AudioCodes One Voice Operations Center

OVOC

Installation, Operation and Maintenance

Version 8.0

audiocodes

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: March-25-2021

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes

Document Name
OVOC Documents
Migration from EMS and SEM Ver. 7.2 to One Voice Operations Center
One Voice Operations Center IOM Manual
One Voice Operations Center Product Description

Document Name
One Voice Operations Center User’s Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center Alarms Monitoring Guide
One Voice Operations Center Performance Monitoring Guide
One Voice Operations Center Security Guidelines
One Voice Operations Center Integration with Northbound Interfaces
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Agent Installation and Configuration Guide
ARM User’s Manual
Documents for Managed Devices
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500Li MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User’s Manual
Mediant 800 MSBR User’s Manual
Mediant 1000B Gateway and E-SBC User’s Manual
Mediant 1000B MSBR User’s Manual
Mediant 2600 E-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

Document Revision Record

LTRT	Description
94179	Updated Section: Managed VoIP Equipment; Hardware and Software Specifications; OVOC Capacities; Viewing Process Statuses; Before Enabling Cloud Architecture Mode; Upgrading OVOC Server on Amazon AWS and Microsoft Azure; Full Restore; OVOC License; Configuring the Firewall; Update to HTTPS SSL TLS Security diagram "Specifications for Service Provider Cluster Mode" merged with Section "OVOC Capacities" Added Section: Before Upgrading on Microsoft Azure; AWS Post Upgrade procedure; Step 4 Registering Microsoft Teams Application; Step 5 Configuring Microsoft Graph Permissions; Step 6 Configuring AudioCodes Azure Active Directory
94180	Update to the OVOC Capacities table.

Table of Contents

1 Overview

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

Part I

Pre-installation Information

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

2 Managed VoIP Equipment

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

Table 2-1: Managed VoIP Equipment

Product	Supported Software Version
Gateway, SBC and MSBR Devices	
Mediant 9000 SBC	Versions **7.4.100**, 7.4, 7.2 (including support for MTC), 7.0, 6.8
Mediant 4000 SBC	Versions **7.4.100**,7.4, 7.2, 7.0 and 6.8
Mediant 4000B SBC	Versions **7.4.100**,7.4 , 7.2, 7.0
Mediant 2600 E-SBC	Versions **7.4.100**, 7.4 , 7.2, 7.0 and 6.8
Mediant 2600B E-SBC	Versions **7.4.100**, 7.4, 7.2 and 7.0
Mediant Software (Server Edition) SBC	Versions **7.4.100,** 7.4, 7.2, 7.0 and 6.8
Mediant Software(Virtual Edition) SBC	Versions **7.4.100**, 7.4, 7.2 (including support for MTC), 7.0 and 6.8
Mediant3000 (TP-8410 and TP-6310)	Versions 7.0 and 6.6
Mediant Cloud Edition	Version **7.4.100**, 7.4, 7.2
Mediant 2000 Media Gateways	Version 6.6
[1]Mediant 1000 Gateway	Version 6.6 (SIP)
Mediant 1000B Gateway and E-SBC	Versions **7.4.100**, 7.4, 7.2, 7.0, 6.8 and 6.6
Mediant 800B Gateway and E-SBC	Versions **7.4.100**,7.4, 7.2, 7.0, 6.8 and 6.6

[1] This product does not support Voice Quality Management.

Product	Supported Software Version
Mediant 800C	Version **7.4.100**, 7.4, 7.2
Mediant 1000B MSBR	Version 6.6
Mediant800 MSBR	Versions **7.23A.356.xxx**, 7.2, 6.8 and 6.6
Mediant500 MSBR	Version **7.23A.356.xxx**, 7.2 and 6.8
Mediant 500L MSBR	Versions **7.23A.356.xxx**, 7.2 and 6.8
Mediant 500Li MSBR	Version 7.20AN.4xx.xxx
Mediant 500 E-SBC	Version **7.4.100** ,7.4, 7.2
Mediant 500L E-SBC	Version **7.4.100,** 7.4, 7.2
[1]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-202	Version 4.4.9 Rev. B, D and R
MP-204	Version 4.4.9 Rev. B, D and R
MP-1288	Version **7.4.100**, 7.4, 7.2
SBA[2]	
Mediant 800B SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.2
Mediant 800C SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.2
Mediant 1000B SBA Skype for Business	SBA version 1.1.12.x and later and gateway Version 7.2
Mediant 2600B SBA Skype for Business	SBA version 1.1.12.x and later

[1] As above

[2] As above

Product	Supported Software Version
	and gateway Version 7.0
Mediant800B SBA Lync Server	SBA version 1.1.12.x and later and gateway Version 6.8
Mediant 1000B SBA Lync Server	SBA version 1.1.12.x and later and gateway Version 6.8
Mediant 2000B SBA devices Lync Server	SBA version 1.1.12.x and later and gateway Version 6.8
CloudBond[1]	
CloudBond 365 Pro Edition	Version 7.6 with MediantServer version 7.2.100 and later
CloudBond 365 Enterprise Edition	Version 7.6 with MediantServer version 7.2.100 and later
CloudBond 365 Standard+ Edition	Version 7.6 with Mediant800BMediant 800CGX-800C version 7.2.100 and later
CloudBond 365 Standard Edition	Version 7.6 with Mediant 800B version 7.2.100 and later
User Management Pack 365 ENT (Check)	Version 8.0.0
User Management Pack 365	Version 7.8
CloudBond 365	Version 8.0.0 (Skype for Business 2019 and Microsoft Teams)
User Management Pack 365 SP (Check)	Version 8.0.100
CCE Appliance[2]	
Mediant 800 CCE Appliance	Version 2.1 with Mediant 800B

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

[2] As above.

Product	Supported Software Version
Mediant Server CCE Appliance	Version 2.1 with Mediant Server
Other Applications	
SmartTAP 360° Recording	Version 4.3, Version 5.0**,** **Version 5.1**
IP Phones	**Supported Software Versions/Models**
Skype for Business	From Version 3.0.0: 420HD, 430HD 440HD and 405HD
	From Version 3.0.1: 420HD, 430HD 440HD, 405HD and 450HD
	From Version 3.0.2: HRS 457 (with Jabra firmware support)
	From **Version 3.1.0**: 445HD, 430HD 440HD, 405HD, 450HD and HRSFrom
	From Version 3.2.0: C450HD
	From **Version 3.2.1**: C450HD, 445HD, 430HD 440HD, 405HD,450HD and HRS
	From **Version 3.4.2**: RX50 Conference Device[1]
Native Teams (Android-based)	■ **From Version 1.8: C470HD, C448HD and C450HD** ■ **From Version 1.9: RXV80** ■ **From Version 1.11 (Preliminary): C435HD**[2]
Third-party Vendor Devices	

[1] This device is not yet supported

[2] This device has not reached GA.

Product	Supported Software Version
Spectralink	Spectralink 8440
Polycom	Polycom Trio 8800
	Polycom VVX 410
Jabra Headset Support	Jabra BIZ, Jabra Coach, Jabra DIAL, Jabra Eclipse, Jabra Elite, Jabra Engage, Jabra Evolve, Jabra Handset, Jabra LINK, Jabra Motion, Jabra Pro, Jabra Pulse, Jabra SPEAK, Jabra Sport, Jabra STEALTH, Jabra Steel, Jabra SUPREME. For a complete list of supported Jabra phones, see document Device Manager for Third-Party Vendor Products Administrator's Manual.

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

3 Hardware and Software Specifications

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

OVOC Server Minimum Requirements

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

Resources	Virtual Platform	Memory	Disk Space	Processors
Low Profile				
VMWare	■ VMware: ESXi 6.7 ■ VMware HA cluster: VMware ESXi 6.5	24 GiB RAM	500 GB	■ 1 core with at least 2.5 GHz ■ 2 cores with at least 2.0 GHz
HyperV	■ Microsoft Hyper-V Server 2016 ■ Microsoft Hyper-V Server 2016 HA Cluster	24 GiB RAM	500 GB	■ 1 core with at least 2.5 GHz ■ 2 cores with at least 2.0 GHz
Azure	VM Size: D8ds_ v4	32 GiB (D8ds_ v4	500 GB SSD	Low Profile: 8 vCPUs (D8ds_ v4
AWS	-	-		-
High Profile				
VMWare	■ VMware: ESXi 6.7 ■ VMware HA cluster: VMware ESXi 6.5	40 GiB RAM	1.2 TB	6 cores with at least 2 GHz

Resources	Virtual Platform	Memory	Disk Space	Processors
HyperV	Microsoft Hyper-V Server 2016 Microsoft Hyper-V Server 2016 HA Cluster	40 GiB RAM	1.2 TB	6 cores with at least 2 GHz
Azure	VM Size: D16ds_v4	64 GiB (D16ds_v4)	2 TB SSD	16 vCPUs (D16ds_v4)
AWS	AWS EC2: InstanceSize: m5.4xlarge	64 GiB (m5.4xlarge)	AWS EBS: General Purpose SSD (GP2) 2TB	16 vCPUs (m5.4xlarge)
Bare Metal (HP DL360p Gen10)				
	-	64 GiB RAM	Disk: 2x 1.92 TB SSD configured in RAID 0	CPU: Intel (R) Xeon(R) Gold 6126 (12 cores 2.60 GHz each)
SP Single				
	VMware: ESXi 6.7 VMware HA cluster: VMware ESXi 6.5 Ethernet ports: 10GB ports[1]	256 GB	Standalone mode: SSD 6TB	24 cores at 2.60 GHz
SP Cluster (three VMware servers)				
	VMware: ESXi 6.7 VMware HA	256 GB	20T for management server	24 cores at 2.60 GHz

[1] Relevant for SP Single and SP Cluster only

Resources	Virtual Platform	Memory	Disk Space	Processors
	cluster: VMware ESXi 6.5 Ethernet ports: 10GB ports		■ 10T for VQ/PM servers	

OVOC Client Requirements

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

Table 3-1: OVOC Client Minimum Requirements

Resource	OVOC Client
Hardware	Screen resolution: 1280 x 1024
Operating System	Windows 7 or later
Memory	8 GB RAM
Disk Space	-
Processor	-
Web Browsers	■ Mozilla Firefox version 39 and higher ■ Google Chrome version 79 and higher ■ Microsoft Edge Browser version 80 and higher
Scripts	■ PHP Version 7.4 ■ Angular 10.0

Bandwidth Requirements

This section lists the OVOC bandwidth requirements.

OVOC Bandwidth Requirements

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

Voice Quality Bandwidth Requirements

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

Table 3-2: Voice Quality Bandwidth Requirements

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

Device	SBC Sessions (each session has two legs)	Required Kbits/sec or Mbit/sec
Endpoints	_	56 Kbits/sec

OVOC Capacities

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

Table 3-3: OVOC Capacities

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server	Service Provider Cluster Mode
OVOC Management Capacity					
Managed devices	100	5,000	5,000	10,000	50,000
Links	200	10,000	10,000	10,000	10,000
Operators	25				
Device Manager Pro					
Managed devices	1,000	■ 30,000 Microsoft Lync/Skype for Business and third-party vendor devices [1] ■ 4,000 Microsoft Teams devices	■ 10,000 Microsoft Lync/Skype for Business and third- party vendor devices[2] ■ 4,000 Microsoft Teams devices	■ 30,000 Skype for Business devices ■ 4,000 Teams device	■ 30,000 Skype for Business devices ■ 4,000 Teams devices
Disk space allocated for firmware files	5 GB	10 GB			20 GB
Alarm and Journal Capacity					
History alarms	Up to 12 months or 10,000,000 million alarms				Up to 12 months or 50,000,000
Journal logs	Up to 12 months	Up to 12 months	Up to 12 months	Up to 12 months	Up to 12 months
Steady state	20 alarms per second			50 alarms per second	100 alarms per second

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

[2] Including phones, headsets and Conference Suite devices

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server	Service Provider Cluster Mode
Performance Monitoring					
Polled parameters per polling interval per OVOC- managed device	50,000	100,000	100,000	500,000	500,000
Polled parameters per polling interval per OVOC instance	50,000	500,000	500,000	1,000,000	■ 5,000,000 for Version 7.4 devices (REST interface) ■ 500,000 for Version 7.2 devices (SNMP interface)
Storage time	One year				
QoE Call Flow (for SBC calls only)					
CAPS per device	10	100	100	300	300
CAPS (calls attempts per second) per OVOC instance	6	25	100	300	1,000
Maximum number of calls	1,000,000				10,000,000
OVOC QoE for Devices					
QoE for managed devices	100	1,200	3,000	10,000	25,000
CAPS (calls attempts per second) per device	30	120	300	1,000	1,000
CAPS per OVOC instance (SBC and SFB/Teams and RFC SIP Publish 6035)	30 Teams CAPS=30[1]	120 Teams CAPS=120[2]	300	1,000 Teams CAPS=[3]	2,500
QoE concurrent sessions	3,000	12,000	30,000	100,000	250,000
Call Details Storage - detailed information per call	Up to one year or 6,000,000	Up to one year or 80,000,000	Up to one year or 80,000,000	Up to one year or 250,000,000	Up to one year or 400,000,000
Calls Statistics Storage - statistics information storage	Up to one year or 12,000,000	Up to one year or 150,000,000	Up to one year or 150,000,000	Up to one year or 500,000,000	Up to one year or 750,000,000
QoE Capacity with SBC Floating License Capability					
CAPS (calls attempts per second) per OVOC instance with SIP call flow.	5	22	90	-	-

[1] The TEAMS CAPS estimation is based on round trip delay of 500 milliseconds to Microsoft Azure.

[2] As above

[3] Please contact AudioCodes OVOC Product Manager

Machine Specifications	Low Profile	High Profile	Bare Metal	Service Provider Single Server	Service Provider Cluster Mode
CAPS (calls attempts per second) per OVOC instance without SIP call flow.	27	108	270	-	-
Managed devices with floating license.	100	500	1,000	-	-
Lync and AD Servers– applicable for QoE license only					
MS Lync servers	Up to 2				
AD Servers for Users sync	Up to 2				
Users sync	Up to 150,000				

Skype for Business Monitoring SQL Server Prerequisites

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

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

- The server must be configured to collect calls before the OVOC can connect to it and retrieve Skype for Business calls.
- Call Detail Records (CDRs) and Quality of Experience (QoE) Data policies must be configured to capture data.
- Network administrators must be provisioned with the correct database permissions (refer to the *One Voice Operations Center User's Manual*).
- Excel macros must be enabled so that the SQL queries and reports can be run; tested with Excel 2010.
- Detailed minimum requirements for Skype for Business SQL Server can be found in the following link:

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

4 OVOC Software Deliverables

The following table describes the OVOC software deliverables.

Table 4-1: OVOC Software Deliverables

Installation/Upgrade Platform	Media
Installation	
Dedicated	■ DVD1-Linux CentOS Operating System ■ DVD2-Oracle Installation ■ DVD3-OVOC Software Installation
VMware	■ **Standard mode:** DVD5-OVOC Software Installation OVA file ■ **Service Provider Cluster mode:** ✔ Option 1: ● Management: DVD1-DVD2-DVD3 ● VQM/PM: DVD1-DVD3 ✔ Option 2: ● Management: DVD5-Management-OVA ● VQM: DVD5-VQM-OVA ● PM: DVD5-PM-OVA
HyperV	■ DVD5-OVOC Software Installation 7z file
Amazon AWS	■ Create OVOC instance from Public AMI image provided by AudioCodes
Microsoft Azure	■ Create OVOC virtual machine from Azure Marketplace.
Upgrade	
Dedicated	■ DVD3-OVOC Server Application DVD OR ■ DVD3-OVOC Server Application ISO file
VMware	■ DVD3-OVOC Server Application ISO file (including separate scripts for Management, VQM and PM servers)
Microsoft HyperV	■ DVD3-OVOC Server Application ISO file

Installation/Upgrade Platform	Media
Amazon AWS	■ DVD3-OVOC Server Application ISO file

Note the following

- **DVD1:** Operating System DVD (OVOC server and Client Requirements):
- **DVD2:** Oracle Installation: Oracle installation version 12.1.0.2 DVD.
- **DVD3:** Software Installation and Documentation DVD:

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

  - 'EmsServerInstall' – OVOC server software (including Management server, PM server and VQM server) to install on the dedicated OVOC server machine.
  - Documentation – All documentation related to the present OVOC version. The documentation folder includes the following documents and sub-folders:
    - OVOC Release Notes Document – includes the list of the new features introduced in the current software version as well as version restrictions and limitations.
    - OVOC Server IOM Manual – Installation, Operation and Maintenance Guide.
    - OVOC Product Description
    - OVOC User's Manual
    - OVOC Integration with Northbound Interfaces
    - OVOC Security Guidelines
    - OVOC Alarms Monitoring Guide
    - OVOC Performance Monitoring Guide

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

Part II

OVOC Server Installation

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

5 Files Verification

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

- Windows (Windows below)
- Linux (Linux below)

Windows

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

- Verify the checksum with WinMD5 (see www.WinMD5.com)

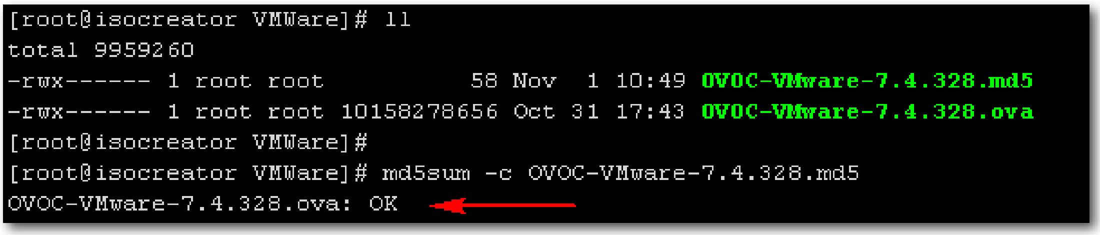
Linux

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 5-1: ISO File Integrity Verification



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

OVOC Server Users

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

- 'root' user: User permissions for installation, upgrade, maintenance using OVOC Server Managerand OVOC application execution.
- *acems* user: The only available user for login through SSH/SFTP tasks.
- *emsadmin* user: User with permissions for mainly the OVOC Server Manager and OVOC application for data manipulation and database access.

- *oracle* user: User permissions for the Oracle database access for maintenance such as installation, patches upgrade, backups and other Oracle database tasks.
- *oralsnr* user: User in charge of oracle listener startup.

In addition the OVOC server includes the following DB operator permissions:

- *Analytics* user: User used to connect to Northbound DB access clients

6 Installing OVOC Server on Virtual Machines on Cloud-based Platforms

This section describes how to install the OVOC server on the following Cloud-based platforms:

- Launching Public OVOC Image on Amazon Web Services (AWS) below
- Creating OVOC Virtual Machine and Configuring Microsoft Azure on page 31

Launching Public OVOC Image on Amazon Web Services (AWS)

This chapter describes how to create the OVOC virtual machine in an AWS cloud deployment, including the following procedures:

- Step 1 Launching Public Image on AWS below
- Step 2-2 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS on page 27

Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8).

Step 1 Launching Public Image on AWS

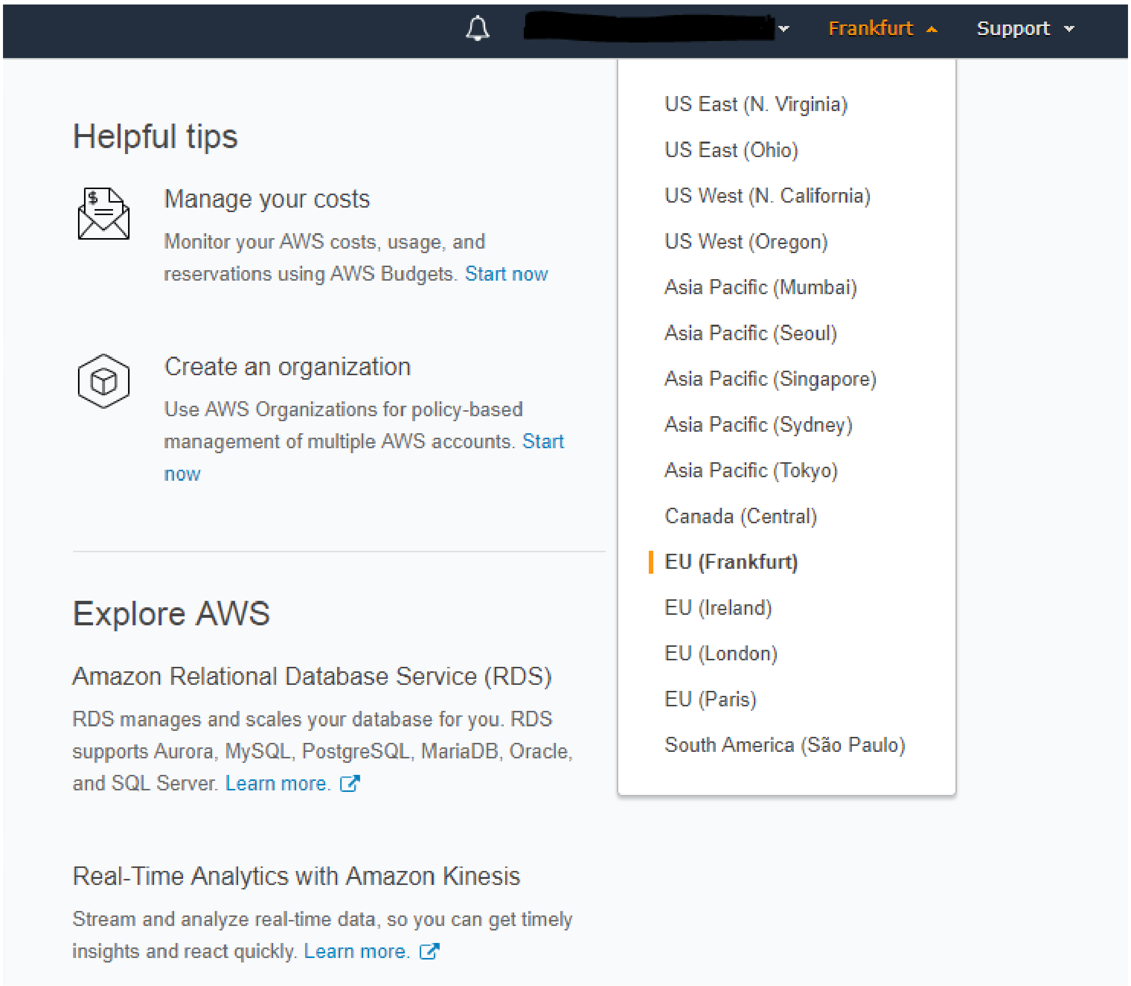
This section describes how to setup and load the AWS image.

