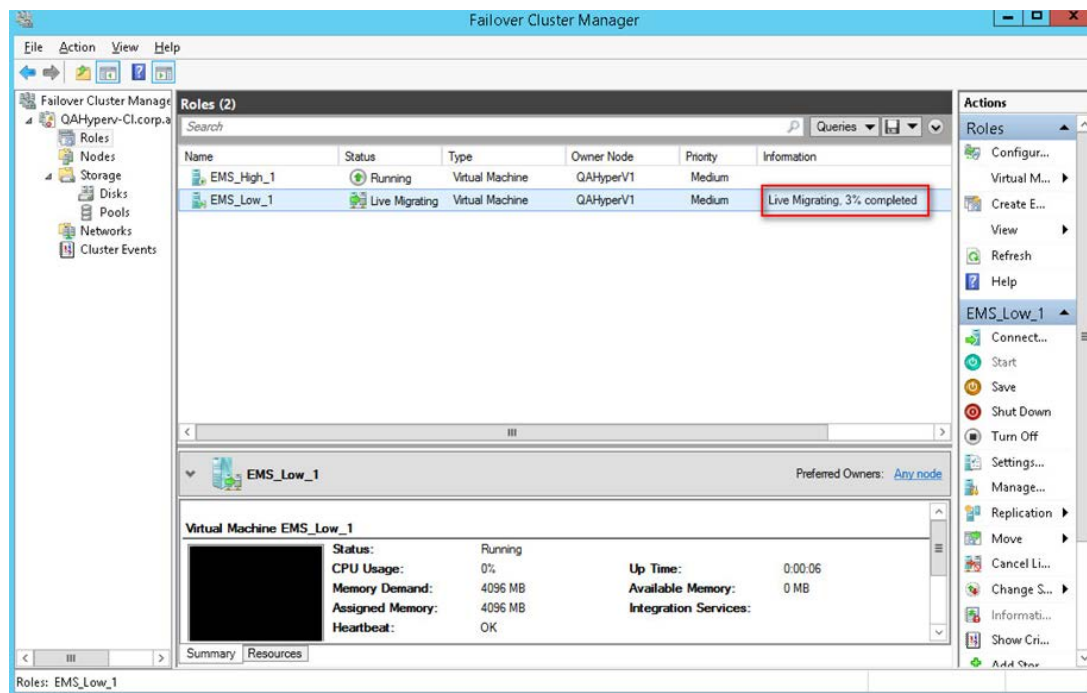
**Figure B-6: Move Virtual Machine**



2. Select the relevant node and click **OK**.

The migration process starts.

**Figure B-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.

**This page is intentionally left blank.**

## C Supplementary Security Procedures

The procedures in this appendix describe supplementary procedures for completing the setup of X.509 Custom certificates.



**Note:** 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 (see Section [C.1](#))
- Cleaning up Temporary files on the OVOC server (see Section [C.2](#))

### C.1 Installing Custom Certificates on AudioCodes Devices

This section describes how to install Custom certificates on AudioCodes 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 (see Section [C.1.1](#)).
- MP-1xx devices (see Section [C.1.2](#)).



**Note:**

- 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 AudioCodes 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).

## C.1.1 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**.

### C.1.1.1 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**).
3. 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 C-8: Context Certificates**

⊕ TLS Context [#0] > Context Certificates

CERTIFICATE SIGNING REQUEST

Subject Name [CN]	<input style="width: 90%;" type="text"/>
Organizational Unit [OU] <i>(optional)</i>	<input style="width: 90%;" type="text" value="Headquarters"/>
Company name [O] <i>(optional)</i>	<input style="width: 90%;" type="text" value="Corporate"/>
Locality or city name [L] <i>(optional)</i>	<input style="width: 90%;" type="text" value="Poughkeepsie"/>
State [ST] <i>(optional)</i>	<input style="width: 90%;" type="text" value="New York"/>
Country code [C] <i>(optional)</i>	<input style="width: 90%;" type="text" value="US"/>
Signature Algorithm	<input style="width: 90%;" type="text" value="SHA-1"/> ▼

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 C-9: Certificate Signing Request Group