➢ **To setup and load the AWS image:**

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)
   - ap-south-1 (Asia Pacific-Mumbai)

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

Figure 6-1: Select Region



Helpful tips

Manage your costs

Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

Amazon Relational Database Service (RDS)

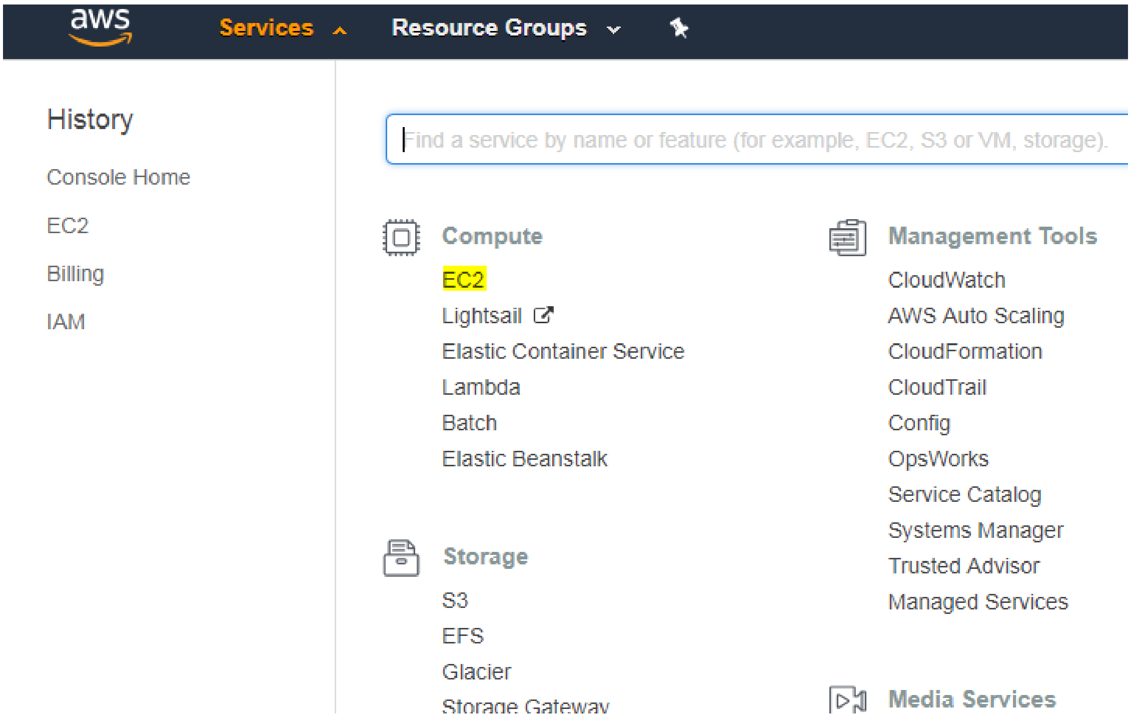
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

Real-Time Analytics with Amazon Kinesis

Stream and analyze real-time data, so you can get timely insights and react quickly. Learn more.

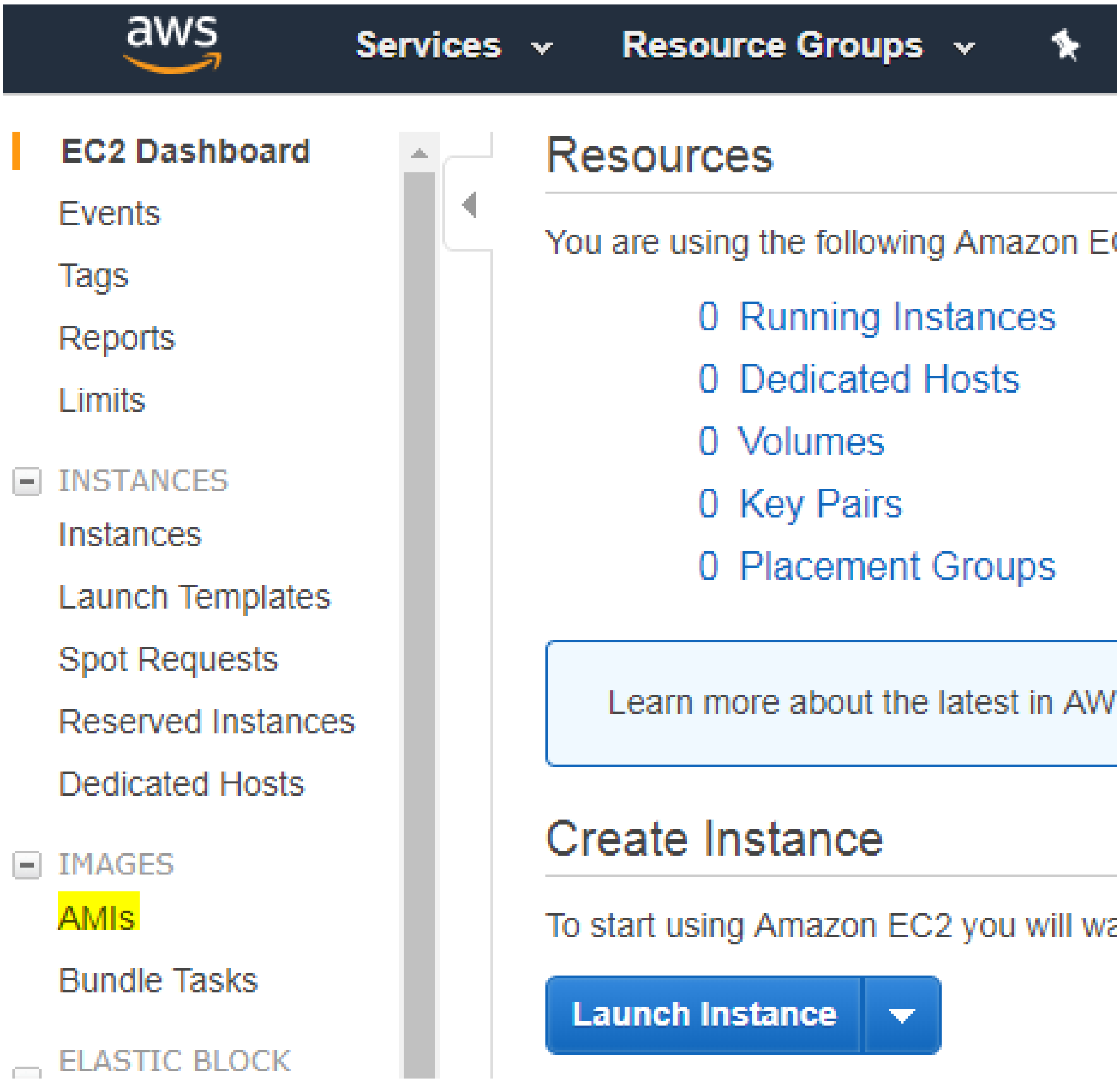
3. In the “Services” menu, choose EC2.

Figure 6-2: Services Menu - EC2



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

Figure 6-3: Images

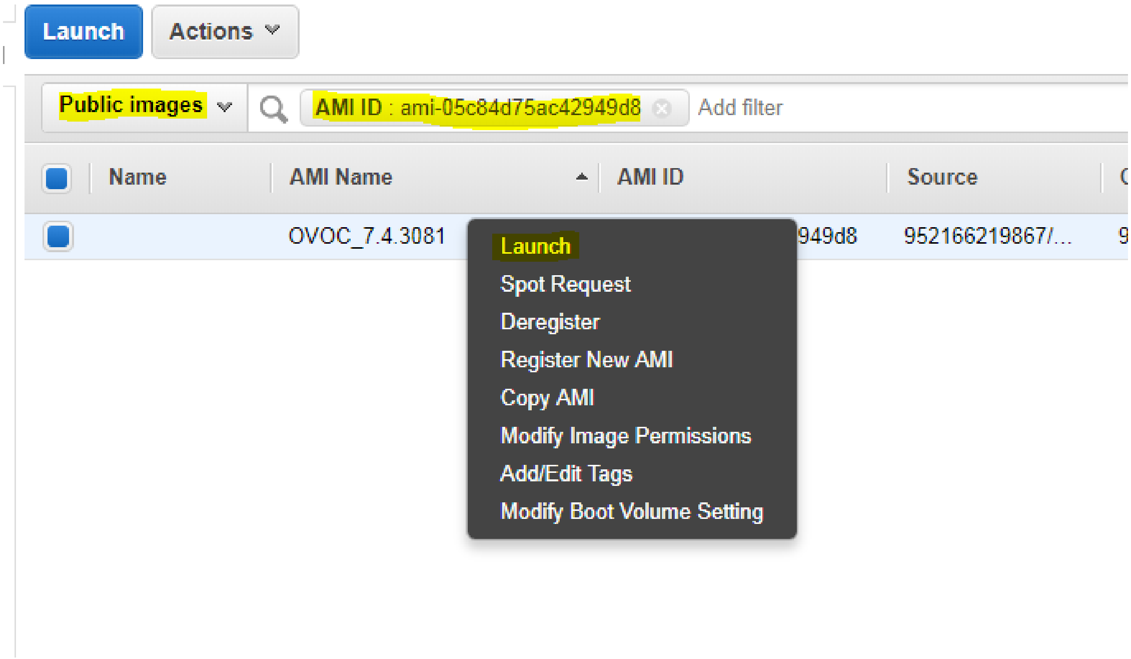


5. In the search bar, choose Public images and apply the following filter:

   AMI ID : ami-00000000000 replacing ami-00000000000 with the AMI ID you received from AudioCodes according to the region you have chosen.

6. Right-click the AMI and choose Launch.

Figure 6-4: Launch Public Images



7. Choose an Instance type according to the requirements specified in OVOC Server Minimum Requirements on page 8.

8. Configure Instance (Optional). Using this option, you can edit network settings, for example, placement.

9. Configure a Security Group; you should select an existing security group or create a new one according to the firewall requirements specified in the table below:

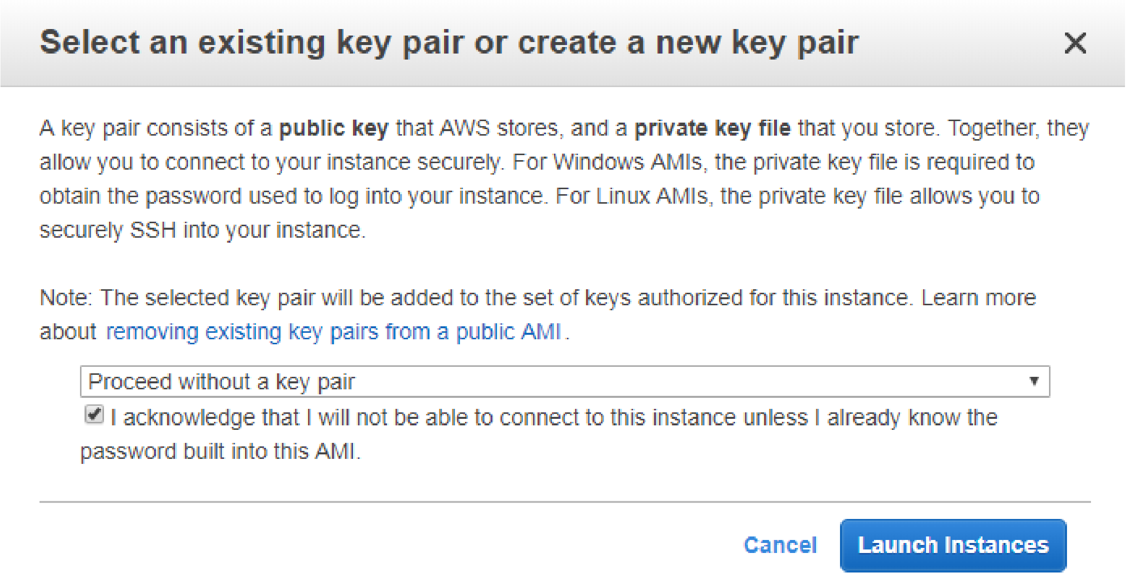
Table 6-1: Firewall for Amazon AWS

Protocol	Port	Description
UDP	162	SNMP trap listening port on the OVOC server.
UDP	1161	Keep-alive - SNMP trap listening port on the OVOC server used for NAT traversal.
TCP	5000	Communication for control, media data reports and SIP call flow messages
TCP (TLS)	5001	TLS secured communication for control, media data reports and SIP call flow messages
NTP	123	NTP server port (also configure the AWS IP address/Domain Name as the NTP server on both the managed device and OVOC server; see relevant procedures in Step 3 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS

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 6-5: Select an Existing Key Pair



Select an existing key pair or create a new key pair ✕

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

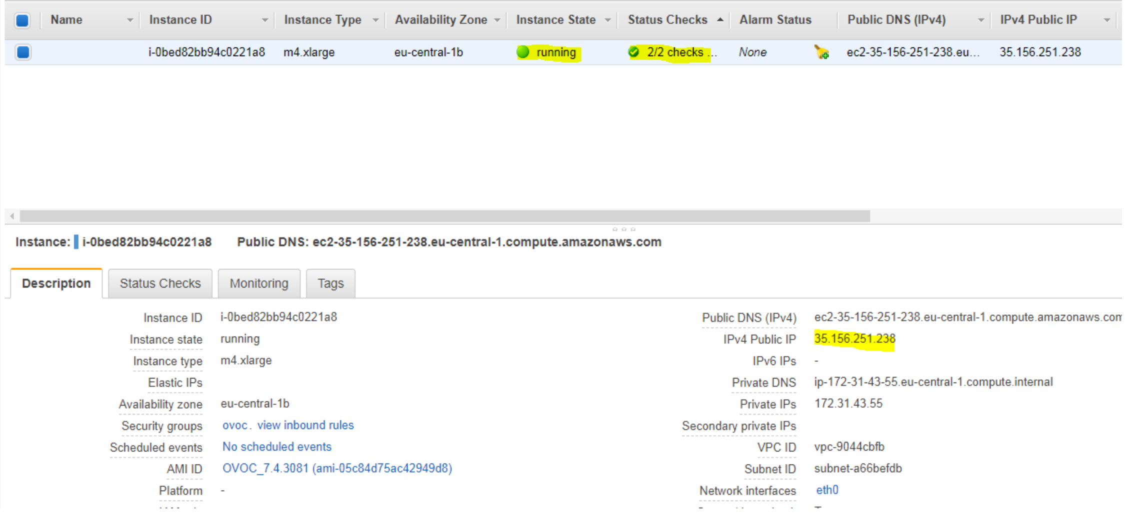
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Proceed without a key pair ▾

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

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

Figure 6-6: 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

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

Note the AWS public IP address as its later configured in Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS on the next page

Step 2 Connecting Mediant Cloud Edition (CE) SBC Devices on AWS

This section describes the procedure for establishing a secure connection between the OVOC server which is installed in the AWS Cloud and Mediant Cloud Edition (CE) SBC devices which are also deployed in the AWS Cloud. Communication between OVOC and Mediant CE SBC devices is carried over the public IP addresses on both sides, requiring NAT translation from internal to public IP addresses. This can be performed by either configuring the OVOC server with the public IP address of the AWS platform where the OVOC server is deployed (see Configure OVOC Server with Public or NAT IP Address on page 114) or by configuring OVOC Cloud Architecture mode (seeConfigure OVOC Cloud Architecture Mode on page 115

> The Mediant CE SBC devices must be added to OVOC using Automatic Detection. Refer to Section "Adding AudioCodes Devices Automatically" in the *OVOC User's Manual*.

This section includes the following procedures:

- Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS below
- Step 2-2 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS on the next page

Step 2-1 Configuring the OVOC Server (OVOC Server Manager) on AWS

This section describes the required configuration actions on the OVOC server deployed in the AWS Cloud.

> Restart the OVOC server where specified in the referenced procedures for changes to take effect.

➢ **To configure the OVOC server:**

1. Login to the OVOC Server Manager (see Connecting to the OVOC Server Manager on page 163).
2. Change the following default passwords:
   - acems OS user (see OS Users Passwords on page 227)
   - root OS user (see OS Users Passwords on page 227)

> 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 theses default passwords to minimize exposure to password hacking.

3. Load OVOC license (see License on page 183).
4. Configure the OVOC server with AWS Public IP address to enable devices deployed behind a NAT to connect to OVOC server (see Configure OVOC Server with Public or NAT IP Address on page 114). See the setup of the virtual machine Step 1: Creating Virtual Machine on Azure on page 32 to find the AWS Public IP.
5. Configure the AWS Public IP address/Domain Name (where OVOC is installed) as the external NTP clock source (see NTP on page 211).

⚠ The same clock source should be configured on the managed devices (see Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface on the next page).

Step 2-2 Configuring Mediant Cloud Edition (CE) SBC Devices on AWS

This step describes the following configuration procedures on the Mediant CE SBC devices to connect them to the OVOC server that is deployed in the AWS Cloud:

- Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager below
- Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface on the next page

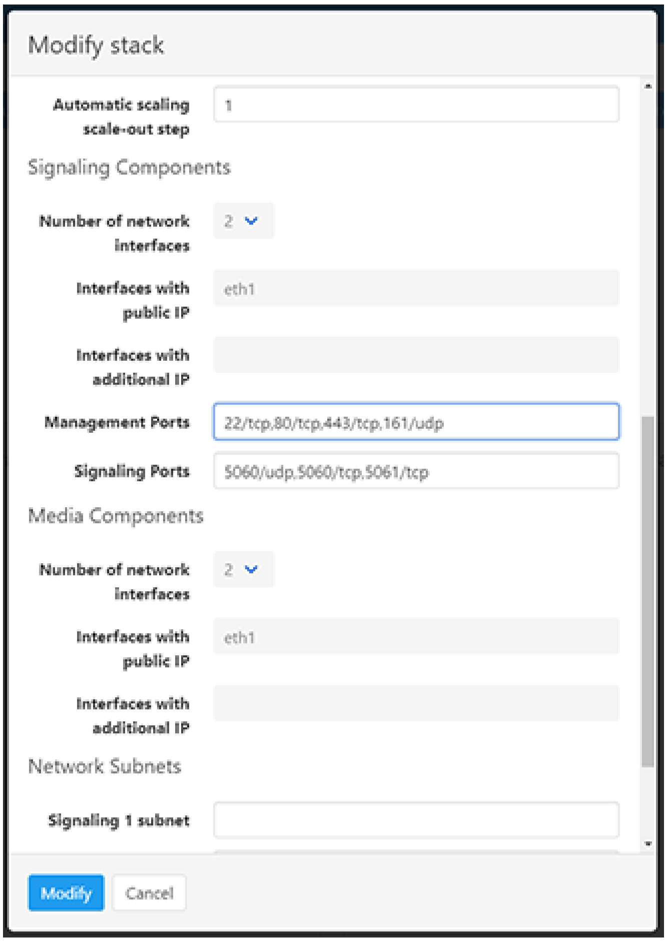
Step 2-2-1: Configuring Mediant CE SNMP Connection with OVOC in Cloud using Stack Manager

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

➢ **To configure the Stack Manager:**

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

Figure 6-7: Modify Stack



Modify stack

Automatic scaling scale-out step: 1

Signaling Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

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

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

Media Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Network Subnets

Signaling 1 subnet:

Step 2-2-2 Configuring Mediant CE Communication Settings Using Web Interface

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

> ⚠ The following procedure describes the required configuration for a single CE SBC device. For mass deployment, you can load configuration files to multiple devices using 'Full' or 'Incremental' INI file options (refer to the relevant *SBC User's Manual* for more information).

➢ To configure the Mediant Cloud Edition (CE) SBC for AWS:

1. Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
2. Open the Quality of Experience Settings screen (**Setup** Menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience** > **Quality of ExperienceSettings**).
3. Click **Edit** and configure the **Keep-Alive Time Interval** to **1**.
4. Click **Apply** to confirm changes.

5. Open the TIME & DATE page (**Setup** menu > **Administration** tab) and configure the AWS site IP address/FQDN Domain Name(where the OVOC server is installed) as the NTP server clock source.
6. Click **Apply** to confirm changes.
7. Open the SNMP Community Settings Page (**Setup** menu > **Administration** tab > **SNMP** folder).
8. Set parameter SNMP Disable to **No** ('Yes' by default).
9. Click **Apply** to confirm changes.
10. Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPaddress/AdminPage) and configure the following ini parameters:

```
HostName = <Load Balancer IP>
SendKeepAliveTrap = 1
KeepAliveTrapPort = 1161
SNMPManagerIsUsed_0 = 1
SNMPManagerTableIP_0 = <OVOC Public IP Address>
```

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

Step 3 Configuring AWS SES Service

This section describes how to configure the OVOC server as the Email server on Amazon AWS. These steps are necessary in to overcome Amazon security restrictions for sending emails outside of the AWS domain.

> If AWS Simple Email Service (SES) runs in Sandbox mode, both sender and recipient addresses should be verified (see https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html)

➢ To configure OVOC as email server on AWS SES:

1. Login to the OVOC server with root permissions.
2. Open file /root/.muttrc:

```
cat .muttrc
```

3. Replace "OVOC@audiocodes.com" with authenticated source email.
4. Open file /etc/exim/exim.conf and using a text editor, find the respective "begin …" statements and paste the below configuration accordingly

- Replace : AWS_SES_LOGIN : AWS_SES_PASSWORD with the credentials received from AWS
- Replace : SOURCE_EMAIL with an authenticated source email address
- Replace: HOSTNAME with the VM hostname

```
==============================================================
begin routers
send_via_ses:
driver = manualroute
domains = ! +local_domains
transport = ses_smtp
route_list = * email-smtp.eu-central-1.amazonaws.com;
==============================================================
begin transports
ses_smtp:
driver = smtp
port = 587
hosts_require_auth = *
hosts_require_tls = *
==============================================================
begin authenticators
```

```
ses_login:
driver = plaintext
public_name = LOGIN
client_send = : AWS_SES_LOGIN : AWS_SES_PASSWORD
============================================================
begin rewrite
^root@HOSTNAME SOURCE_EMAIL SFfrs
============================================================
```

5. Remove old unsent emails from buffer and restart exim service:

```
systemctl restart exim
exim -bp | exiqgrep -i | xargs exim -Mrm
rm -rf /var/spool/exim/db/*
```

6. Send test email using mutt:

```
echo "Hello!" > ~/message.txt
mutt -s "Test Mail from OVOC" -F /root/.muttrc EMAIL_ADDRESS < ~/message.txt
```

7. Verify in the exim log in /var/log/exim/main.log to check that the email was sent correctly.

Creating OVOC Virtual Machine and Configuring Microsoft Azure

This chapter describes how to install the OVOC server on a virtual machine in a Cloud-based deployment from the Microsoft Azure Marketplace, including the following procedures:

- Step 1: Creating Virtual Machine on Azure on the next page

- Step 2: Configuring OVOC as the Email Server on Microsoft Azure on page 38
- Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on page 43
- Step 4 Registering Microsoft Teams Application on page 50
- Step 5 Configuring Microsoft Graph API Permissions on page 54
- Step 6 Configuring AudioCodes Azure Active Directory (Operator Authentication) on page 57

> Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8).

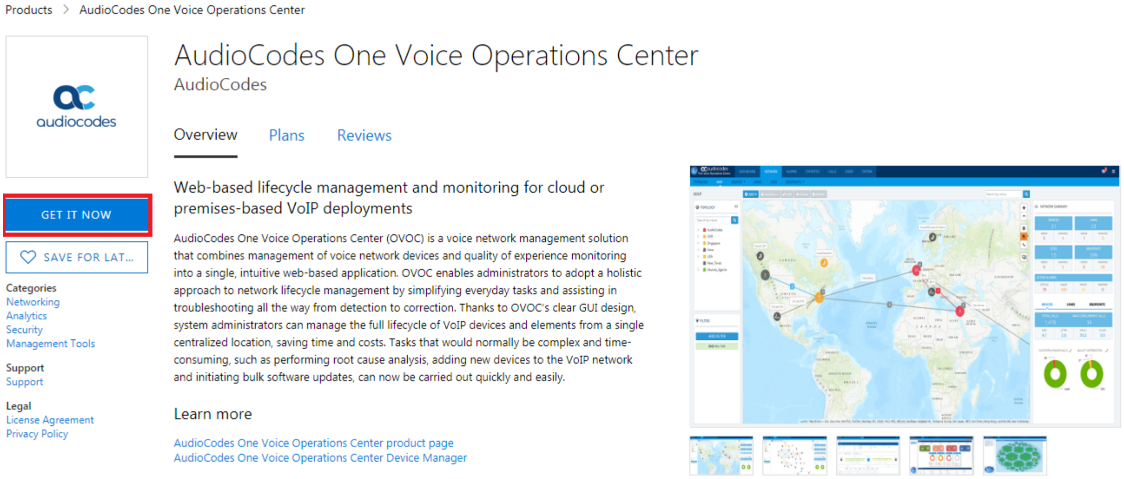
Step 1: Creating Virtual Machine on Azure

This procedure describes how to setup and load the virtual image.

➢ To install OVOC from the Microsoft Azure Marketplace:

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

Figure 6-8: Get it Now



Products > AudioCodes One Voice Operations Center

AudioCodes One Voice Operations Center

AudioCodes

Overview Plans Reviews

Web-based lifecycle management and monitoring for cloud or premises-based VoIP deployments

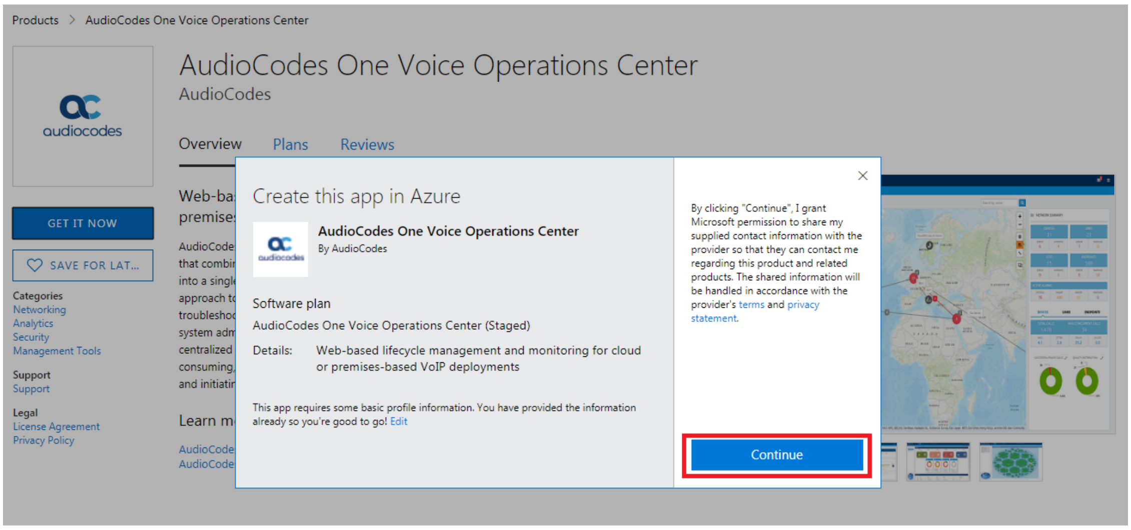
AudioCodes One Voice Operations Center (OVOC) is a voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web-based application. OVOC enables administrators to adopt a holistic approach to network lifecycle management by simplifying everyday tasks and assisting in troubleshooting all the way from detection to correction. Thanks to OVOC's clear GUI design, system administrators can manage the full lifecycle of VoIP devices and elements from a single centralized location, saving time and costs. Tasks that would normally be complex and time-consuming, such as performing root cause analysis, adding new devices to the VoIP network and initiating bulk software updates, can now be carried out quickly and easily.

Learn more

AudioCodes One Voice Operations Center product page
AudioCodes One Voice Operations Center Device Manager

2. Click **Continue.**

Figure 6-9: Create this App in Azure



Create this app in Azure

AudioCodes One Voice Operations Center
By AudioCodes

Software plan
AudioCodes One Voice Operations Center (Staged)

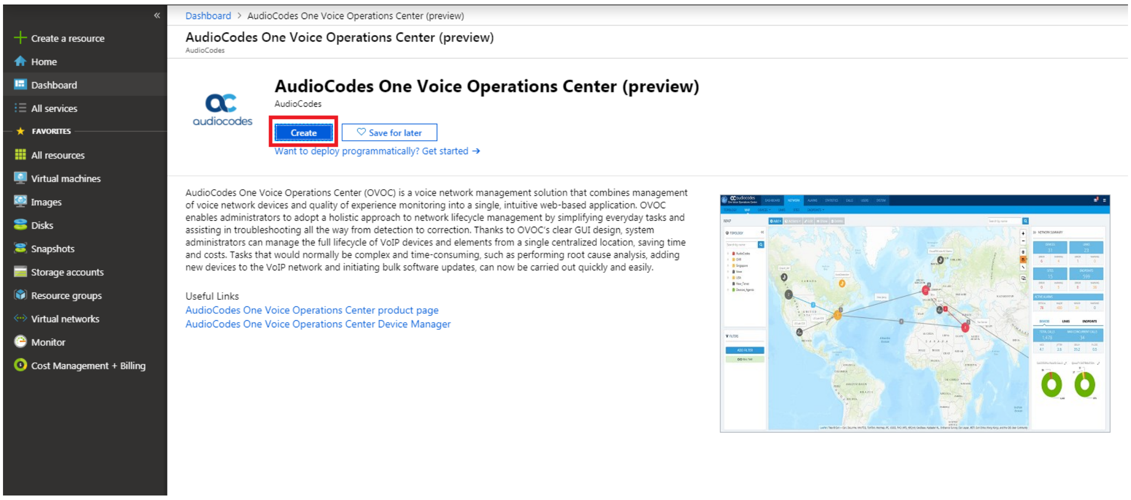
Details: Web-based lifecycle management and monitoring for cloud or premises-based VoIP deployments

This app requires some basic profile information. You have provided the information already so you're good to go! Edit

By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be handled in accordance with the provider's terms and privacy statement.

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

Figure 6-10: Create Virtual Machine



AudioCodes One Voice Operations Center (preview)
AudioCodes

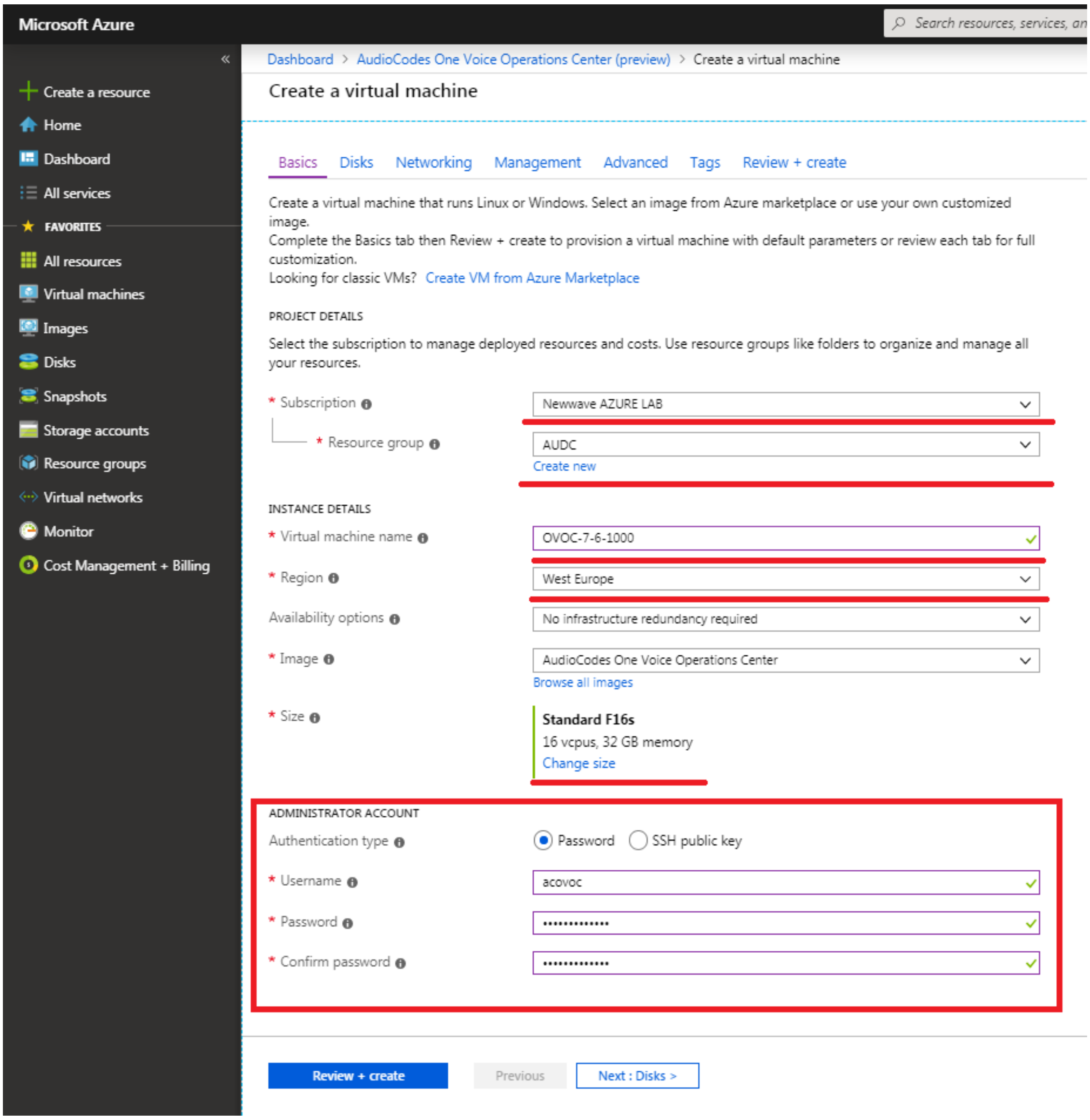
AudioCodes One Voice Operations Center (preview)
AudioCodes

AudioCodes One Voice Operations Center (OVOC) is a voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web-based application. OVOC enables administrators to adopt a holistic approach to network lifecycle management by simplifying everyday tasks and assisting in troubleshooting all the way from detection to correction. Thanks to OVOC's clear GUI design, system administrators can manage the full lifecycle of VoIP devices and elements from a single centralized location, saving time and costs. Tasks that would normally be complex and time-consuming, such as performing root cause analysis, adding new devices to the VoIP network and initiating bulk software updates, can now be carried out quickly and easily.

Useful Links
AudioCodes One Voice Operations Center product page
AudioCodes One Voice Operations Center Device Manager

4. Configure the following:
    a. Choose your Subscription.
    b. Choose your Resource Group or create a new one
    c. Enter the name of the new Virtual Machine.
    d. Choose the Region.
    e. Choose the VM Size (see Hardware and Software Requirements).
    f. Choose Authentication Type "Password" and enter username and user-defined password or SSH Public Key.

Figure 6-11: Virtual Machine Details



Create a virtual machine

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

PROJECT DETAILS

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

* Subscription: Newwave AZURE LAB

* Resource group: AUDC
Create new

INSTANCE DETAILS

* Virtual machine name: OVOC-7-6-1000

* Region: West Europe

Availability options: No infrastructure redundancy required

* Image: AudioCodes One Voice Operations Center
Browse all images

* Size: **Standard F16s**
16 vcpus, 32 GB memory
Change size

ADMINISTRATOR ACCOUNT

Authentication type: ● Password ○ SSH public key

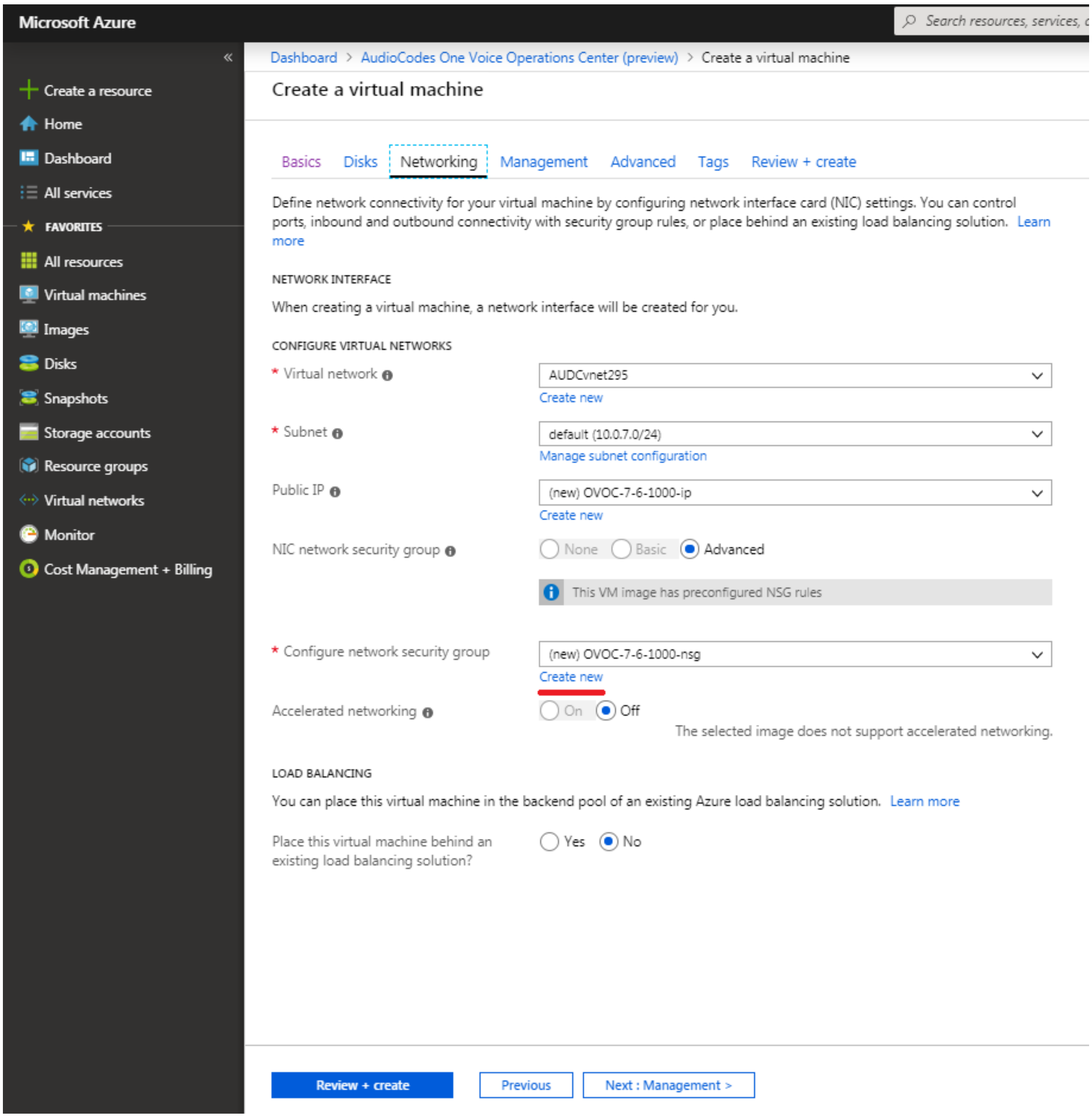
* Username: acovoc

* Password: •••••••••••••

* Confirm password: •••••••••••••

5. Click **Next** until **Networking** section to configure the network settings,

Figure 6-12: Network Settings



Create a virtual machine

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

NETWORK INTERFACE

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

CONFIGURE VIRTUAL NETWORKS

* Virtual network: AUDCvnet295 (Create new)

* Subnet: default (10.0.7.0/24) (Manage subnet configuration)

Public IP: (new) OVOC-7-6-1000-ip (Create new)

NIC network security group: ○ None ○ Basic ● Advanced

This VM image has preconfigured NSG rules

* Configure network security group: (new) OVOC-7-6-1000-nsg (Create new)

Accelerated networking: ○ On ● Off

The selected image does not support accelerated networking.

LOAD BALANCING

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

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No

a. From the Virtual Network and Subnet drop-down lists, select an existing virtual network/subnet or click **Create new** to create a new virtual network/subnet.

b. From the Public IP drop-down list, configure "none", use the existing Public IP or create a new Public IP.

> If you do not wish the public IP address to change whenever the VM is stopped/started, choose **Static SKU** or **Basic SKU + Static**.

c. Under Configure network security group, click **Create new** to configure a Network Security Group. Configure this group according to the Firewall rules shown in the table below.

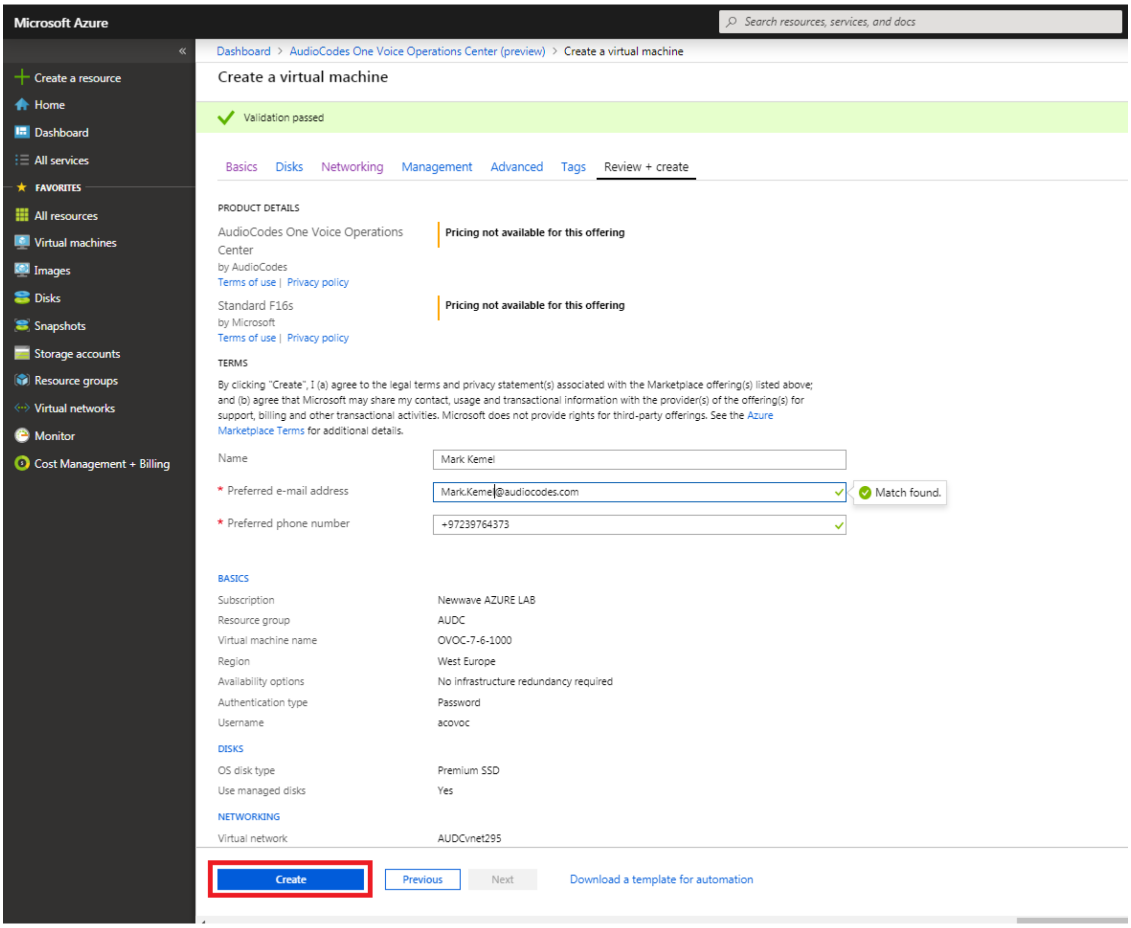
⚠ By default, only ports 22 and 443 are open for inbound traffic; open other ports for managing devices behind a NAT (outside the Azure environment) as described in the table below.

Table 6-2: Microsoft Azure Firewall

Protocol	Port	Description
UDP	162	SNMP trap listening port on the OVOC server.
UDP	1161	Keep-alive - SNMP trap listening port on the OVOC server used for NAT traversal. This rule is required if Auto-detection is used to add devices in OVOC. See Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on page 43
TCP	5000	Communication for control, media data reports and SIP call flow messages sent from Mediant Cloud Edition (CE) SBC.
TCP (TLS)	5001	TLS secured communication for control, media data reports and SIP call flow messages sent from Mediant Cloud Edition (CE) SBC. This rule is used if the OVOC Server and managed devices (specifically Mediant CE devices) are deployed in separate Azure Virtual networks communicating behind a firewall. See Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address on page 43
NTP	123	NTP server port (set the Microsoft Azure site IP address/Domain Name(where the OVOC server is installed) as the NTP server clock source. Referenced in procedures in Step 3 Connecting Mediant Cloud Edition (CE) Devices on page 43

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

Figure 6-13: Review and Create



Create a virtual machine

✓ Validation passed

PRODUCT DETAILS

AudioCodes One Voice Operations Center
by AudioCodes
Terms of use | Privacy policy — Pricing not available for this offering

Standard F16s
by Microsoft
Terms of use | Privacy policy — Pricing not available for this offering

TERMS

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

Name	Mark Kemel
* Preferred e-mail address	Mark.Kemel@audiocodes.com ✓ Match found.
* Preferred phone number	+97239764373 ✓

BASICS

Subscription	Newwave AZURE LAB
Resource group	AUDC
Virtual machine name	OVOC-7-6-1000
Region	West Europe
Availability options	No infrastructure redundancy required
Authentication type	Password
Username	acovoc

DISKS

OS disk type	Premium SSD
Use managed disks	Yes

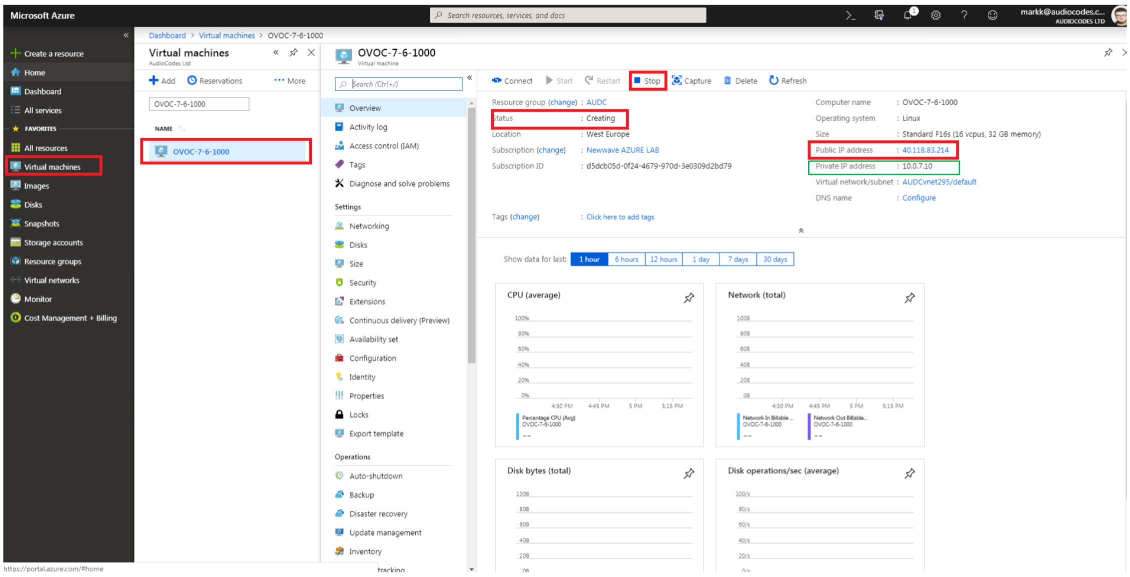
NETWORKING

Virtual network	AUDCvnet295

7. Navigate to the "Virtual machines" section, where you can, for example, monitor the Virtual Machine creation process and find the Public or Private (Internal) IP addresses to access the Virtual Machine.