5. Copy the text and send it to the certificate authority (CA) to sign this request.

### C.1.1.2

## 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-----
MIIBuTCCASKgAwIBAgIFAKKlMbGwDQYJKoZIhvcNAQEFBQAwFzEVMBMGAlUEAxMM
RUl1TIFJPTlQgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTE1MDUwMzA4NTE0MFowKjET
...
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEExNJol0
L6V81lzUYOfHrEiq/6g==
-----END CERTIFICATE-----
```



### Notes:

- 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.

### C.1.1.3 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 C-10: 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

**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.

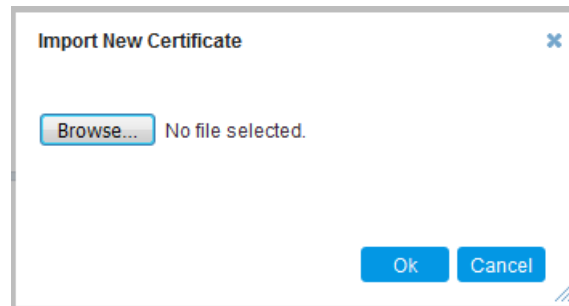
Send File

### C.1.1.4 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 C-11: Importing Certificate into Trusted Certificates Store**

4. If you received intermediary CA certificates – ca1.crt, ca2.crt, etc. – import them in a similar way.

### C.1.1.5 Step 5: Configure HTTPS Parameters on the Device

This section describes how to configure HTTPS related parameters on the device.



**Note:**

- 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 (see Section 20.10.3), add the following parameter.

```
QOENABLETLS=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 C-12: TLS Contexts: Edit Record**

The screenshot shows the 'TLS Contexts: Edit Record' form. The form is titled 'TLS Contexts [default]' and has two tabs: 'GENERAL' and 'OCSP'. The 'GENERAL' tab is active, showing fields for Index (0), Name (default), TLS Version (Any - Including SSLv3), DTLS Version (Any), Cipher Server (RC4:AE5128), Cipher Client (RC4:DEFAULT), Strict Certificate Extension Validation (Disable), and DH key Size (1024). The 'OCSP' tab is also visible, showing fields for OCSP Server (Disable), Primary OCSP Server, Secondary OCSP Server, OCSP Port (2560), and OCSP Default Response (Reject). At the bottom, there are 'Cancel' and 'APPLY' buttons.

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**.

### C.1.1.6 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 C-13: Device Reset**

The screenshot displays the AudioCodes web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. Below it, a secondary bar shows 'IP NETWORK', 'SIGNALING & MEDIA', 'ADMINISTRATION', and a highlighted 'Save' button. The left sidebar contains a 'TIME & DATE' section and a 'MAINTENANCE' section with options like 'Configuration File', 'Auxiliary Files', 'Maintenance Actions' (selected), 'License Key', and 'Software Upgrade'. The main content area, titled 'Maintenance Actions', is divided into two panels. The 'RESET DEVICE' panel features a 'Reset Device' button (labeled 'Reset'), a 'Save To Flash' dropdown set to 'Yes', and a 'Graceful Option' dropdown set to 'No'. The 'LOCK / UNLOCK' panel features a 'Lock' button (labeled 'LOC'), a 'Graceful Option' dropdown set to 'No', and a 'Gateway Operational State' set to 'UNLOCKED'. Below these panels, two paragraphs provide additional context: 'For Reset Device' states that changes will be lost if not saved to flash, and 'For Save Configuration' notes that saving to flash may cause temporary voice quality degradation.

2. 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.

### C.1.2 MP-1xx Devices

This section describes how to install Custom certificates on the MP 1xx devices.

### C.1.2.1 Step 1: Generate a Certificate Signing Request (CSR)

This step describes how to generate a Certificate Signing Request (CSR).

➤ **To generate a CSR:**

1. 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.
2. 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.
3. Login to the MP-1xx Web server.
4. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
5. Under the **Certificate Signing Request** group, do the following:
  - a. In the 'Subject Name [CN]' field, enter the DNS name.
  - 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 C-14: 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
<div>Create CSR</div>	