Note the public or private (Internal) IP addresses as you need to configure them in Configuring the OVOC Server Manager on Azure (Public IP) on page 44 and Configuring the OVOC Server Manager on Azure (Internal IP) on page 47 respectively.

Figure 6-14: Azure Deployment Process Complete



Resource group (change) : AUDC
Status : Creating
Location : West Europe
Subscription (change) : Newwave AZURE LAB
Subscription ID : d5dcb05d-0f24-4679-970d-3e0309d2bd79
Tags (change) : Click here to add tags

Computer name : OVOC-7-6-1000
Operating system : Linux
Size : Standard F16s (16 vcpus, 32 GB memory)
Public IP address : 40.118.83.214
Private IP address : 10.0.7.10
Virtual network/subnet : AUDCvnet295/default
DNS name : Configure

Step 2: Configuring OVOC as the Email Server on Microsoft Azure

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

- Configuring Alarm Forwarding by Email on Microsoft Azure using Microsoft Office 365
- Configuring Alarm Forwarding by Email on Microsoft Azure using SMTP Relay

Step 2-1: Configuring OVOC as the Email Server on Microsoft Azure using Microsoft Office 365

This procedure describes how to configure the OVOC server to forward alarms by email through the configuration of a user account on the Microsoft Office 365 platform. Replace OFFICE365_USERNAME and PASSWORD with an existing customer's Office 365 username and password.

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

➢ **Do the following:**

1. Configure the Exim service on the OVOC server:

   a. Login into the OVOC server by SSH, as ‘acems’ user and enter password *acems*.

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

   ```
   su - root
   ```

   c. Backup the exim configuration file:

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

d. Edit the exim configuration file:

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

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

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

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

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

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

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

h. Restart the exim service:

```
systemctl restart exim
```

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

Step 2-2 Configuring OVOC as the Email Server on Microsoft Azure using SMTP Relay

This procedure describes how to configure the OVOC server to forward alarms by email using SMTP Relay. This setup is recommended by Microsoft, and SendGrid is one of the available options. SendGrid service can be easily configured in the Azure Portal and in addition, includes a free tier subscription, supporting up to 25,000 emails per month.

➢ **Do the following:**

1. Create SendGrid service on the Azure platform:
    a. Open portal.azure.com
    b. Go to "SendGrid Accounts" section, (via Search or in "All services" section).
    c. Click **Add.**
    d. Fill in the following fields:

       Name: Choose a name
       Password
       Subscription
       Resource Group (create a new one or choose existing)
       Pricing tier: choose Free or one of the other plans
       Contact Information
       Read legal terms

    e. Click **Create**.
    f. Wait for the service to be created.
    g. Go back to "SendGrid Accounts", click on the new account name
    h. Click the"Configurations" section in the **Settings** tab.
    i. Copy the Username – it will be used in the next step along with the password (format azure_xxxxxxxx@azure.com)
2. Configure the Exim service on the OVOC server:
    a. Login into the OVOC server by SSH, as ‘acems’ user and enter password *acems*.
    b. Switch to 'root' user and provide root password (default password is root):

```
su - root
```

c. Backup the exim configuration file:

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

d. Edit the exim configuration file:

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

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

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

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

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

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

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

h. Save the file and exit back to the command line.

i. Restart the Exim service.

```
systemctl restart exim
```

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

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

Step 3 Connecting Mediant Cloud Edition (CE) Devices

This section describes how to connect Mediant Cloud Edition (CE) devices to OVOC using one of the following options:

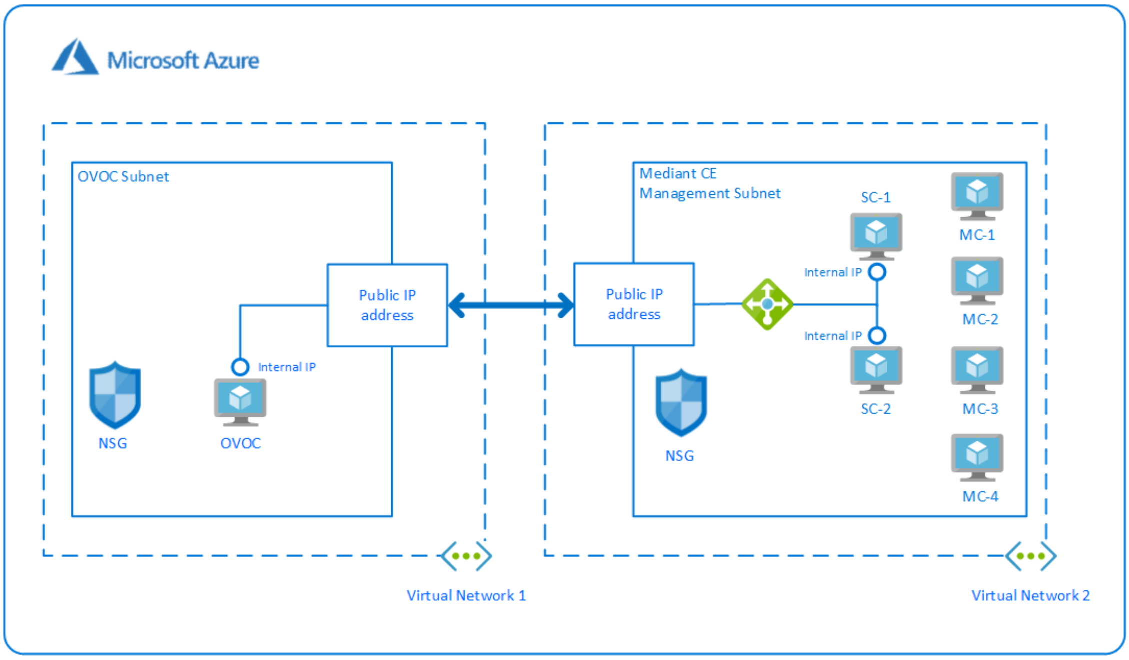
- Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address below
- Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address on page 46

Option 1: Connecting Mediant Cloud Edition (CE) SBC Devices to OVOC on Azure using Public IP Address

This section describes how to establish a secure connection between the OVOC server and Mediant Cloud Edition (CE) SBC devices which are both deployed in the Azure Cloud in separate Virtual networks. Communication between OVOC and Mediant CE SBC devices is carried over the public IP addresses on both sides, requiring NAT translation from internal to public IP addresses. This is performed by configuring the OVOC server with the public IP address of the Azure platform where the OVOC server is installed (see Configure OVOC Server with Public or NAT IP Address on page 114). The figure below illustrates this topology.

The Mediant CE SBC devices must be added to OVOC using Automatic Detection. Refer to Section "Adding AudioCodes Devices Automatically" in the *OVOC User's Manual*.

Figure 6-15: Microsoft Azure Topology



This section includes the following procedures:

1. Configuring the OVOC Server Manager on Azure (Public IP) on the next page

2. Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Public IP) below

Configuring the OVOC Server Manager on Azure (Public IP)

This section describes the required configuration actions on the OVOC server deployed in the Azure Cloud.

> ⚠ Restart the OVOC server where specified in the referenced procedures for changes to take effect.

➢ **To configure the OVOC server:**

1. Login to the OVOC Server Manager (see Connecting to the OVOC Server Manager on page 163).
2. Change the following default passwords:
   - acems OS user (see OS Users Passwords on page 227)
   - root OS user (see OS Users Passwords on page 227)

> ⚠ Unless you have made special configurations, the Azure instance is in the public cloud and therefore is accessible over the Internet. Consequently, it is highly recommended to change theses default passwords to minimize exposure to password hacking.

3. Load the OVOC license (see License on page 183).
4. Configure the OVOC server with Azure Public IP address to enable devices deployed behind a NAT to connect to OVOC (see Configure OVOC Server with Public or NAT IP Address on page 114). See the setup of the virtual machine to find the Azure Public IP (see Creating OVOC Virtual Machine and Configuring Microsoft Azure on page 31
5. Configure the Azure IP address/Domain Name (where OVOC is installed) as the external NTP clock source (see NTP on page 211).

> ⚠ The same clock source should be configured on the managed devices (see Configuring Mediant CE OVOC Public IP Connection Settings using Web Interface on the next page).

Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Public IP)

This step describes the following configuration procedures on the Mediant CE to connect to the OVOC server that is deployed in the Azure Cloud:

1. Configuring Mediant CE SNMP Public IP Connection using Stack Manager on the next page
2. Configuring Mediant CE OVOC Public IP Connection Settings using Web Interface on the next page

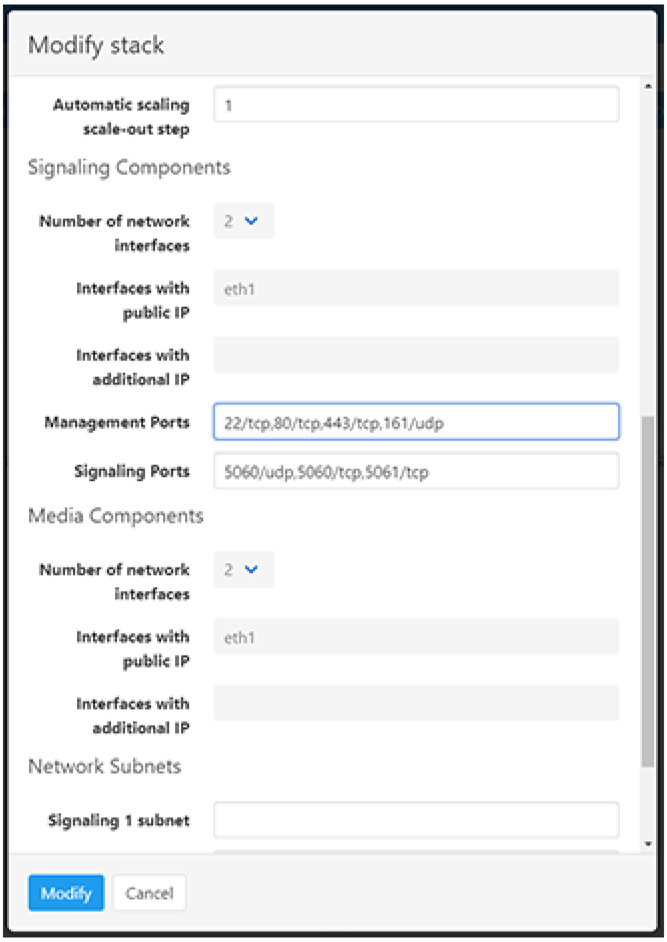
Configuring Mediant CE SNMP Public IP Connection using Stack Manager

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

➢ **To configure the Stack Manager:**

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

Figure 6-16: Modify Stack



Modify stack

Automatic scaling scale-out step: 1

Signaling Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

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

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

Media Components

Number of network interfaces: 2

Interfaces with public IP: eth1

Interfaces with additional IP:

Network Subnets

Signaling 1 subnet:

Configuring Mediant CE OVOC Public IP Connection Settings using Web Interface

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

The following procedure describes the required configuration for a single CE SBC device. For mass deployment, you can load configuration files to multiple devices using 'Full' or 'Incremental' INI file options (refer to the relevant *SBC User's Manual* for more information).

➢ To configure the Mediant Cloud Edition (CE) SBC :

1. Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
2. Open the Quality of Experience Settings screen (**Setup** Menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience** > **Quality of ExperienceSettings**).
3. Click **Edit** and configure the **Keep-Alive Time Interval** to **1**.
4. Click **Apply** to confirm the changes.
5. Open the TIME & DATE page (**Setup** menu > **Administration** tab) and in the NTP Server Address field, set the Microsoft Azure site IP address/Domain Name(where the OVOC server is installed) as the NTP server clock source.
6. Click **Apply** to confirm the changes.
7. Open the SNMP Community Settings Page (**Setup** menu > **Administration** tab > **SNMP** folder).
8. Set parameter SNMP Disable to **No** ('Yes' by default).
9. Click **Apply** to confirm changes.
10. Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPaddress/AdminPage) and configure the following ini parameters:

```
HostName = <Load Balancer IP>
SendKeepAliveTrap = 1
KeepAliveTrapPort = 1161
SNMPManagerIsUsed_0 = 1
SNMPManagerTableIP_0 = <OVOC Public IP Address>
```

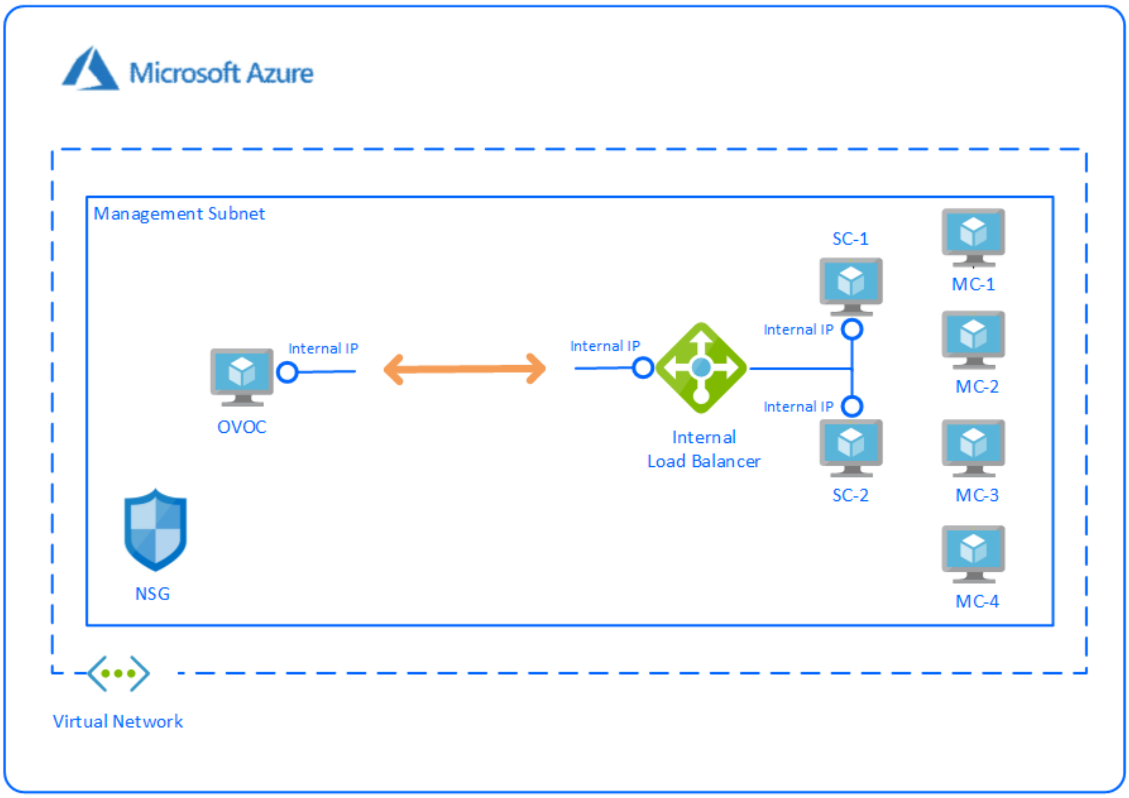
11. Reset the device for your settings to take effect (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

Option 2 Connecting Mediant Cloud Edition (CE) Devices to OVOC on Azure using Internal IP Address

This section describes how to establish a secure connection between the OVOC server and Mediant CE devices which are both deployed in the Azure Cloud in the same Virtual network. Communication between OVOC and Mediant CE SBC devices is carried over internal IP addresses (Private IP addresses) on both sides. The figure below illustrates this topology.

> The Mediant CE SBC devices must be added manually to OVOC. Refer to Section "Adding AudioCodes Devices Manually " in the *OVOC User's Manual*.

Figure 6-17: Internal IP Connection



This section includes the following procedures:

- Configuring the OVOC Server Manager on Azure (Internal IP) below
- Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Internal IP) on the next page

> The Mediant CE SBC devices must be added to OVOC manually. Refer to Section "Adding AudioCodes Devices Manually" in the *OVOC User's Manual*.

Configuring the OVOC Server Manager on Azure (Internal IP)

This section describes the required configuration actions on the OVOC server deployed in the Azure Cloud when CE devices are deployed in the same Virtual network.

> Restart the OVOC server where specified in the referenced procedures for changes to take effect.

➢ To configure the OVOC server:

1. Login to the OVOC Server Manager (see Connecting to the OVOC Server Manager on page 163).
2. Change the following default passwords:
   - acems OS user (see OS Users Passwords on page 227)
   - root OS user (see OS Users Passwords on page 227)

> ⚠ Unless you have made special configurations, the Azure instance is in the public cloud and therefore is accessible over the Internet. Consequently, it is highly recommended to change theses default passwords to minimize exposure to password hacking.

3. Load the OVOC license (see License on page 183).
4. Configure the OVOC server with its internal (private) IP address to enable devices deployed in the same Azure Virtual network to connect to OVOC (see Server IP Address on page 195). See the setup of the virtual machine Step 1: Creating Virtual Machine on Azure on page 32 to find the Azure Internal IP.
5. Configure the Azure IP address/Domain Name (where OVOC is installed) as the external NTP clock source (see NTP on page 211).

> ⚠ The same clock source should be configured on the managed devices (see Configuring Mediant CE OVOC Internal IP Connection Settings using Web Interface on the next page

Configuring Mediant Cloud Edition (CE) SBC Devices on Azure (Internal IP)

This step describes the following configuration procedures on the Mediant CE to connect to the OVOC server that is deployed in the Azure Cloud in the same Virtual network by connecting through internal IP addresses on both sides:

- Configuring Mediant CE SNMP Internal IP Connection with OVOC using Stack Manager below
- Configuring Mediant CE OVOC Internal IP Connection Settings using Web Interface on the next page

Configuring Mediant CE SNMP Internal IP Connection with OVOC using Stack Manager

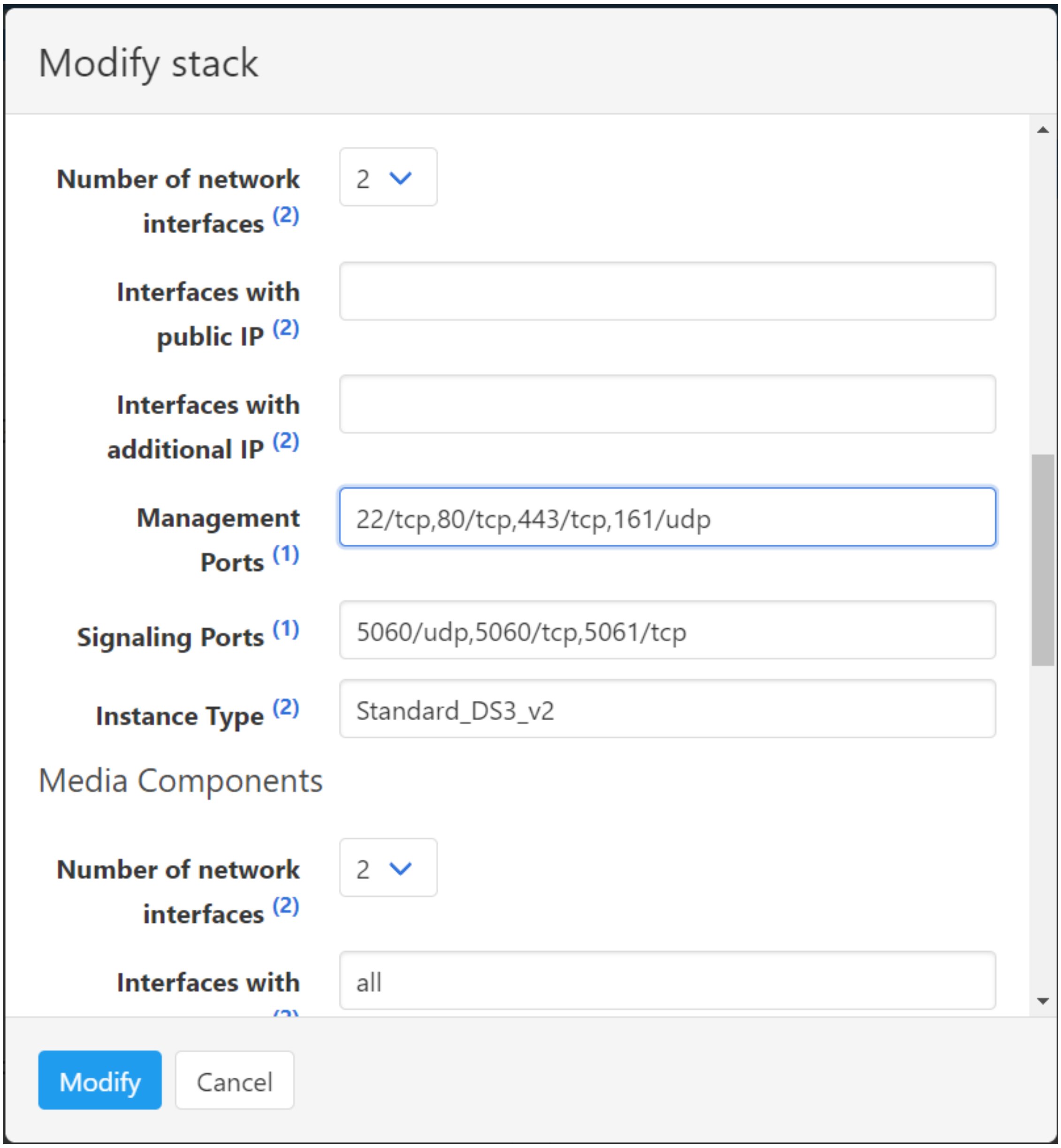
This step describes how to configure the SNMP communication between the OVOC server and Mediant CE devices using the Stack Manager when both are deployed in the same Azure Virtual network.

➢ To configure the Stack Manager:

1. Log in to the Web interface of the Stack Manager that was used to create Mediant Cloud Edition (CE) SBC. Refer to *Stack Manager for Mediant CE SBC User's Manual.*

2. Click the "Mediant CE stack".
3. Click the **Modify** button and append **161/udp port** (for SNMP traffic) to "Management Ports" parameter.
4. Click **Update** to apply the new configuration.

Figure 6-18: Modify Stack



Modify stack

Number of network interfaces (2): 2

Interfaces with public IP (2):

Interfaces with additional IP (2):

Management Ports (1): 22/tcp,80/tcp,443/tcp,161/udp

Signaling Ports (1): 5060/udp,5060/tcp,5061/tcp

Instance Type (2): Standard_DS3_v2

Media Components

Number of network interfaces (2): 2

Interfaces with: all

Configuring Mediant CE OVOC Internal IP Connection Settings using Web Interface

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

⚠ The following procedure describes the required configuration for a single CE SBC device. For mass deployment, you can load configuration files to multiple devices using 'Full' or 'Incremental' INI file options (refer to the relevant *SBC User's Manual* for more information).