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-----
MIIBtjCCAR8CAQAwdjESMBAGA1UEAxMJYXVkaW8uY29tMRUwEwYDVQQLEwxIZWFk
cXVhcnRlcnMxExJhAQBgNVBAOTCUNvbnVcnBvcnF0ZTEVMBMGA1UEBjMUMGU9
12hr2WVW
c211MRUwEwYDVQQLEiw0ZkcgwW9yazELMAKGA1UEBhMCMVUwmg28wdQYJKoZI
hvcN
AQEBBQADgY0AMIGJAoGBAHPfpf2t4OLy3FRk5Bw7F12FWCKQ7nvuocHtu7Nns071M
xL7Of8Yol63eeIK2eDo8nm6rJ0677z/AHWJmf65pAK1CboIFgoZNS0g6+5JAmJAA
1LNuocqJEsk7CF32uvolH//gfkhy5zleNvobi+25Pn38aJzExc8DkgwZ19rRoqRz
AqMBAAGADANBgkqhkiG9w0BAQQAQBgGDIidqbc1zkhdlFr+5BRusckYgUXBM6
7FGjFXAf2k1MmqnBMC/MyfSGTbawrQF7p6dnJ60divmucPF6gz25m2uqC6LqoIi
nLnQpVcmbdva/B1QyEpPbQhZqpULJ8CseSrrY3ru23AzeDuBvYyho901kRbAp//+3
zvnZze5M5CB3Lg==
-----END CERTIFICATE REQUEST-----

```

6. Copy the text and send it to the certificate authority (CA) to sign this request.

### C.1.2.2 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
JGUjETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBT
ZXJ2ZXVYMB4XDTE4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1
UEBhMCRlIxEzARBgNVBAAoTCKNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9z
dGUxG9U2VydmV1cjcCCASEwDQYJKoZIhvcNAQEBBQADggEODCAQkCggEAPqd4Mz
iR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWUL
f7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMyb
FkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Ag3o8pWDguJ
uZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```



#### Notes:

- 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.

### C.1.2.3 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 (see Section C.1.2.6 below).

### C.1.2.4 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-----
MIIDNjCCA6gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVNFQ0EYMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5UgxflPjJeNggnlQiUYhOK
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLdYzZp117J53FIsnCSxpVqcYfMoBbCL/
0fmXKHwLPIIbovWpZddgz8UlpEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwqe4yk
ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR4cu
5B6wYNPOTjJX5OXgd9Yf+0IQYB2EiP06uzLtlYWL3AENGwDVeOvlfZgppLEZPBKI
hfULeMjay4fzE4XnS9LDxZGjJ+nV9oJa7WaRB5tl6nEJQ/7sLQIDAQABo3oweDAM
BgNVHRMEBTADAQH/MB0GA1UdDgQWBBrY2JQ1yZrvN4GifsXUB7AvctWvrTBjBgNV
HSMEQjBAGBTBhf6GbmQbo5b0CkLV8kW+Rg0AAhQElpCMwITEMMAoGA1UEChMDQUNM
MREwDwYDVQQQDFAhFTVNFUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQEAAsYyfcg
TdkF/uDxLOGk0ygXrRAXHG2WFO56afrcJHoZCCH3PNsvftRrEAwroGwx7tsnl/o+
CNV5YalstIz7BDIEIjTzCDRpO9sUsiHqxGuOnNhjLDUoLrelGDC00yiKb4B0hlCq
hiemkXRe+eN7xcg0IfUo78VLTpuFMUhz0Bdn7Tue7QbiSayq2fy2ktHHOyDEKJGO
RUosIqqVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAWZ+V
XoAhN6pH17PMXLpClm9L/MlkVkmf0tp1bPmefrEBlo+np/O8F+P551uH0iOYA6Cc
Cj6oHGLq8RIndA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDNzCCA6gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQKEwNBQ0wx
ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIwMDEwMTAwMDAw
MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQQDFAhFTVNFUk9PVDCCASIdQYJKoZI
hvcNAQEBBQADgGEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FSFhnUQrS
667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEoIs+7/q
ebESJyW8pTLTszGQns2E2l4+U18sKHItPUZvsldVUIX6xQiSYFDG1CDIPR5/70pq
zwtdbIipSsKgYijos0yRV3roVqNi4e+hmLVZA9rOI6LR72Ta9HMFJ4gyxJPUQA
jV3Led2Y4JObvBTnlka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPuf1wRjDWgl4G
BRw2MACYsu/M9z/H821UOICtsZ4oKUJMqbwjQ9lXI/HQkKRSTf8CAwEAAAN6MHgw
DAYDVR0TBAAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYNAAIYwSQYD
VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCExDDAKBgNVBAoTA0FD
TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADgGEBAHqkg4F6
wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFcz1q4QVpQNYAwdBdEAKENznZttoP3aPZE
3EOx1C8Mw2u4pOxD7B6pH0XO+oJ4LrxLB3SAJd5hW495X1RDF99BBA9eGUZ2nXJ
9pin4Pwbnfc8eppq8Tpl8jJMW0Zl3prfPt012q93iEalkDEZX+wxkHGZEqs4ayBn
```



```
8bU3NHt5qh0Egpai8hB/nth1xnA1m841wxCbJW86AMRs2NznROyG695InAYaN1Io
HU9zBRdRRASV5vmBN/q5JnDhshZhL1Bm+M6QxOyGoNjL1DqE+aWZkmsw2k9STOpN
itSUGyGwEagnsMU=
-----END CERTIFICATE-----
```



**Notes:** 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.

### C.1.2.5 Step 5: Configure HTTPS Parameters on Device

- Configure HTTPS Parameters on the device (see Section C.1.1.5 above).

### C.1.2.6 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 C-15: Maintenance Actions Page**

▼ Reset Configuration	
Reset Board	<b>Reset</b>
Burn To FLASH	Yes <input type="button" value="v"/>
Graceful Option	No <input type="button" value="v"/>
▼ LOCK / UNLOCK	
Lock	<b>LOCK</b>
Graceful Option	No <input type="button" value="v"/>
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.

## C.2 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
```

## D Transferring Files

This appendix describes how to transfer files to and from the OVOC server using any SFTP/SCP file transfer application.



**Note:** .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.

**This page is intentionally left blank.**

## E 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
```

**This page is intentionally left blank.**

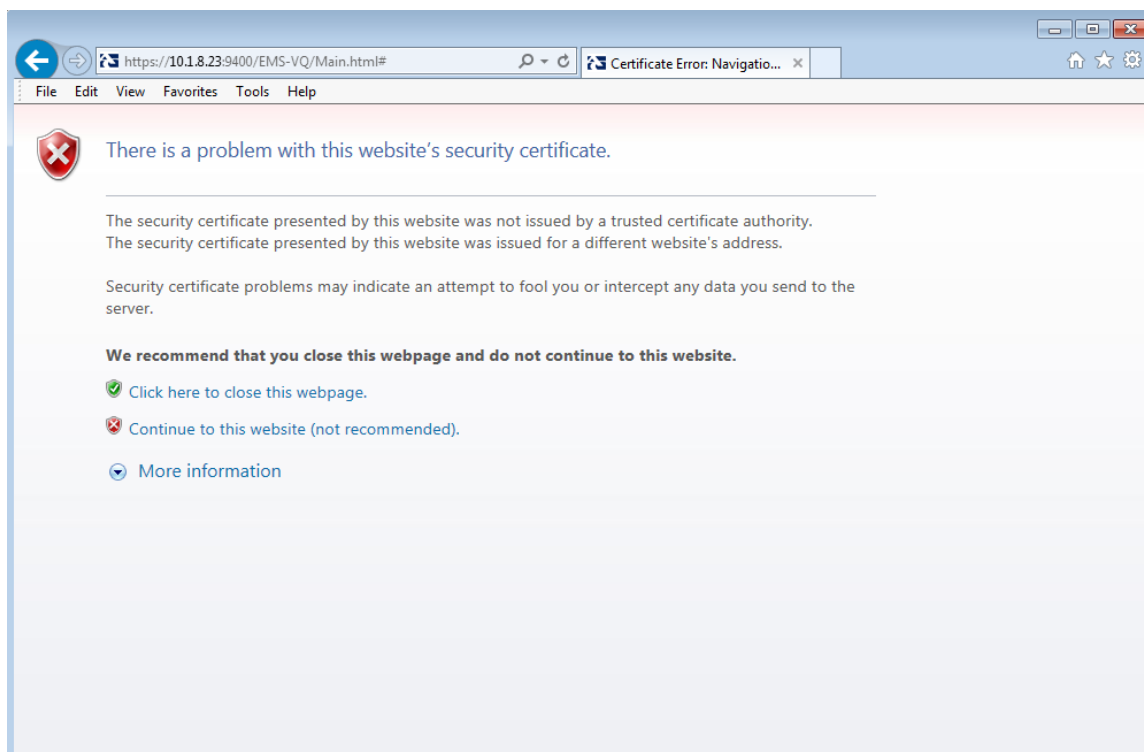
## F Self-Signed Certificates

When using self-signed certificates, use the following instructions for recognizing the secure connection with the OVOC server from your OVOC client browsers.

### F.1 Internet Explorer

When the following screen is displayed, select the “Continue to website (not recommended)” option.