➢ To configure the Mediant Cloud Edition (CE) SBC:

1. Login to the Mediant Cloud Edition (CE) SBC Web interface or connect from the Devices page in the OVOC Web interface.
2. Open the TIME & DATE page (**Setup** menu > **Administration** tab) and in the NTP Server Address field, set the Microsoft Azure site IP address/Domain Name(where the OVOC server is installed) as the NTP server clock source.
3. Click **Apply** to confirm the changes.
4. Open the SNMP Community Settings Page (**Setup** menu > **Administration** tab > **SNMP** folder).
5. Set parameter SNMP Disable to **No** ('Yes' by default).
6. Click **Apply** to confirm changes.
7. Open the Mediant Cloud Edition (CE) SBC AdminPage (deviceIPaddress/AdminPage) and configure the following ini parameters:

```
HostName = <Load Balancer IP>
SNMPManagerIsUsed_0 = 1
SNMPManagerTableIP_0 = <OVOC Server Internal IP>
```

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

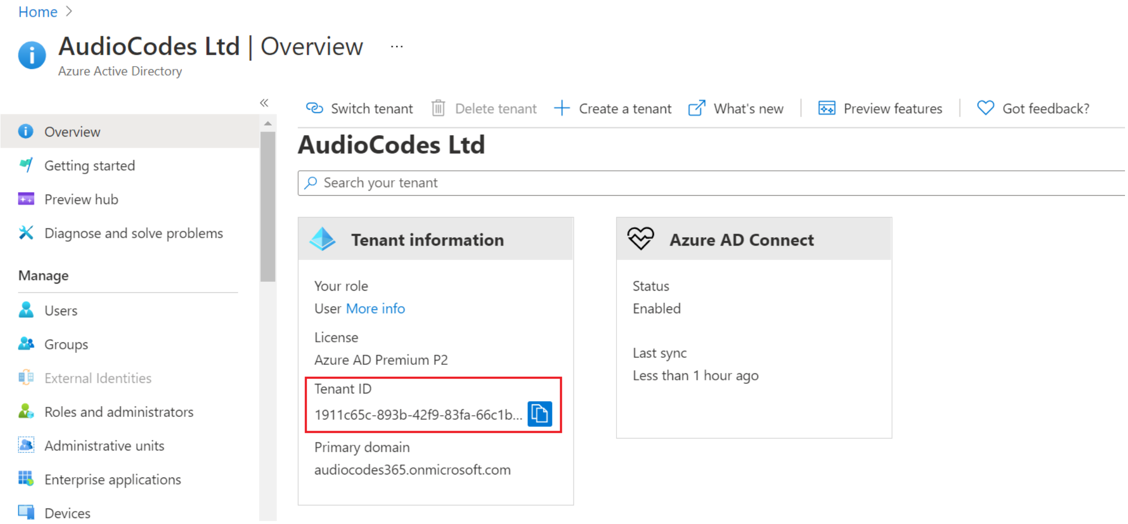
Step 4 Registering Microsoft Teams Application

This procedure describes how to register the Microsoft Teams application that is used for retrieving Call Notifications for the managed Microsoft Teams tenant.

➢ To register the application:

1. Open the Azure Portal, the Overview page is displayed with the Tenant ID of the managed Teams tenant.

Figure 6-19: Tenant ID



Your role
User More info

License
Azure AD Premium P2

Tenant ID
1911c65c-893b-42f9-83fa-66c1b...

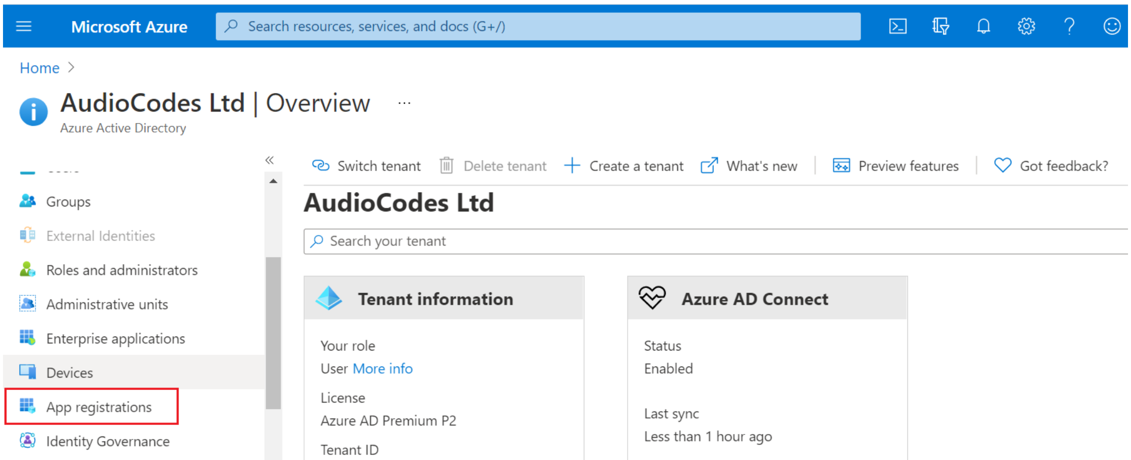
Primary domain
audiocodes365.onmicrosoft.com

Status
Enabled

Last sync
Less than 1 hour ago

2. In the Navigation pane, select **App registrations.**

Figure 6-20: App Registrations



Your role
User More info

License
Azure AD Premium P2

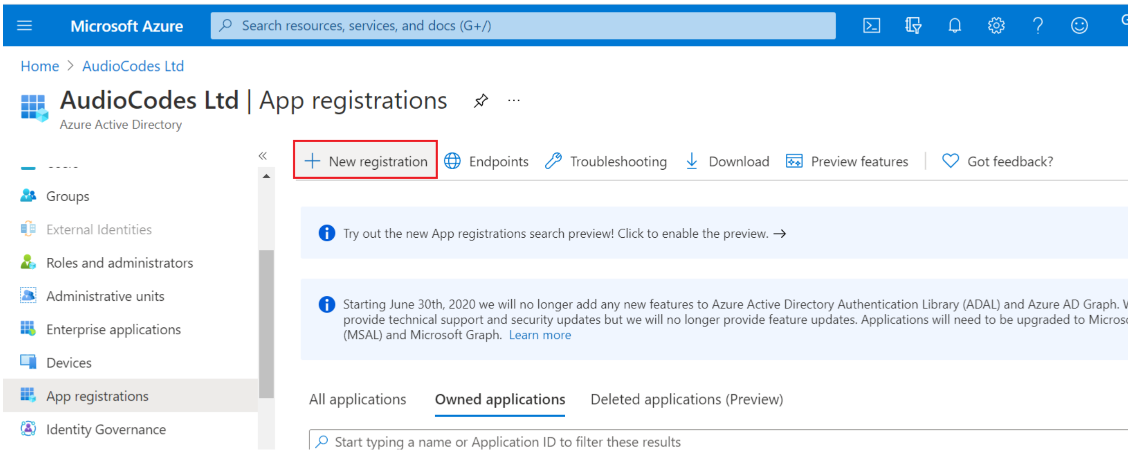
Tenant ID

Status
Enabled

Last sync
Less than 1 hour ago

3. Click **New registration.**

Figure 6-21: New registration

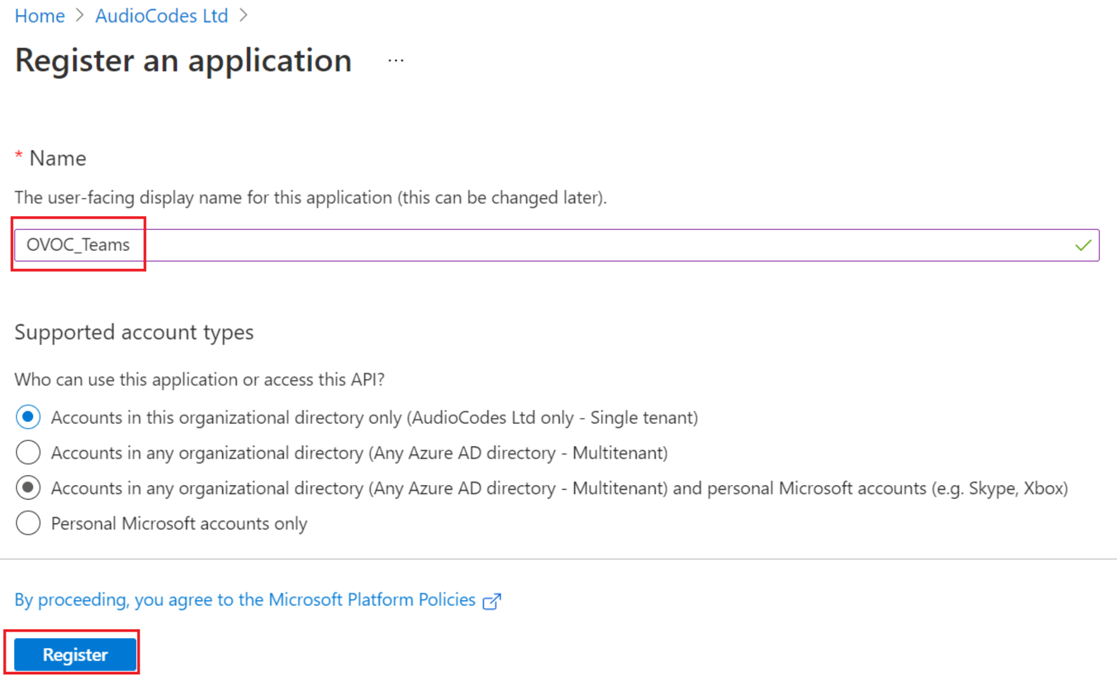


Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. W provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Micros (MSAL) and Microsoft Graph. Learn more

4. Enter the name of the application and then click **Register**.

Figure 6-22: Name the application



Home > AudioCodes Ltd >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

OVOC_Teams ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Ltd only - Single tenant)

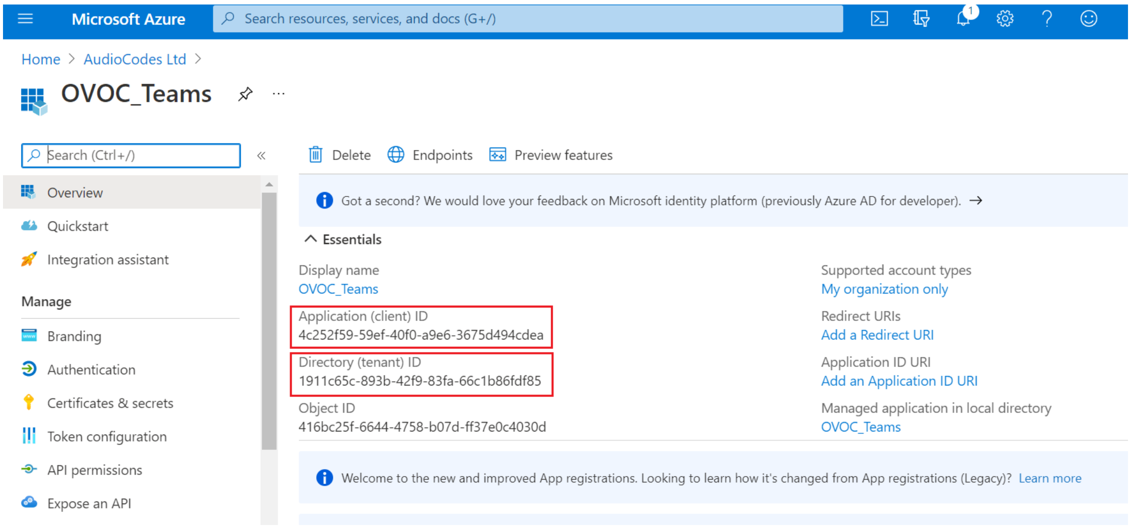
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

By proceeding, you agree to the Microsoft Platform Policies

Figure 6-23: Successful Registration



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

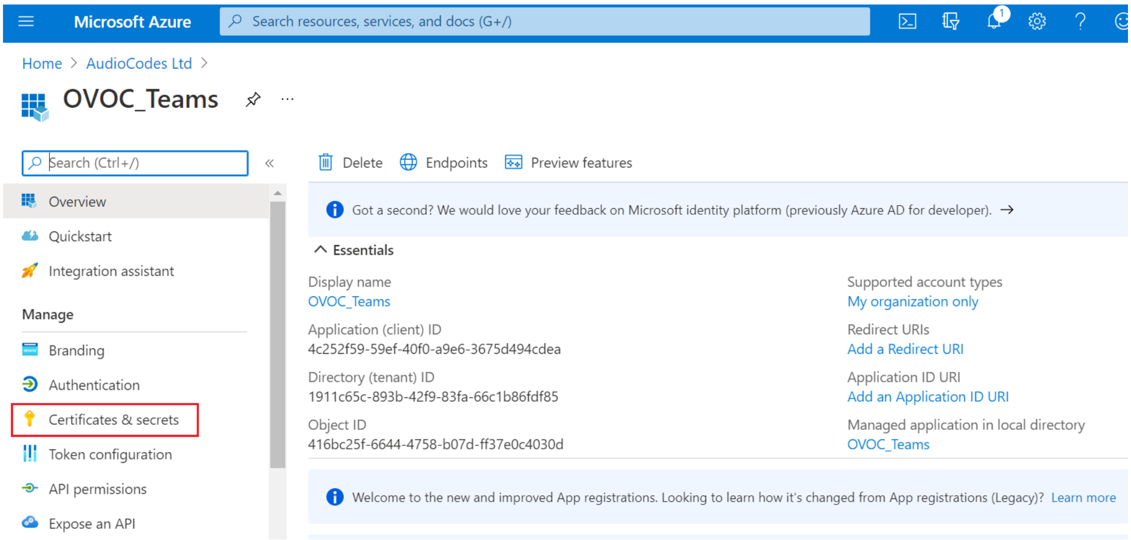
Essentials

Display name OVOC_Teams	Supported account types My organization only
Application (client) ID 4c252f59-59ef-40f0-a9e6-3675d494cdea	Redirect URIs Add a Redirect URI
Directory (tenant) ID 1911c65c-893b-42f9-83fa-66c1b86fdf85	Application ID URI Add an Application ID URI
Object ID 416bc25f-6644-4758-b07d-ff37e0c4030d	Managed application in local directory OVOC_Teams

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

5. In the Navigation pane select **Certificate & Secrets.**

Figure 6-24: Certificate & Secrets



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name: OVOC_Teams

Application (client) ID: 4c252f59-59ef-40f0-a9e6-3675d494cdea

Directory (tenant) ID: 1911c65c-893b-42f9-83fa-66c1b86fdf85

Object ID: 416bc25f-6644-4758-b07d-ff37e0c4030d

Supported account types: My organization only

Redirect URIs: Add a Redirect URI

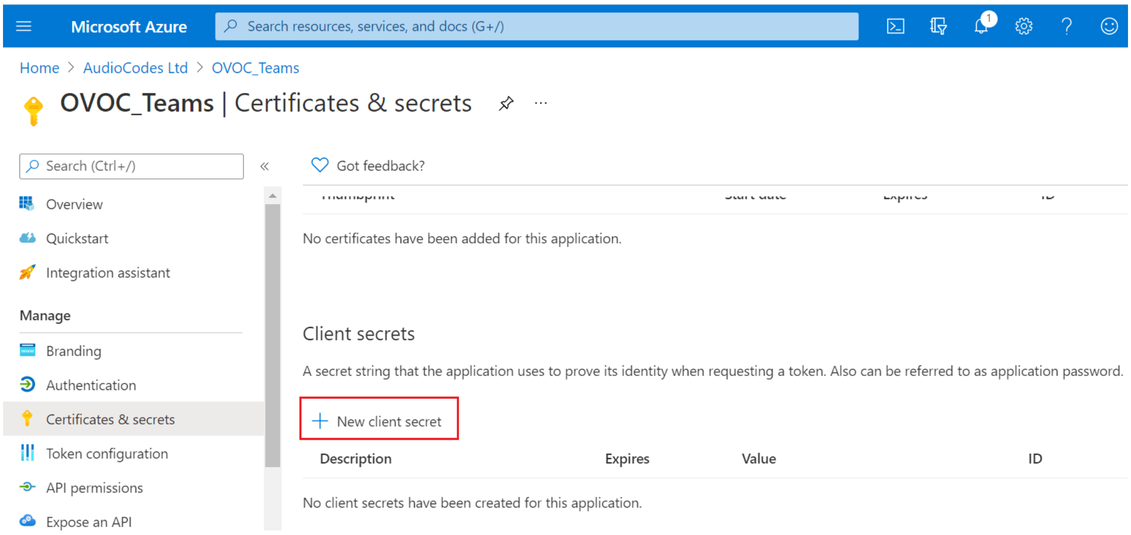
Application ID URI: Add an Application ID URI

Managed application in local directory: OVOC_Teams

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

6. Click **New client secret**.

Figure 6-25: New Client Secret



No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

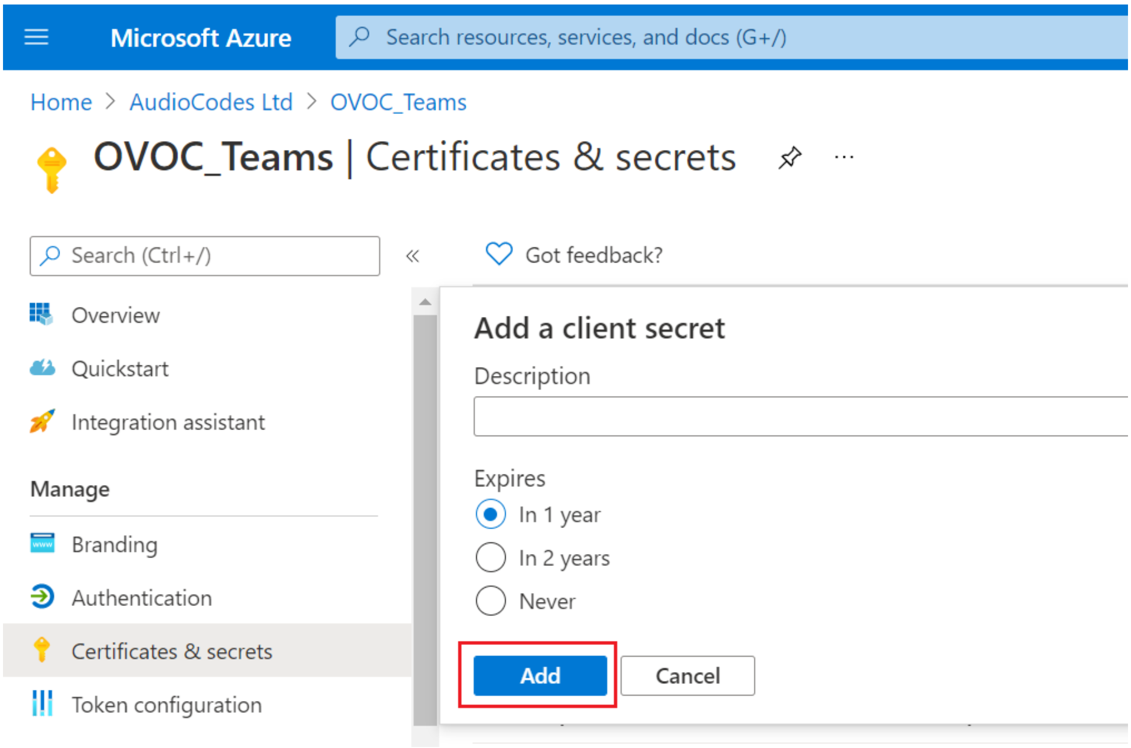
Description	Expires	Value	ID

No client secrets have been created for this application.

7. Click **Add**.

The newly added client secret is added as shown in the figure below.

Figure 6-26: Add a client secret



Add a client secret

Description

Expires

● In 1 year

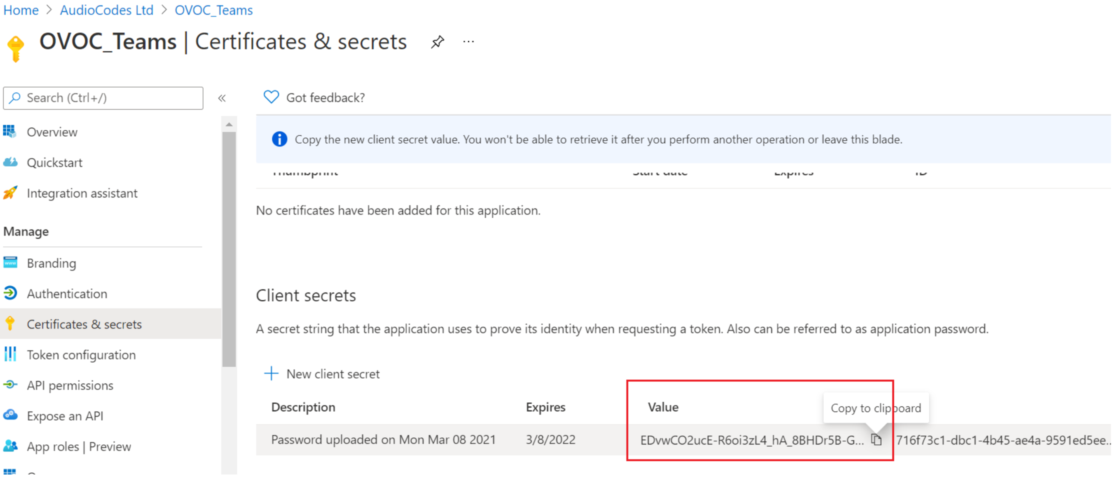
○ In 2 years

○ Never

Add | Cancel

8. The client secret is added as shown in the screen below. Copy it to the clipboard as you will be required to enter it in later configuration.

Figure 6-27: Added Certificates & Secrets



Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	
Password uploaded on Mon Mar 08 2021	3/8/2022	EDvwCO2ucE-R6oi3zL4_hA_8BHDr5B-G...	716f73c1-dbc1-4b45-ae4a-9591ed5ee..

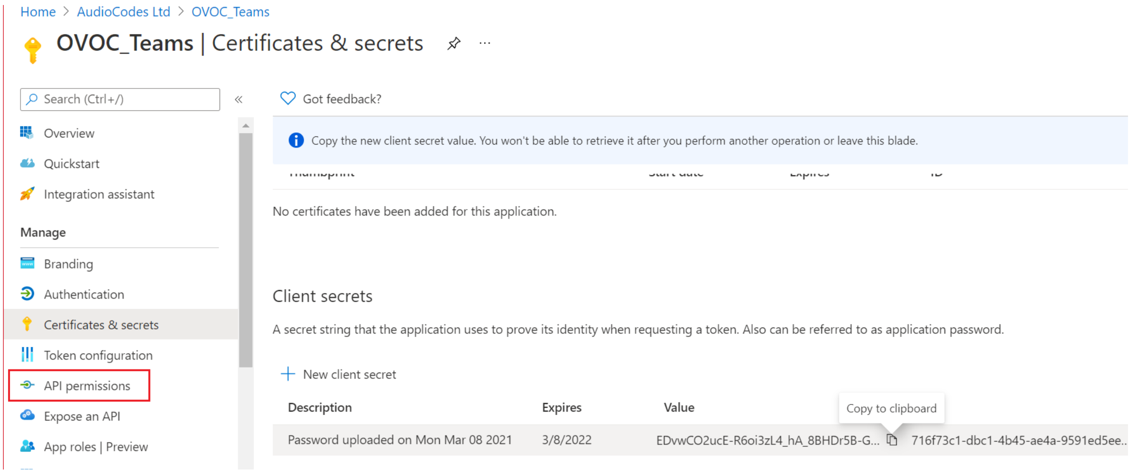
Step 5 Configuring Microsoft Graph API Permissions

This procedure describes how to configure the appropriate permissions to connect to Microsoft Graph API that is used to interface with Microsoft Teams to retrieve the Call Notifications.