**Figure F-1: Continue to Website**

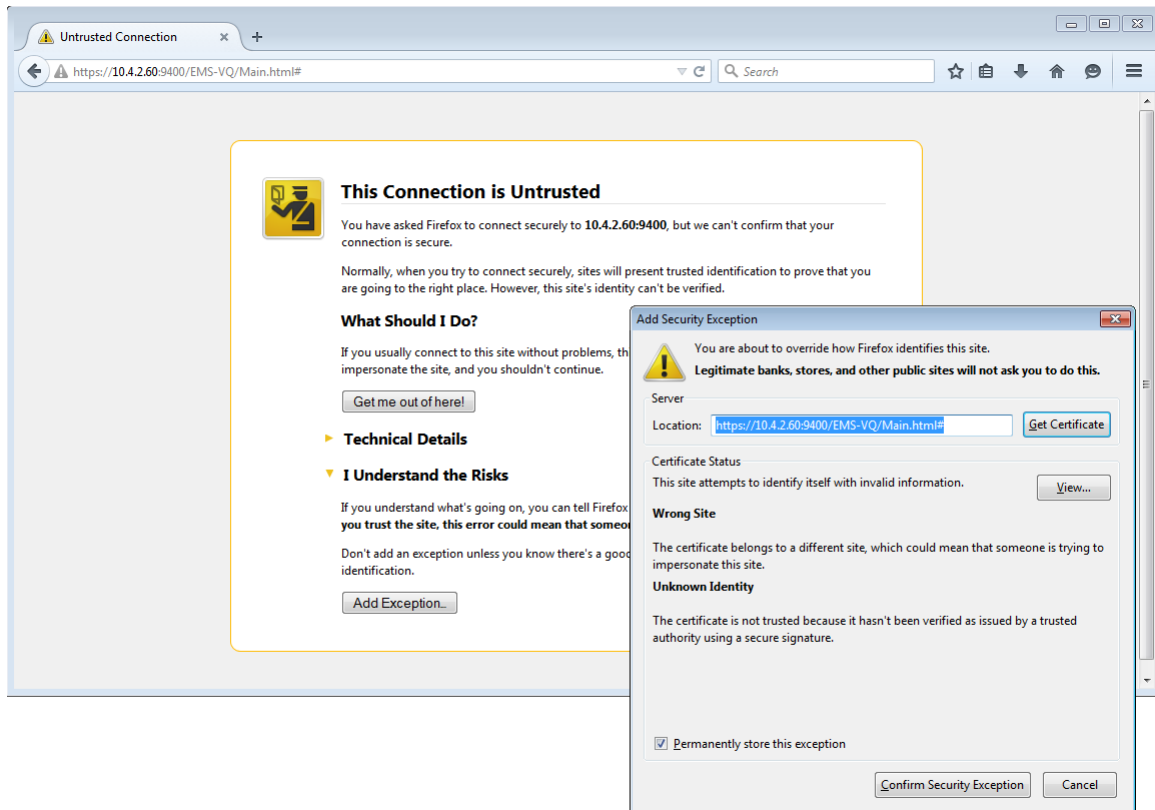


## F.2 Using Mozilla Firefox

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 F-2: Mozilla Firefox Settings

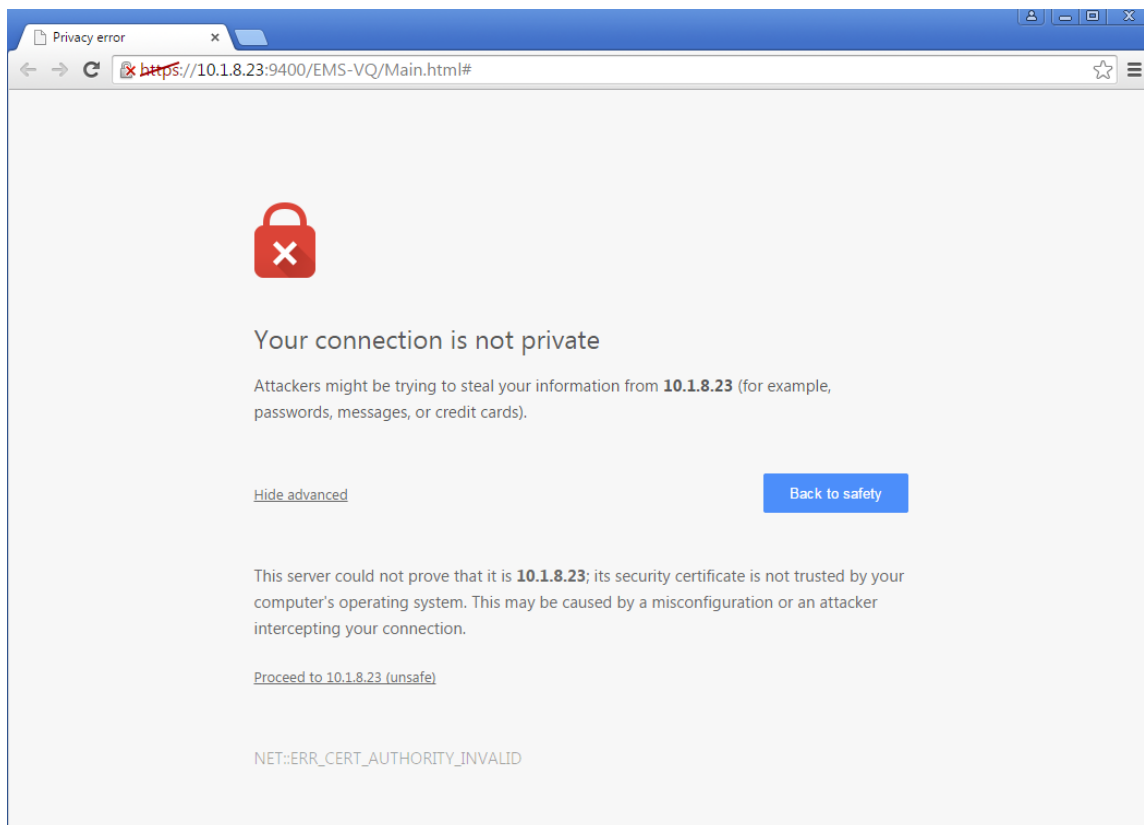




## F.3 Chrome

When the following screen is displayed, click **Advanced** and then click the “Proceed to <Server IP> (unsafe)” link.

**Figure F-3: Chrome Browser Settings**



**This page is intentionally left blank.**

# G Datacenter Disaster Recovery

## G.1 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.



**Note:** Examples shown in this Appendix are for the VMware platform; however, these procedures are also relevant for Hyper-V platform.

## G.2 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.

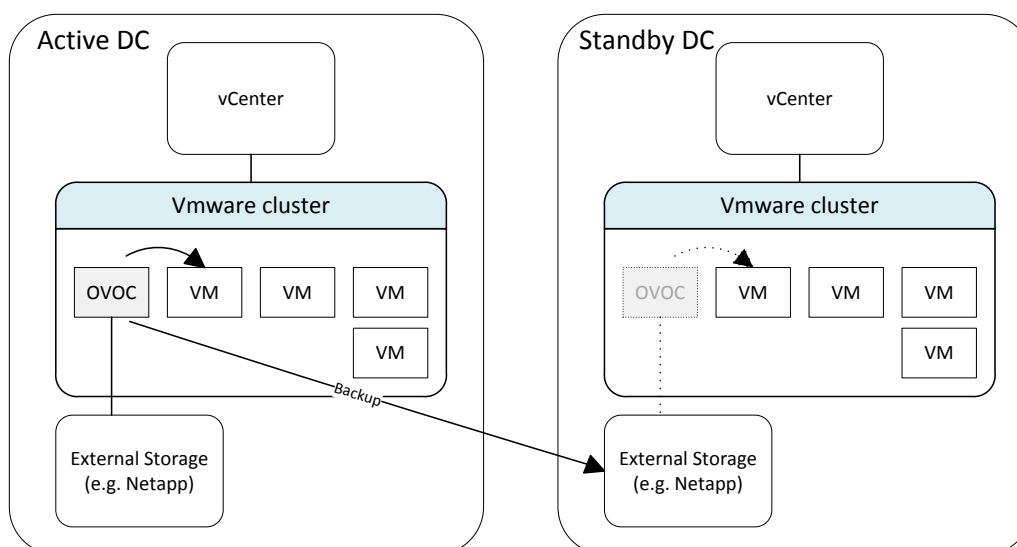
It is recommended that each OVOC machine will have a VMware High Availability (HA) setup to support local Data Center (DC) HA.