➢ To configure Microsoft Graph permissions:

1. In the Navigation pane, select **API permissions**.

Figure 6-28: API Permissions



Home > AudioCodes Ltd > OVOC_Teams

OVOC_Teams | Certificates & secrets

Search (Ctrl+/)

Got feedback?

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

No certificates have been added for this application.

Client secrets

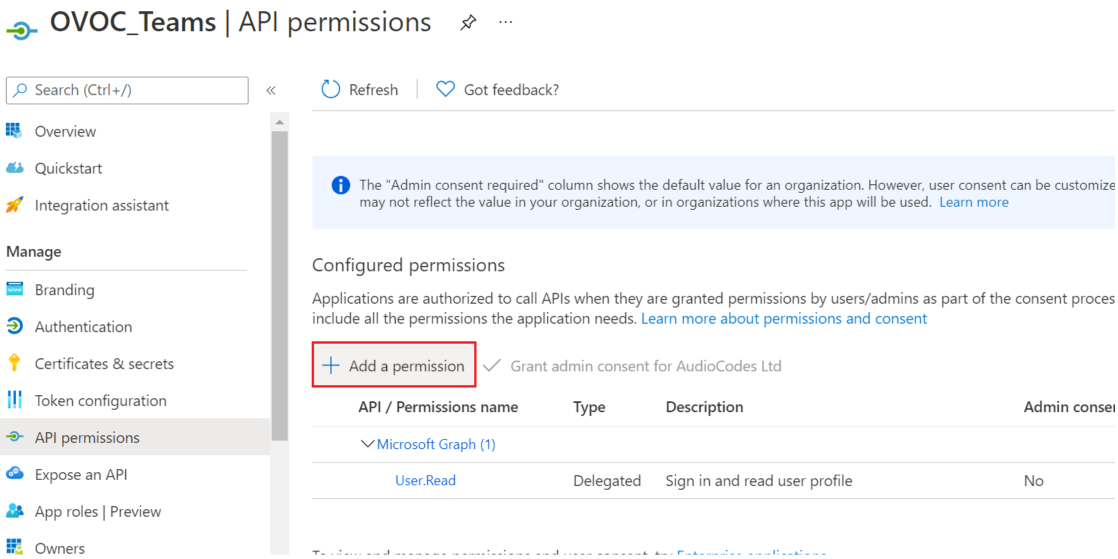
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	
Password uploaded on Mon Mar 08 2021	3/8/2022	EDvwCO2ucE-R6oi3zL4_hA_8BHDr5B-G...	716f73c1-dbc1-4b45-ae4a-9591ed5ee..

2. Click **Add a permission.**

Figure 6-29: Add a permission



OVOC_Teams | API permissions

Search (Ctrl+/)

Refresh | Got feedback?

The "Admin consent required" column shows the default value for an organization. However, user consent can be customize may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent proces include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for AudioCodes Ltd

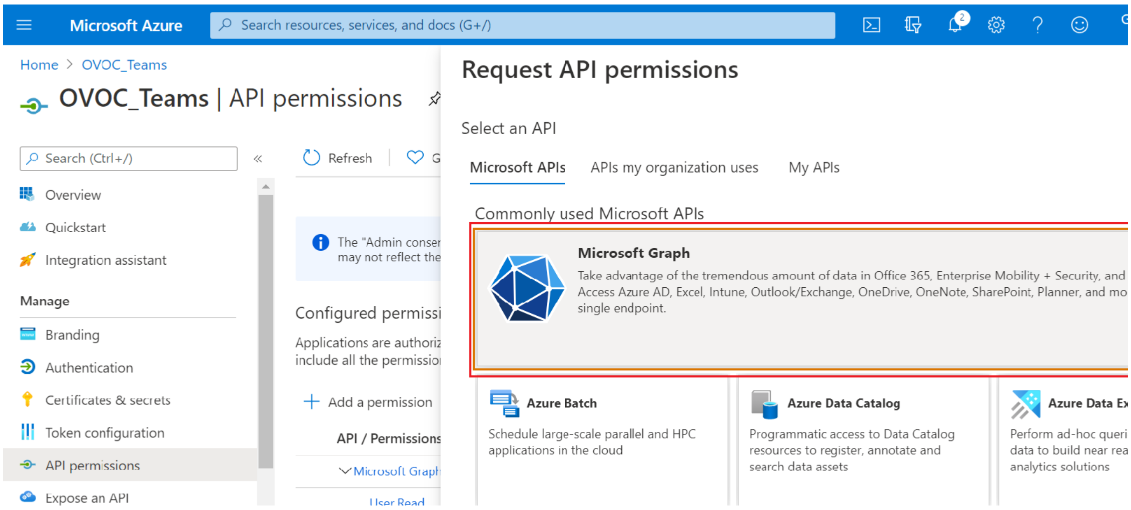
API / Permissions name	Type	Description	Admin consei
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

3. Select **Grant Admin Consent for** …. and select **Yes**.

If the App hasn't been granted admin consent, users are prompted to grant consent the first time they use the App.

4. Select **Microsoft Graph**.

Figure 6-30: Request API Permissions



The "Admin conser may not reflect the

Applications are authoriz include all the permissio

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and mo single endpoint.

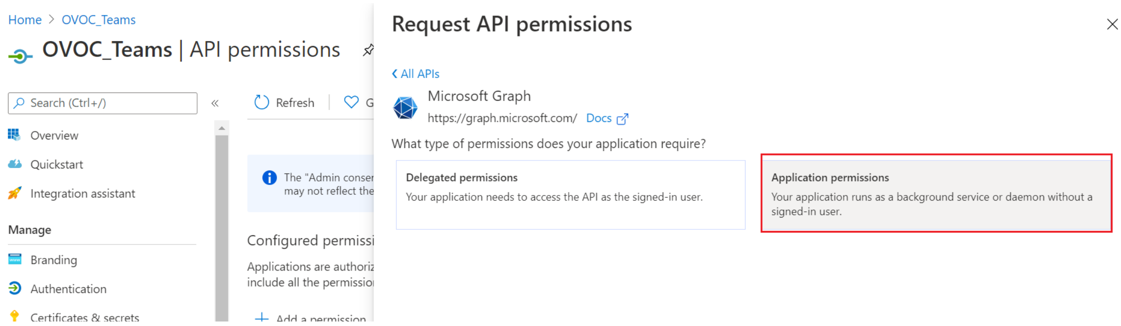
Schedule large-scale parallel and HPC applications in the cloud

Programmatic access to Data Catalog resources to register, annotate and search data assets

Perform ad-hoc queri data to build near rea analytics solutions

5. Select **Application permissions**.

Figure 6-31: Application permissions



The "Admin conser may not reflect the

Applications are authoriz include all the permissio

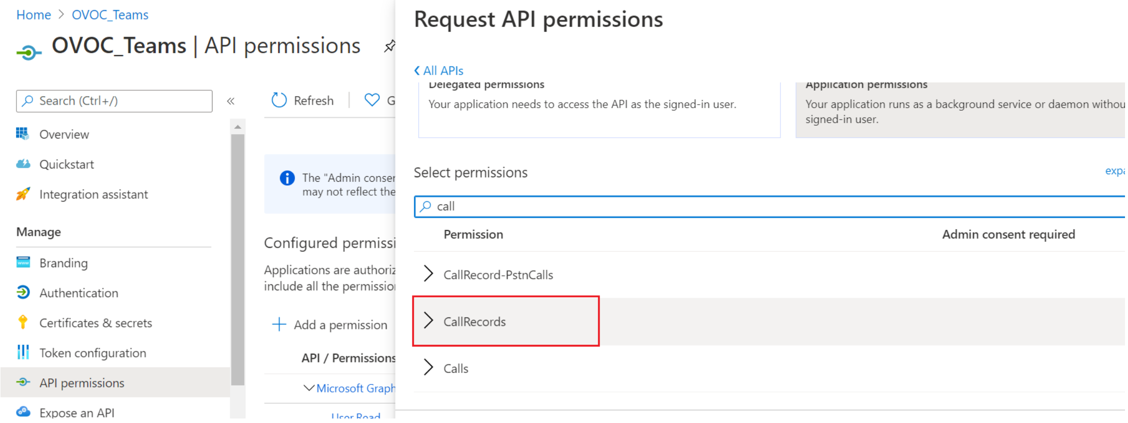
What type of permissions does your application require?

Your application needs to access the API as the signed-in user.

Your application runs as a background service or daemon without a signed-in user.

6. Search for Permission **Call Records**.

Figure 6-32: Call Records



The "Admin conser may not reflect the

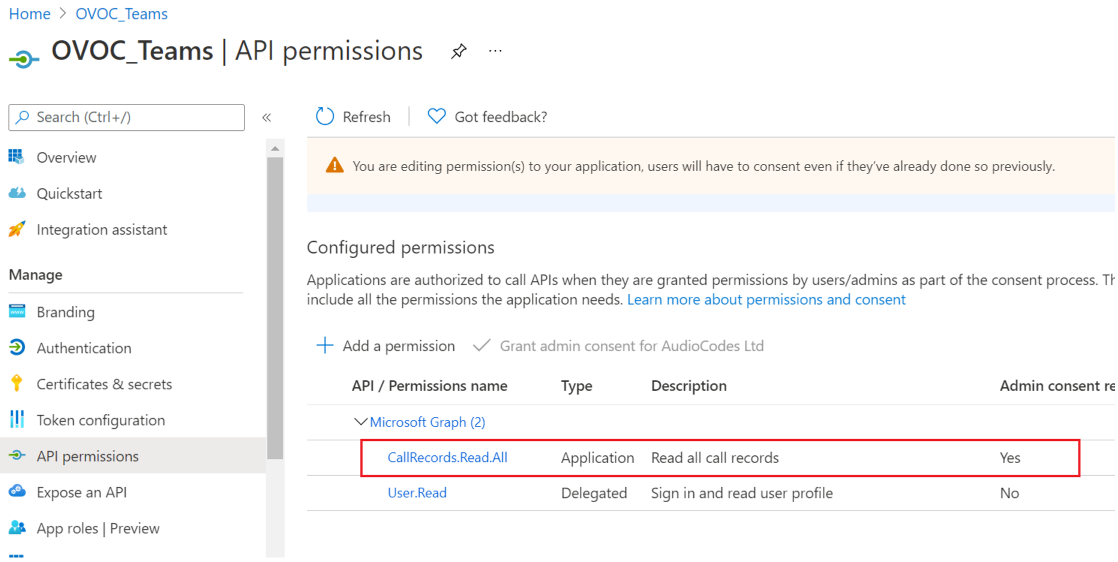
Applications are authoriz include all the permissio

Your application needs to access the API as the signed-in user.

Your application runs as a background service or daemon withou signed-in user.

7. Set permission **CallRecords.Read.All** to enable access to retrieved call notifications.

Figure 6-33: API Permissions



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

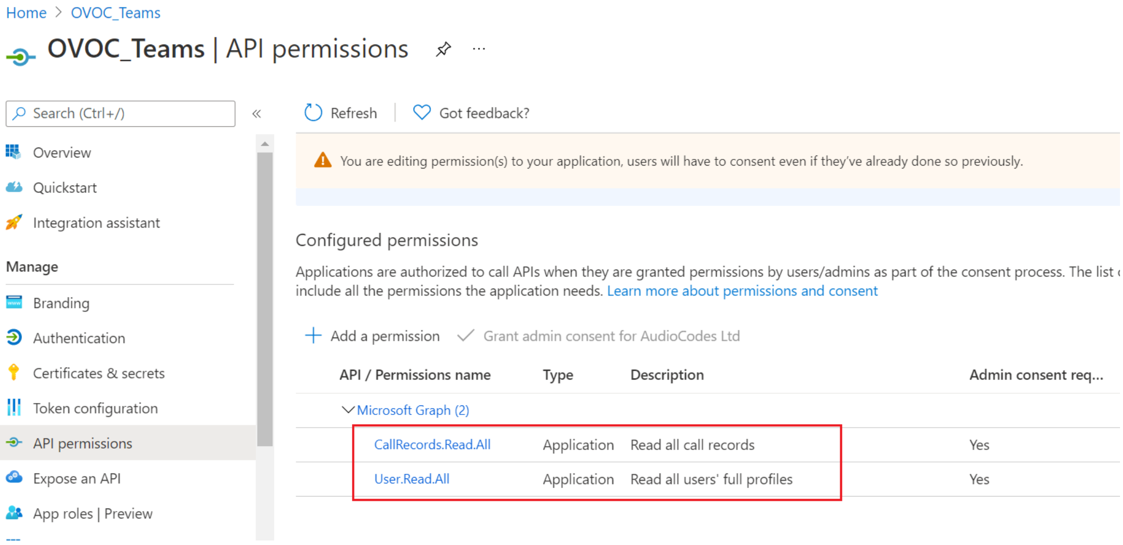
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. Th include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent re
Microsoft Graph (2)			
CallRecords.Read.All	Application	Read all call records	Yes
User.Read	Delegated	Sign in and read user profile	No

8. You can optionally set permission **User.Read** to display caller details in retrieved call records.

Figure 6-34: User Read Permissions



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (2)			
CallRecords.Read.All	Application	Read all call records	Yes
User.Read.All	Application	Read all users' full profiles	Yes

Step 6 Configuring AudioCodes Azure Active Directory (Operator Authentication)

This procedure describes how to configure security permissions for OVOC operators who are authenticated with Azure Active Directory (when the "Azure" authentication type is configured in the OVOC Web (**Security** > **Authentication** settings page).

➢ To configure Microsoft Azure:

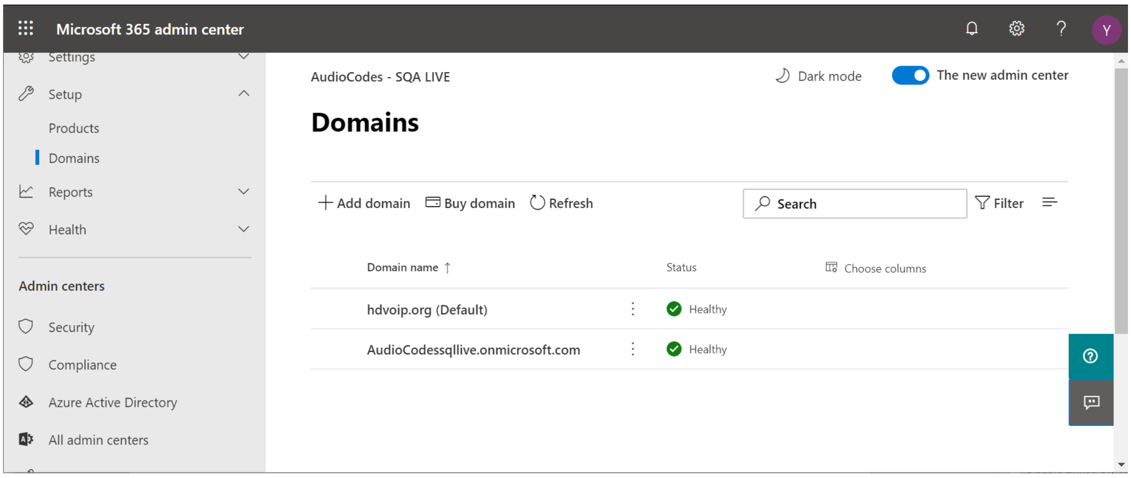
1. **Add Service Providers Account Domain:**

   a. Open the Microsoft 365 Admin Center.

   b. Login to AudioCodes with administrator privileges (via office.com).

c. In the Navigation pane, select **Setup** > **Domains**

Figure 6-35: Domains



Domain name ↑	Status
hdvoip.org (Default)	Healthy
AudioCodessqllive.onmicrosoft.com	Healthy

2. **Create a new Tenant in the Azure Portal:** Sign into Azure portal as Global Administrator and extract the Tenant ID of your directory (required for the OVOC Azure authentication setup in OVOC Azure Configuration).

   For details, see https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant

3. **Add Tenant Operators on AudioCodes Microsoft Azure:**

- You must change passwords for new users upon first login via Azure portal sign-in before logging in to OVOC.
- At this stage guest users you invite from another tenants/directories are not fully supported by OVOC.
- For details, refer to the following:
  - ✔ https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal#create-a-basic-group-and-add-members
  - ✔ https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory#add-a-new-user

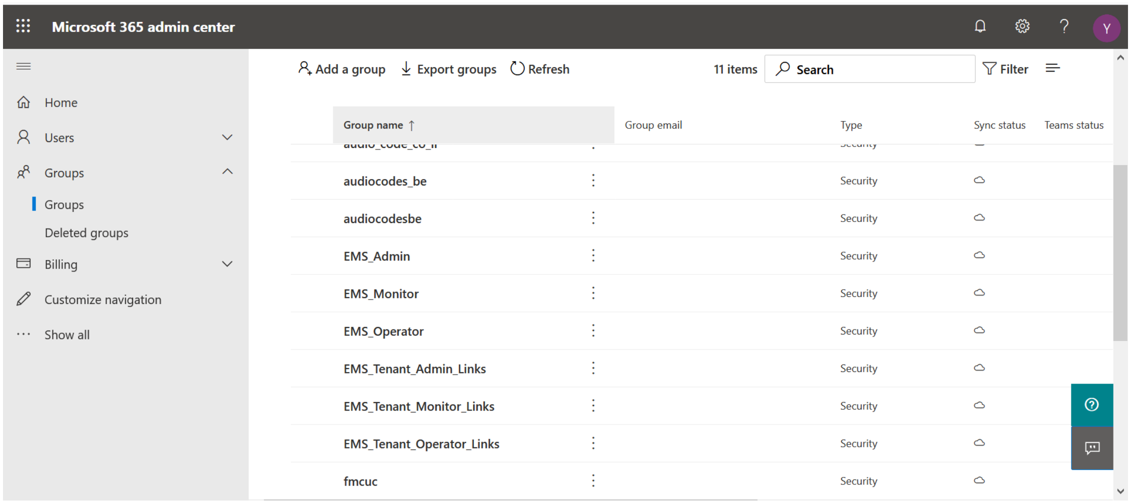
4. **Add Security Groups:**

   a. Open AudioCodes Office 365.

   b. Open the Admin page.

   c. In the Navigation pane, select **Groups**.

Figure 6-36: Add a Security Group



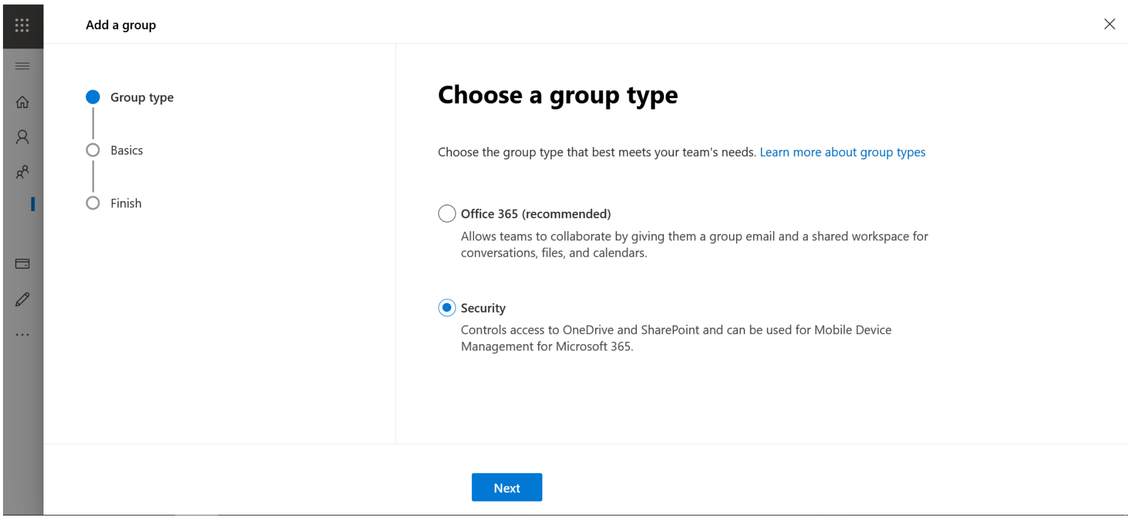
Group name ↑	Group email	Type	Sync status	Teams status
audiocodes_be		Security		
audiocodesbe		Security		
EMS_Admin		Security		
EMS_Monitor		Security		
EMS_Operator		Security		
EMS_Tenant_Admin_Links		Security		
EMS_Tenant_Monitor_Links		Security		
EMS_Tenant_Operator_Links		Security		
fmcuc		Security		

A list of existing groups are displayed. Note that there are several predefined custom security groups that have been predefined for OVOC displayed in the screen below with ‘EMS_’ prefix.

d. Click **Add a group**.

e. Select the Security option and then click **Next**.

Figure 6-37: Choose a Group Type



Choose a group type

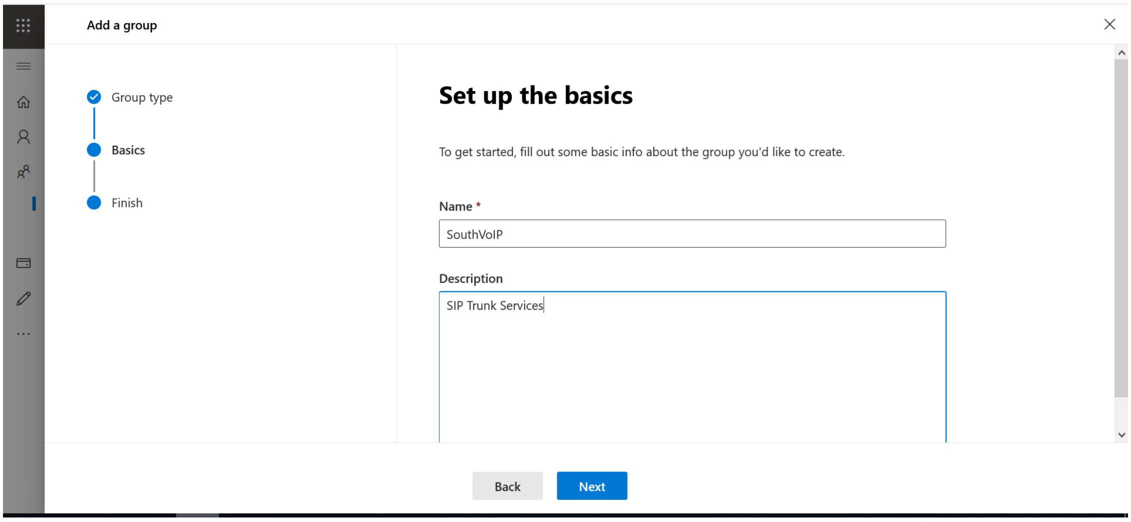
Choose the group type that best meets your team's needs. Learn more about group types

○ Office 365 (recommended)
Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars.

● Security
Controls access to OneDrive and SharePoint and can be used for Mobile Device Management for Microsoft 365.

f. Enter the Service Provider Domain account name and then click **Next**.

Figure 6-38: Setup the Basics



Set up the basics

To get started, fill out some basic info about the group you'd like to create.