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 G-4: Disaster Recovery Between Two Datacenters with VMware HA**



## G.3 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 EMS 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.



**Note:** 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 Chapter 11.

- Make sure that active server backups are not stored on the server machine.

## G.4 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

## G.5 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.

## G.6 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 (see Chapter 12).
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 Static and Floating License Pool customers, run the *Update* command for all the devices which are managed by the pool or CLM.

See the table below summarizing the features affected by Disaster Recovery functionality.

**Table G-1: Features Affected by Disaster Recovery Functionality**

Feature	Status
<b>Management</b>	
Alarms+ NAT communication based on Keepalive traps	Supported
License Pool and CLM	Not Supported
IP Phones Manager Pro: Alarms / Status reports	Not Supported
<b>Advanced Quality Package</b>	
SBC/GW Voice Quality Monitoring	Supported
Endpoint Quality monitoring (RFC 6035)	Not Supported
<b>Server</b>	
Server: Device NTP Server	Supported
Server: Device Syslog Server	Not Supported
Server: Device TP Debug recording server	Not Supported



**Note:** This procedure is intended to be officially tested and released by April 2018 as part of the OVOC 7.4.3000 release.

# H Service Provider - Enhanced Specifications

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 (see Section [H.1](#)).

The following table describes the machine specifications for this platform.

**Table H-1: Service provider custom VMware Hardware Specification**

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 H-2: Service Provider - Enhanced Capacity**

Item	Capacity
<b>Topology</b>	
OVOC Managed Devices <sup>2</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).	-
<b>Voice Quality</b>	
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

<sup>2</sup> If OVOC links are not used, up to 10,000 devices are supported.

Item	Capacity
Maximum number of devices per region	100
Maximum number of managed devices.	10,000
Call Details Storage - Detailed information per Call (not including Trends)	Up to one year or 250 million calls.
Calls Statistics Storage - Statistic information storage.	Up to one year or 500 million intervals.
IP Phone Manager Pro	
Maximum number of IP Phones managed in OVOC.	-
Maximum number of CAPS per IP Phone	-
<b>Alarms</b>	
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)



## H.1 Required Updates

After machine is installed with the proper OVOC software version, manual changes should be made on the OVOC server machine to support the enhanced capacity as described below:

- Property Files Updates (see Section [H.1.1](#))
- REST API Updates (see Section [H.1.2](#))
- Database Updates (see Section [H.1.3](#))

### H.1.1 Property Files Updates

The changes described below are preserved in the event of OVOC server restart; however, should be re-applied if the software is upgraded because the property files are located under the version installation folder.

➤ **Do the following:**

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

```
su - root
```

3. Update the devices messages queue max allocation:

- a. Open the file:

```
/opt/ACEMS/server_7.4.2094/externals/configurationProperties/acVQMConfig.properties.
```

- b. Update as follows:

```
TOTAL_BUFFER_SIZE = 800000000
```

4. Disable the firewall on Voice Quality Package ports 5000/5001:

- a. Open the file `/opt/ACEMS/server_7.4.2094/runVQServer_unix`.

- b. Disable the following rows:

```
set ipt_isdown=(`iptrulecnt` == 0)
if ($ipt_isdown) then
    csh runFwRules_unix &
endif
```

5. Increase the size of the OVOC server Log file:

- a. Open the file

```
/opt/ACEMS/server_7.4.2094/externals/configurationProperties/serverLog4j.xml.
```

- b. For each log file defined in this file, update the "MaxFileSize" parameter as follows:

```
<param name="MaxFileSize" value="300000KB"/> value
```

6. Increase the maximal number of DB rows for Statistics reports calculation:
  - a. Open the file:  
/opt/ACEMS/server\_7.4.2094/externals/configurationProperties/serverGeneralConfig.properties
  - b. Update as follows:
 

```
maxRowCountForReports 10000000
```
7. Increase the maximum concurrent calls ("ServerMaxLoad" parameter) allowed on the OVOC server:
  - a. Open the file  
/opt/ACEMS/server\_7.4.2094/externals/configurationProperties/acVQMConfig.properties.
  - b. Update as follows:
 

```
ServerMaxLoad=500000
```
8. Increase the number of threads for polling device status:
  - a. Open file /opt/ACEMS/server\_7.4.2094/externals/configurationProperties/pollingTime.properties file.
  - b. Update as follows:
 

```
mpStatusGroupSize 200
```

## H.1.2 REST API Updates



**Note:** The changes described below are preserved in the event of OVOC server restart or software upgrade.

1. Change the OVOC server configuration via a REST API client to increase the client refresh period:
  - a. Open a REST API client such as ARC or Postman.
  - b. Specify the following URL with Content-Type: application/json with PUT method and "system admin" credentials:

```
Command URL: PUT /ovoc/v1/settings/UI/general
JSON:
{
    "clientRefreshTime": 300
}
```

### H.1.3 Database Updates

The changes described in this section are performed using SQL\*Plus.