Name *

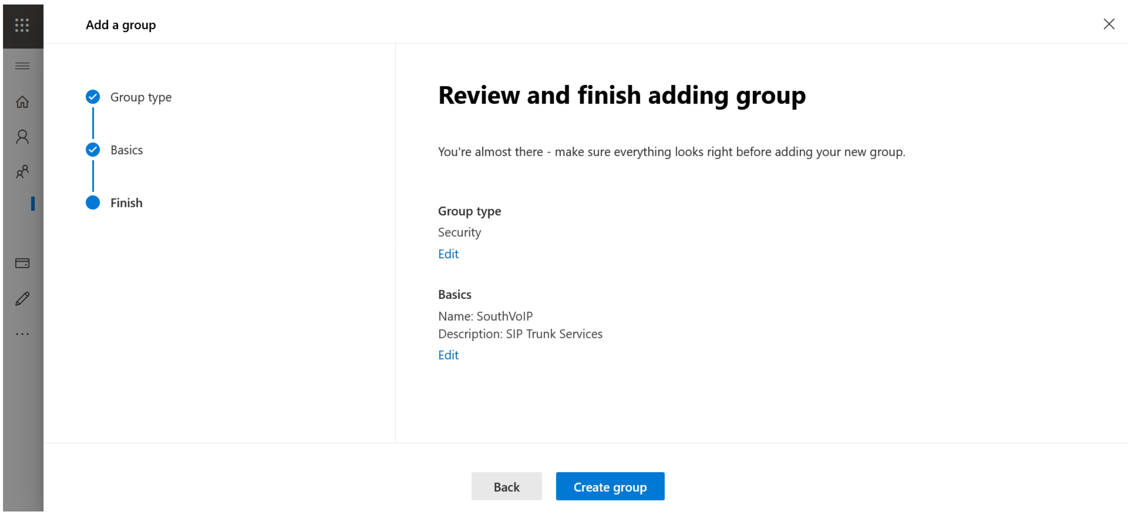
SouthVoIP

Description

SIP Trunk Services

g. Review and finish adding group.

Figure 6-39: Review and Finish



Review and finish adding group

You're almost there - make sure everything looks right before adding your new group.

Group type

Security

Edit

Basics

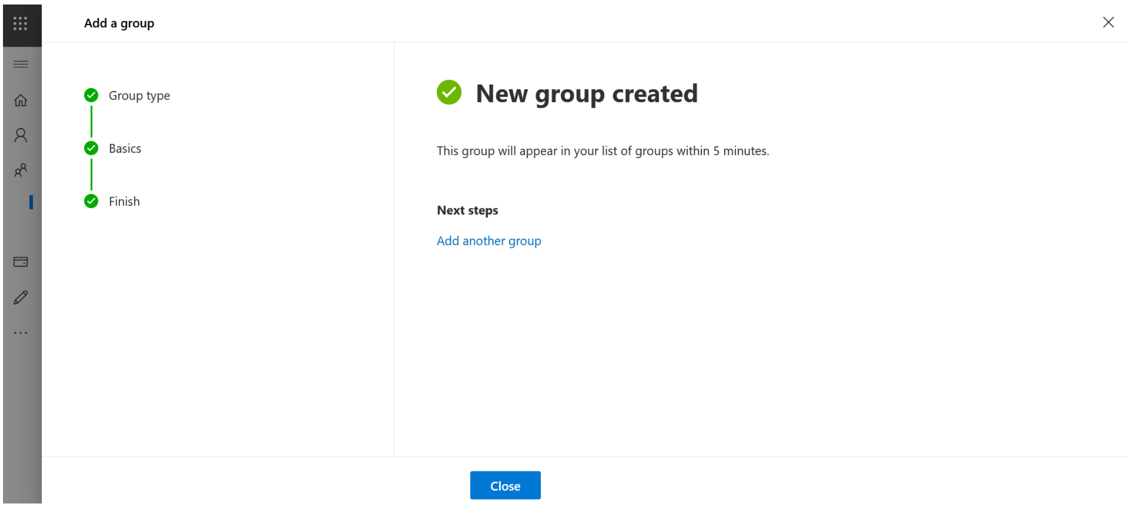
Name: SouthVoIP

Description: SIP Trunk Services

Edit

h. Click **Create group**. A confirmation screen is displayed:

Figure 6-40: New Group Created



New group created

This group will appear in your list of groups within 5 minutes.

Next steps

Add another group

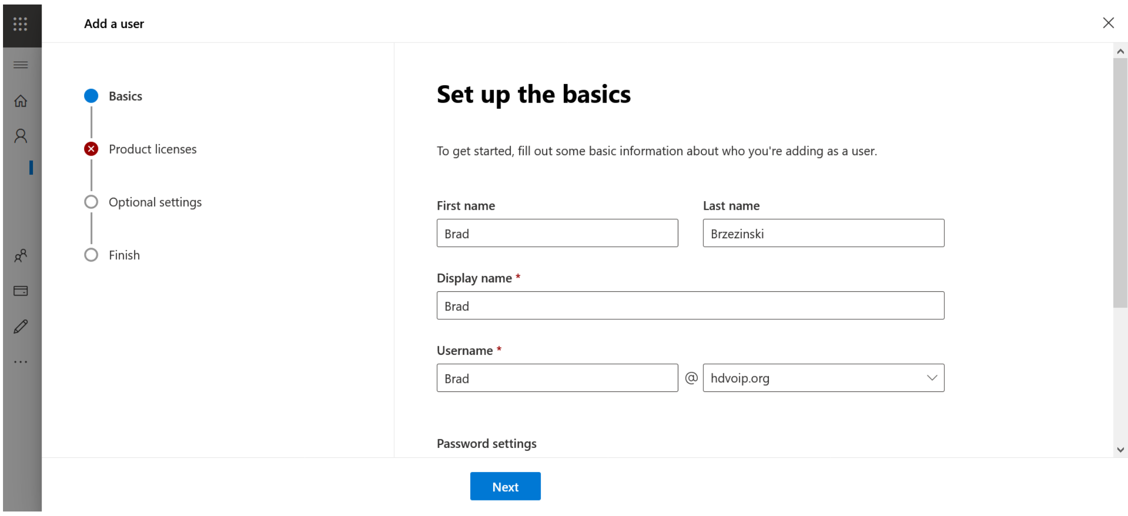
5. **Add New Users:**

   a. In the Navigation pane, select **Active Users**.

   b. Click **Add a User**.

   c. Enter the details of the Service Provider account user.

Figure 6-41: Create New User



Add a user

● Basics
☒ Product licenses
○ Optional settings
○ Finish

Set up the basics

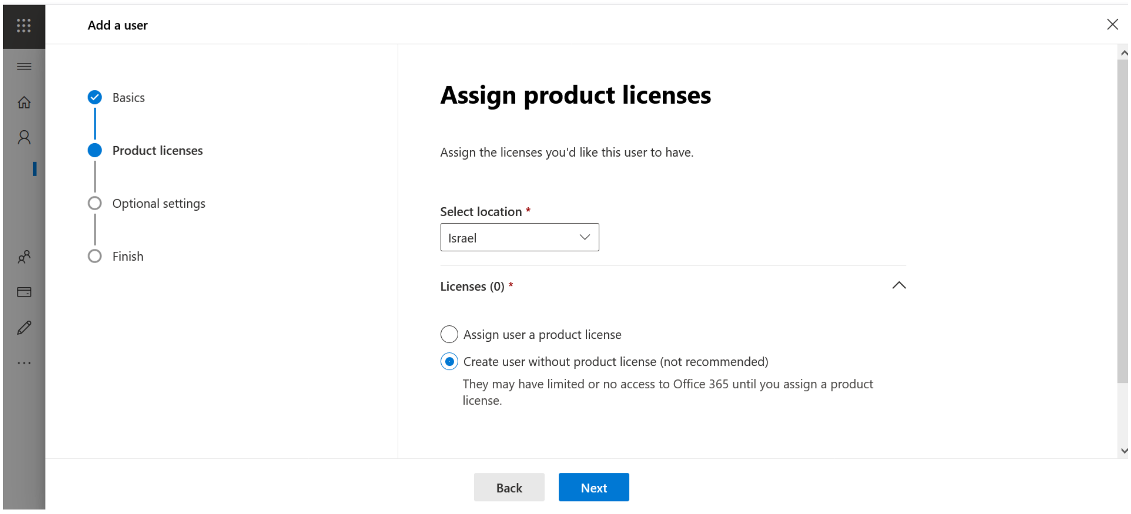
To get started, fill out some basic information about who you're adding as a user.

First name: Brad
Last name: Brzezinski
Display name *: Brad
Username *: Brad @ hdvoip.org

Password settings

   d. Assign Product License (Choose country).

Figure 6-42: Assign Product Licenses



Add a user

✓ Basics
● Product licenses
○ Optional settings
○ Finish

Assign product licenses

Assign the licenses you'd like this user to have.

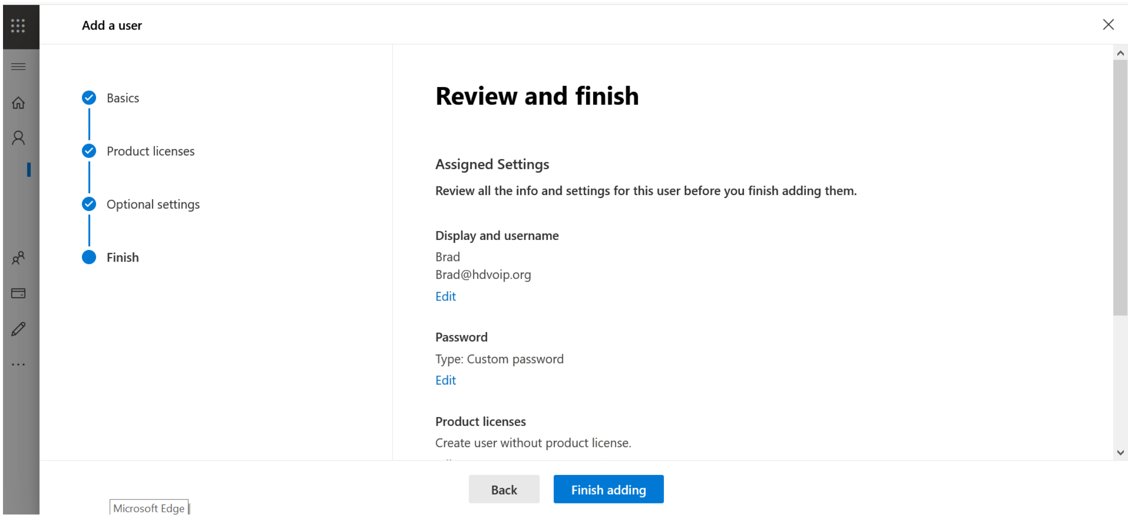
Select location *: Israel

Licenses (0) *

○ Assign user a product license
● Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

   e. Select option **create user without product license** and then click **Next**.

Figure 6-43: Review and finish



Review and finish

Assigned Settings

Review all the info and settings for this user before you finish adding them.

Display and username
Brad
Brad@hdvoip.org
Edit

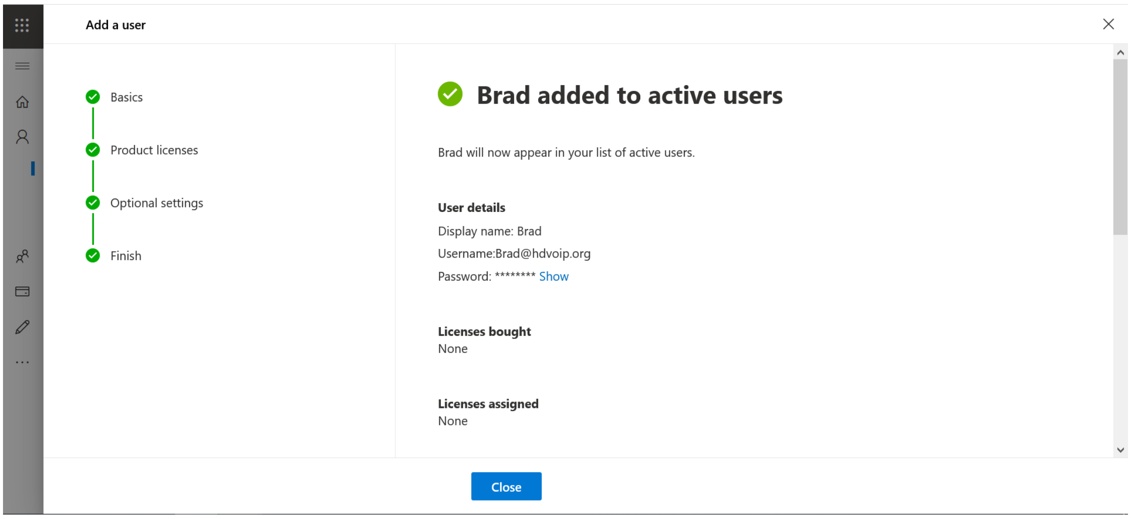
Password
Type: Custom password
Edit

Product licenses
Create user without product license.

f. Click **Finish adding**.

g. Select option create user without product license and then click **Next**.

Figure 6-44: Review and Finish



Brad added to active users

Brad will now appear in your list of active users.

User details
Display name: Brad
Username:Brad@hdvoip.org
Password: ******** Show

Licenses bought
None

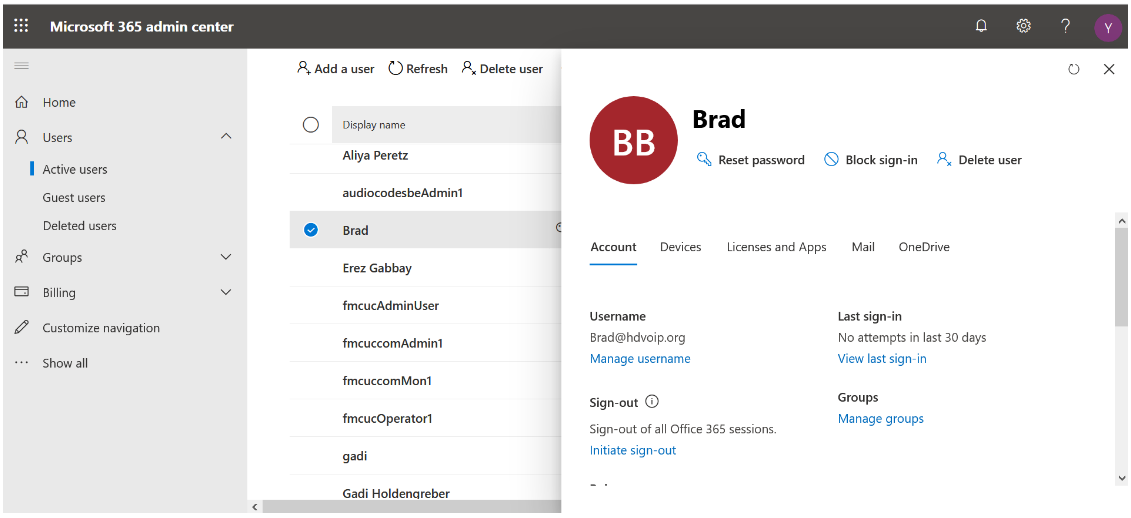
Licenses assigned
None

h. Click **Finish adding**

6. **Add User Membership:** add user membership to the predefined One Voice Live Security groups and to the Security Group that you defined above.

   a. In the Navigation pane, select **Active Users** and then select the new user that you created above.

Figure 6-45: Add User Membership



Microsoft 365 admin center

Home
Users
Active users
Guest users
Deleted users
Groups
Billing
Customize navigation
Show all

Add a user | Refresh | Delete user

	Display name
○	Aliya Peretz
	audiocodesbeAdmin1
✓	Brad
	Erez Gabbay
	fmcucAdminUser
	fmcuccomAdmin1
	fmcuccomMon1
	fmcucOperator1
	gadi
	Gadi Holdengreber

BB Brad

Reset password | Block sign-in | Delete user

Account | Devices | Licenses and Apps | Mail | OneDrive

Username
Brad@hdvoip.org
Manage username

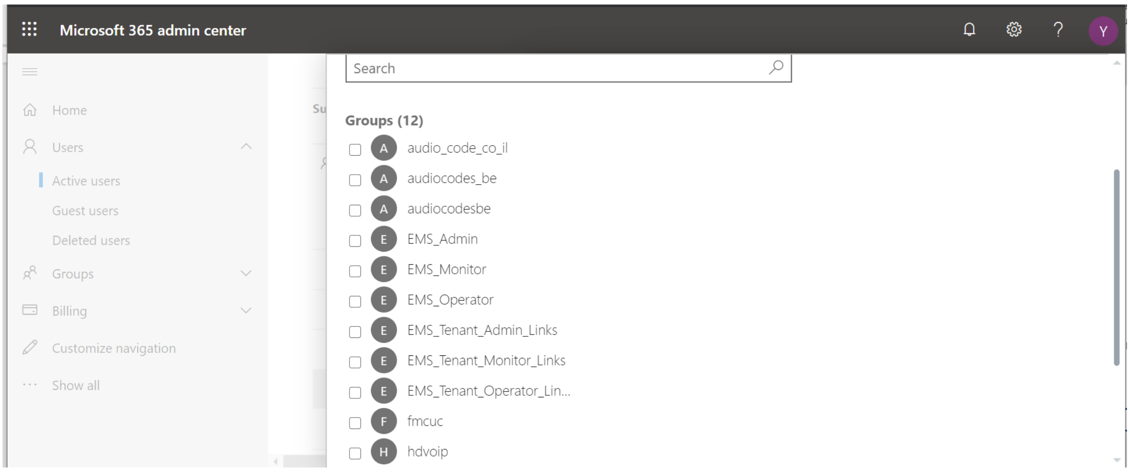
Last sign-in
No attempts in last 30 days
View last sign-in

Sign-out
Sign-out of all Office 365 sessions.
Initiate sign-out

Groups
Manage groups

b. Click **Manage groups** and then **Add Membership**.

Figure 6-46: Add Membership



Microsoft 365 admin center

Search

Groups (12)

- □ A audio_code_co_il
- □ A audiocodes_be
- □ A audiocodesbe
- □ E EMS_Admin
- □ E EMS_Monitor
- □ E EMS_Operator
- □ E EMS_Tenant_Admin_Links
- □ E EMS_Tenant_Monitor_Links
- □ E EMS_Tenant_Operator_Lin...
- □ F fmcuc
- □ H hdvoip

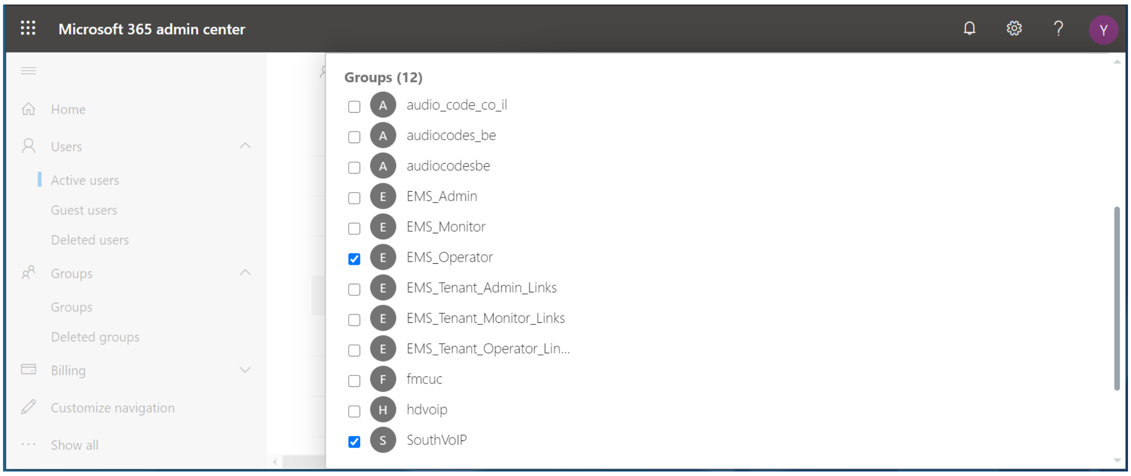
c. Select the checkboxes adjacent to the required OVOC group permissions :

- EMS_Tenant_Admin_Links
- EMS_Tenant_Operator_Links
- EMS_Tenant_Monitor_Links

d. Add membership to the Service Provider Account Group i.e. the Security Group that you created above.

In the example below membership has been added to the 'EMS_Operator' and 'SouthVoIP' Group.

Figure 6-47: Add Membership



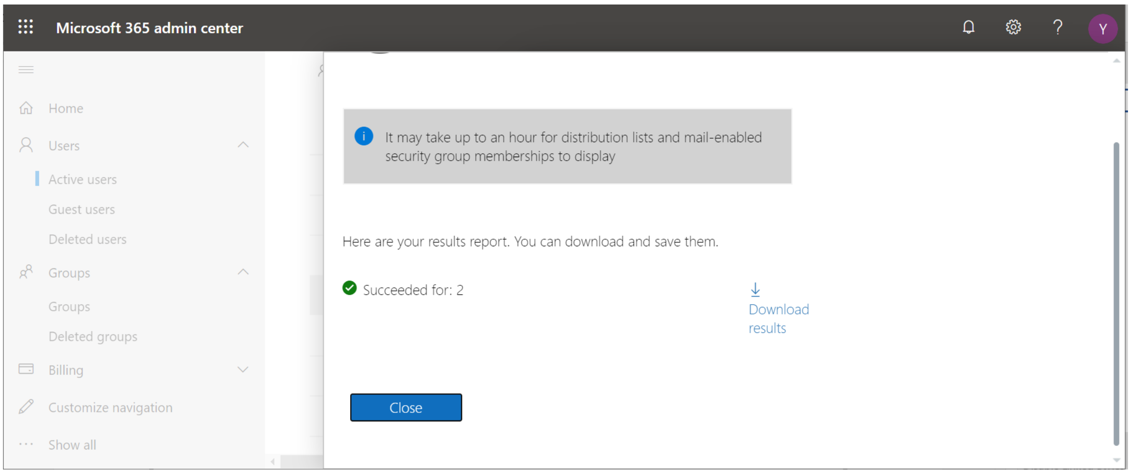
Groups (12)

- □ audio_code_co_il
- □ audiocodes_be
- □ audiocodesbe
- □ EMS_Admin
- □ EMS_Monitor
- ☑ EMS_Operator
- □ EMS_Tenant_Admin_Links
- □ EMS_Tenant_Monitor_Links
- □ EMS_Tenant_Operator_Lin...
- □ fmcuc
- □ hdvoip
- ☑ SouthVoIP

This Group Name corresponds to the "AD Authentication: Group Name" that is configured for the OVOC Tenant created for this account in OVOC.

e. Click Save and close.

Figure 6-48: Successful Membership Assignment



It may take up to an hour for distribution lists and mail-enabled security group memberships to display

Here are your results report. You can download and save them.

Succeeded for: 2

7. **Register new WEB Application:** See [https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app.](https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app)

- The Redirect URI step should be configured like WEB and OVOC's login endpoint should be specified as URI: https://<IP address>/ovoc/v1/security
- Generally for this step you should only keep the Client ID of your application that you need to specify in OVOC Microsoft Azure authentication setup (see Authentication and Authorization using Microsoft Azure).

8. **Create Client Secret for your Registered Application:** See https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#add-credentials-to-your-web-application. You must configure this secret in Authentication and Authorization using Microsoft Azure.

9. **Grant API Permissions:** Extend default application's permissions set and give admin consent to all the existing permissions. Add and provide admin consent to such delegated Microsoft Graph API related permissions**: Group.Read.All**.