**Note:** The changes described below are preserved in the event of an OVOC server restart or software upgrade.

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

```
su - root
```
3. Switch user to oracle user (password not required):  

```
su - oracle
```
4. Login to sqlplus as sysdba:  

```
sqlplus / as sysdba
```
5. Copy the following SQL commands to Notepad and then paste to the SQL\*Plus command line.

```

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS17.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS17.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS18.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS18.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS19.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS19.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS20.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS20.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS21.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS21.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS22.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS22.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS23.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS23.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS24.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS24.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS25.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS25.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS26.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS26.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS27.dbf' SIZE
1000M;

```

```
ALTER DATABASE DATAFILE '/data/oradata/EMS27.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS28.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS28.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS29.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS29.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS30.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS30.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS31.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS31.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS" ADD DATAFILE '/data/oradata/EMS32.dbf' SIZE
1000M;
ALTER DATABASE DATAFILE '/data/oradata/EMS32.dbf' AUTOEXTEND ON NEXT
250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES9.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES9.dbf' AUTOEXTEND ON
NEXT 250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES10.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES10.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES11.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES11.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES12.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES12.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES13.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES13.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;
```

```

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES14.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES14.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES15.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES15.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;

ALTER TABLESPACE "EMS_INDEXES" ADD DATAFILE
'/data/oradata/EMS_INDEXES16.dbf' SIZE 500M;
ALTER DATABASE DATAFILE '/data/oradata/EMS_INDEXES16.dbf' AUTOEXTEND
ON NEXT 250M MAXSIZE 32767M;

create index CURR_ALARM_STATUS1 on
EMSADMIN.CURRENT_ALARMS(ALARM_STATUS) tablespace EMS_INDEXES;

alter table EMSADMIN.NODES_SUMMARY drop constraint PK_NODES_SUMMARY;
alter table EMSADMIN.LINKS_SUMMARY drop constraint PK_LINKS_SUMMARY;
alter table EMSADMIN.SITES_SUMMARY drop constraint PK_SITES_SUMMARY;
alter table EMSADMIN.IPPHONES_SUMMARY drop constraint
PK_IPPHONE_SUMMARY;
alter table EMSADMIN.USER_SUMMARY drop constraint PK_USERS_SUMMARY;

create unique index EMSADMIN.PK_NODES_SUMMARY1 on
EMSADMIN.NODES_SUMMARY (NODE_ID, TIME_STAMP) local tablespace
EMS_INDEXES;
create unique index EMSADMIN.PK_LINKS_SUMMARY1 on
EMSADMIN.LINKS_SUMMARY (LINK_ID, TIME_STAMP) local tablespace
EMS_INDEXES;
create unique index EMSADMIN.PK_SITES_SUMMARY1 on
EMSADMIN.SITES_SUMMARY (SITE_ID, TIME_STAMP) local tablespace
EMS_INDEXES;
create unique index EMSADMIN.PK_IPPHONE_SUMMARY1 on
EMSADMIN.IPPHONES_SUMMARY (NODE_ID, TIME_STAMP) local tablespace
EMS_INDEXES;
create unique index EMSADMIN.PK_USERS_SUMMARY1 on
EMSADMIN.USER_SUMMARY (USER_ID, SUMMARY_SOURCE_TYPE, TIME_STAMP) local
tablespace EMS_INDEXES;

alter system set db_recovery_file_dest_size =900G scope=spfile;
ALTER SYSTEM SET SGA_TARGET=24G SCOPE=SPFILE

```

## 6. Restart the OVOC server.

**This page is intentionally left blank.**

**International Headquarters**

1 Hayarden Street,  
Airport City  
Lod 7019900, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

27 World's Fair Drive,  
Somerset, NJ 08873  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

**Contact us:** <https://www.audiocodes.com/corporate/offices-worldwide>

**Website:** [www.audiocodes.com](http://www.audiocodes.com)

©2018 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 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-94161