   For more details, refer to the following:

   - https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#add-permissions-to-access-web-apis
   - https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#understanding-api-permissions-and-admin-consent-ui

7 Installing OVOC Server on VMware Virtual Machine

This describes how to install the OVOC server on a VMware vSphere machine. This procedure takes approximately 30 minutes. This time is estimated on the HP DL 360 G8 platform (with CPU, disk and memory as specified in Configuring the Virtual Machine Hardware Settings on page 85). The upgrade time depends on the hardware machine where the VMware vSphere platform is installed.

- Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8). Failure to meet these requirements will lead to the aborting of the installation.
- For obtaining the installation files, see OVOC Software Deliverables on page 15
  - ✓ Note that you must verify this file, see Files Verification on page 18

Deploying OVOC Image with VMware vSphere Hypervisor (ESXi)

This section describes how to deploy the OVOC image with the VMware ESXi Web client. This procedure is run using the VMware OVF tool that can be installed on any Linux machine.

- This procedure describes how to deploy the image using the OVF tool, which can be downloaded from: https://www.vmware.com/support/developer/ovf/
- The OVOC image can also be deployed using the vSphere web client GUI.

➢ **To run VMware OVF tool:**

1. Transfer the 7z file containing the VMware Virtual Machine installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 295 for instructions on how to transfer files).
2. Open the VMware OVF tool.
3. Enter the following commands and press Enter:

```
ovftool --disableVerification --noSSLVerify --name=$VMname --
datastore=$DataStore -dm=thin --acceptAllEulas --powerOn $ovaFilePath
vi://$user:$password@$vCenterIP/$dataCenterName/host/$clusterName/$E
SXIHostName
```

Where:

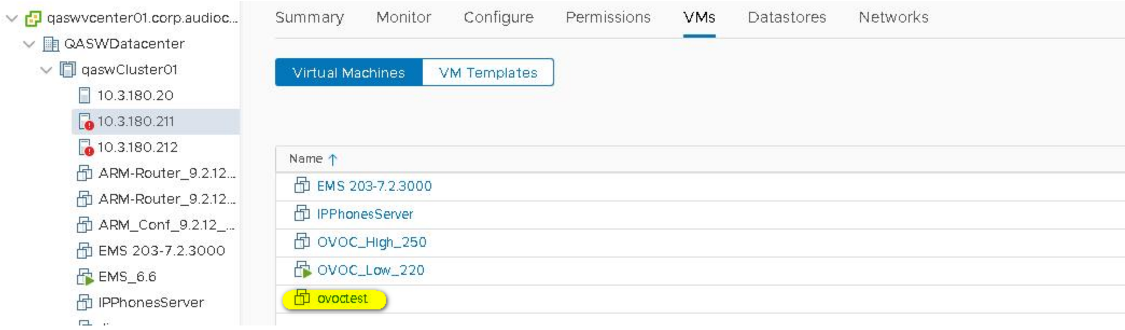
- $VMname(--name): is the name of the deployed machine
- $DataStore: data store for deployment

- $user:$password is the user and password of the VMware Host machine
- $vCenterIP: vCenter IP Address
- $dataCenterName: data center name inside the vCenter
- $clusterName: cluster name under data center tree
- $ESXIHostName: deployed ESXI IP Address

Example:

```
ovftool --disableVerification --noSSLVerify --name=ovoctest --
datastore=Netapp04.lun1 -dm=thin --acceptAllEulas --powerOn
c:\tmp\OVOC_VMware_7.8.2241.ova
vi://vmware:P@ssword123@10.3.94.68/QASWDatacenter/host/qaswCluster
01/10.3.180.211
```

Figure 7-1: OVF Example



The following progress is displayed:

```
Opening OVA source: /data1/ 8.0.110/DVD5/ 8.0.110.xxxx/OVOC-VMware-
8.0.110.xxxx.ova
Opening VI target: vi://root@172.17.135.9:443/
Deploying to VI: vi://root@172.17.135.9:443/
Disk progress: 10%
```

```
Transfer Completed
The manifest validates
Powering on VM: FirstDeploy
Task Completed
Warning:
- No manifest entry found for: 'OVOC-VMware- 8.0.110.xxxx-disk1.vmdk'.
Completed successfully
```

Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) in Service Provider Cluster

This procedure describes how to deploy the OVOC image with VMware vSphere Hypervisor (ESXi) in Service Provider Cluster. The procedure requires you to perform the following steps:

1. On existing OVOC server VM, perform full backup and upgrade to version 8.0.110 (see Step 1 Upgrade Existing Virtual Machine below)
2. On a new VM, install version 8.0.110 Service Provider Cluster **Management OVA** and restore the backup created in step 1 (seeStep 2 Install Service Provider Cluster on Management Server on page 70)
3. On a new VM, install version 8.0.110 Service Provider Cluster **VQM OVA** (seeStep 3 Install VQM Server on page 71)
4. On a new VM, install version 8.0.110 Service Provider Cluster **PM OVA** (see Step 4 Install PM Server on page 71)

Step 1 Upgrade Existing Virtual Machine

Before installing the Service Provider Cluster, you must upgrade your existing virtual machine to OVOC Version 8.0.110

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 existing OVOC server VM:

1. Using the WinSCP utility (see Transferring Files on page 295), copy the **DVD3**.ISO file for OVOC Version 8.0.110 that you saved to your PC in Step 1: Setup the Virtual Machine on page 122 to the OVOC server acems user home directory: /home/acems
2. Open an SSH connection or the VM console.
3. Login into the OVOC server as ‘acems’ user with password *acems* (or customer defined password).
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Mount the CDROM to make it available:

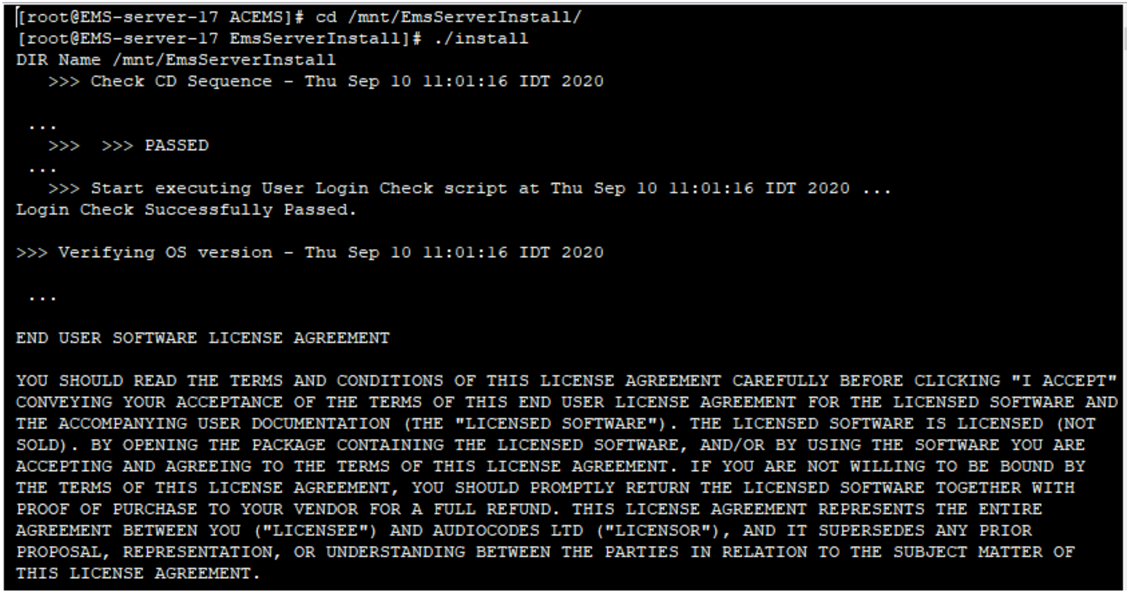
```
mount /home/acems/DVD3_OVOC_ 8.0.110.iso /mnt
```

```
cd /mnt/EmsServerInstall/
```

6. Run the installation script from its location:

```
./install
```

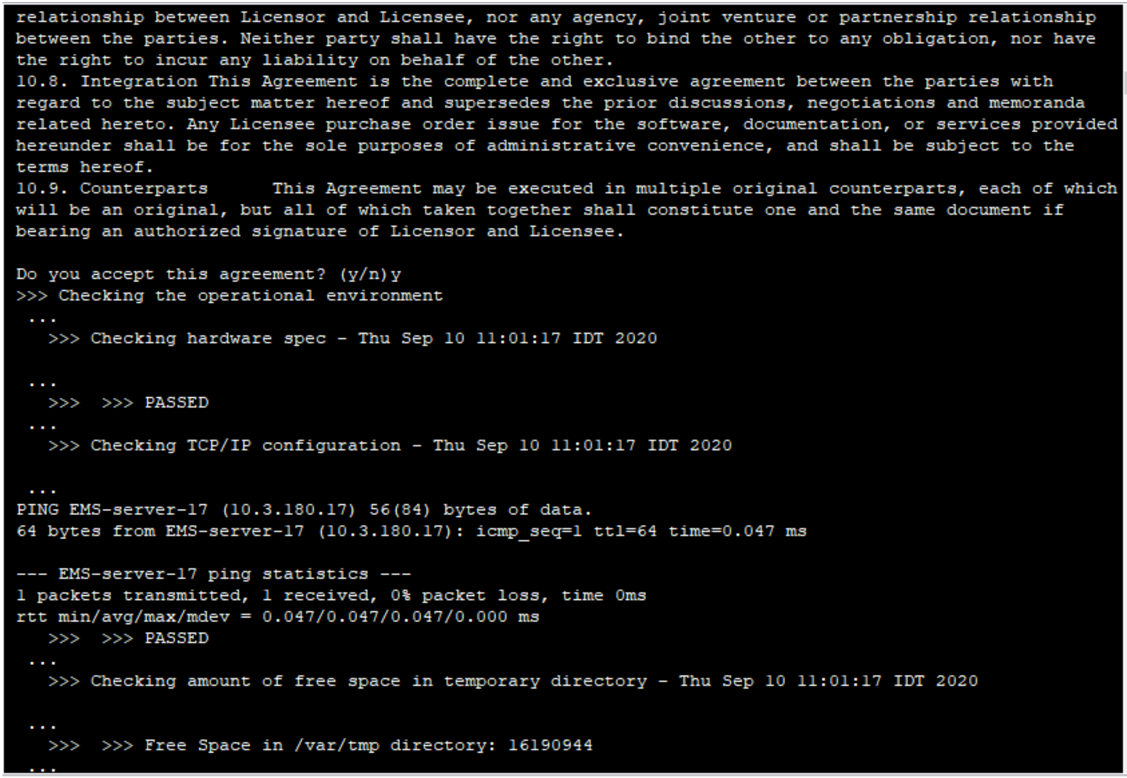
Figure 7-2: OVOC server Installation Script



```
[root@EMS-server-17 ACEMS]# cd /mnt/EmsServerInstall/
[root@EMS-server-17 EmsServerInstall]# ./install
DIR Name /mnt/EmsServerInstall
   >>> Check CD Sequence - Thu Sep 10 11:01:16 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Start executing User Login Check script at Thu Sep 10 11:01:16 IDT 2020 ...
Login Check Successfully Passed.

>>> Verifying OS version - Thu Sep 10 11:01:16 IDT 2020

 ...

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS END USER LICENSE AGREEMENT FOR THE LICENSED SOFTWARE AND
THE ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (NOT
SOLD). BY OPENING THE PACKAGE CONTAINING THE LICENSED SOFTWARE, AND/OR BY USING THE SOFTWARE YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY
THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE LICENSED SOFTWARE TOGETHER WITH
PROOF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE
AGREEMENT BETWEEN YOU ("LICENSEE") AND AUDIOCODES LTD ("LICENSOR"), AND IT SUPERSEDES ANY PRIOR
PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF
THIS LICENSE AGREEMENT.
```

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

Figure 7-3: OVOC server Upgrade – License Agreement

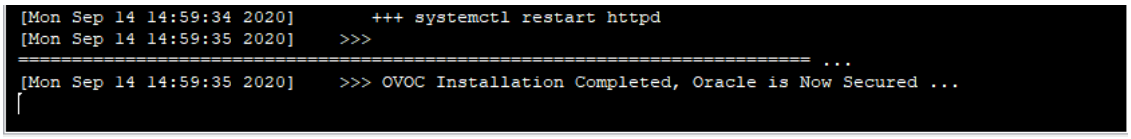


```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```

8. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

- If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).
- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 7-4: OVOC Server Installation Complete



```
[Mon Sep 14 14:59:34 2020]       +++ systemctl restart httpd
[Mon Sep 14 14:59:35 2020]    >>>
=========================================================================== ...
[Mon Sep 14 14:59:35 2020]    >>> OVOC Installation Completed, Oracle is Now Secured ...
```

9. Wait for the installation to complete and reboot the OVOC server by typing **reboot**.
10. Schedule full backup of the OVOC server to the nearest possible time (see Change Schedule Backup Time on page 157) and then verify that all necessary files have been generated (see OVOC Server Backup Processes on page 156).

Step 2 Install Service Provider Cluster on Management Server

This procedure describes how to deploy the OVOC image with VMware vSphere Hypervisor (ESXi) in a Service Provider Cluster configuration on the new virtual machine that is designated as the **Management** server. The procedure describes how to deploy the OVOC image with the VMware ESXi Web client using the OVF tool, which can be downloaded from: https://www.vmware.com/support/developer/ovf/ and installed on any Linux machine.

- The OVOC image can also be deployed using the vSphere web client GUI.
- You must install the Management server prior to installing the VQM and PM servers.
- Refer to OVOC Software Deliverables on page 15 for information on media deliverables.

➢ To install Service Provider Cluster (Management server):

1. **On the new virtual machine:** Transfer the 7z file containing the VMware Virtual Machine **Management** installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 295 for instructions on how to transfer files).
2. Run the VMware OVF tool (see Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) on page 66
3. After the VM has been created, **Inflate Thin Virtual Disk**. For Instructions: https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.storage.doc/GUID-C371B88F-C407-4A69-8F3B-FA877D6955F8.html
4. Restore the backup that you created in Step 1 Upgrade Existing Virtual Machine on page 68 (see OVOC Server Restore on page 158).
5. Configure Service Provider Cluster mode (see Service Provider Cluster on page 188).

6. Install VQM and PM servers (see Step 3 Install VQM Server below and Step 4 Install PM Server below).

Step 3 Install VQM Server

This procedure describes how to install the Service Provider Cluster mode on the new virtual machine that is designated for the **VQM** Server.

- The OVOC image can also be deployed using the vSphere web client GUI.
- Refer to OVOC Software Deliverables on page 15 for information on media deliverables.
- You must install the Management server prior to installing the VQM server (see Step 2 Install Service Provider Cluster on Management Server on the previous page).

➢ **To install VQM server:**

1. **On the new virtual machine:** Transfer the 7z file containing the VMware Virtual Machine **VQM** installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 295 for instructions on how to transfer files).
2. Run the VMware OVF tool (see Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) on page 66
3. After the VM has been created, **Inflate Thin Virtual Disk**. For Instructions: https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.storage.doc/GUID-C371B88F-C407-4A69-8F3B-FA877D6955F8.html

Step 4 Install PM Server

This procedure describes how to install the Service Provider Cluster mode on the new virtual machine that is designated for the **PM** Server.

- The OVOC image can also be deployed using the vSphere web client GUI.
- Refer to OVOC Software Deliverables on page 15 for information on media deliverables.
- You must install the Management server prior to installing the PM server (seeStep 2 Install Service Provider Cluster on Management Server on the previous page)

➢ **To install the PM server:**

1. **On the new virtual machine:** Transfer the 7z file containing the VMware Virtual Machine **PM** installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 295 for instructions on how to transfer files).
2. Run the VMware OVF tool (see Deploying OVOC Image with VMware vSphere Hypervisor (ESXi) on page 66).

3. After the VM has been created, **Inflate Thin Virtual Disk**. For Instructions: https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.storage.doc/GUID-C371B88F-C407-4A69-8F3B-FA877D6955F8.html

Configuring the Virtual Machine Hardware Settings

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

Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see Hardware and Software Specifications on page 8.

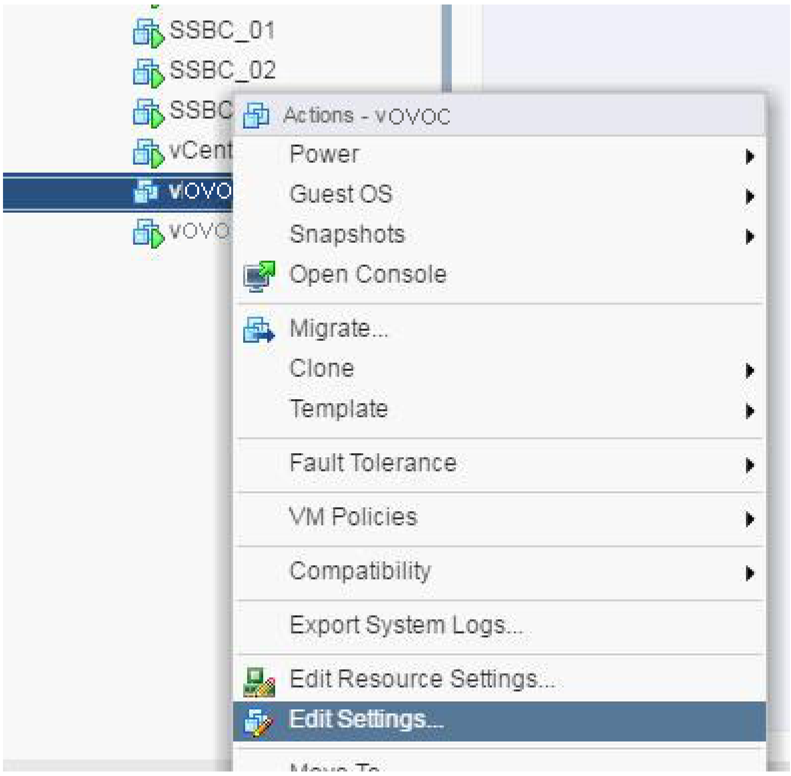
Table 7-1: Virtual Machine Configuration

Required Parameter	Value
Disk size	
Memory size	
CPU cores	

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

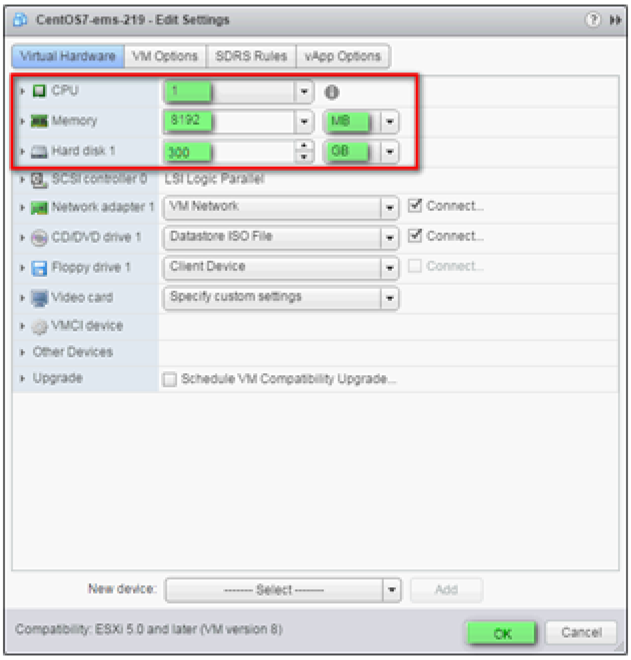
1. Before powering up the machine, go to the virtual machine **Edit Settings** option.

Figure 7-5: Edit Settings option



2. In the **CPU, Memory** and **Hardware** tabs set the required values accordingly to the desired OVOC server VMware Disk Space allocation. (Hardware and Software Specifications on page 8), and then click **OK**.

Figure 7-6: CPU, Memory and Hard Disk Settings



CentOS7-ems-219 - Edit Settings

CPU: 1

Memory: 8192 MB

Hard disk 1: 300 GB

SCSI controller 0: LSI Logic Parallel

Network adapter 1: VM Network ☑ Connect...

CD/DVD drive 1: Datastore ISO File ☑ Connect...

Floppy drive 1: Client Device □ Connect...

Video card: Specify custom settings

VMCI device

Other Devices

Upgrade: □ Schedule VM Compatibility Upgrade...

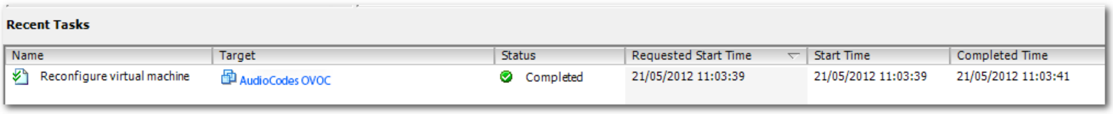
New device: ------- Select -------

Compatibility: ESXi 5.0 and later (VM version 8)

- Once the hard disk space allocation is increased, it cannot be reduced to a lower amount.
- If you wish to create OVOC VMs in a cluster environment supporting High Availability and you are using shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster (Configuring OVOC Virtual Machines (VMs) in a VMware Cluster below).

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

Figure 7-7: Recent Tasks



Recent Tasks

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

Configuring OVOC Virtual Machines (VMs) in a VMware Cluster

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

VMware Cluster Site Requirements

Ensure that your VMware cluster site meets the following requirements:

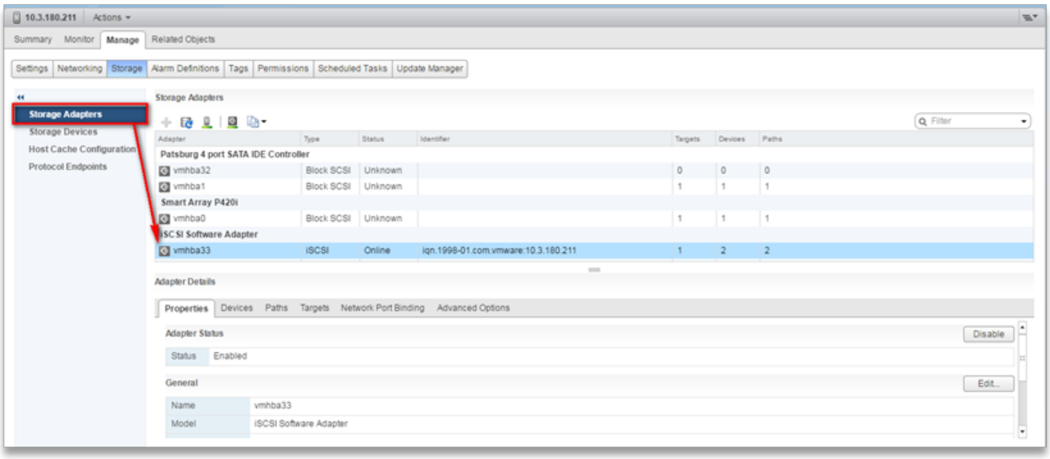
- The configuration process assumes that you have a VMware cluster that contains at least two ESXi servers controlled by vCenter server.

- The clustered VM servers should be connected to a shared network storage of type iSCSI or any other types supported by VMware ESXi.

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

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

Figure 7-8: Storage Adapters



Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Patsburg 4 port SATA IDE Controller						
vmhba32	Block SCSI	Unknown		0	0	0
vmhba1	Block SCSI	Unknown		1	1	1
Smart Array P420i						
vmhba0	Block SCSI	Unknown		1	1	1
iSCSI Software Adapter						
vmhba33	iSCSI	Online	iqn.1998-01.com.vmware:10.3.180.211	1	2	2

Adapter Details

Adapter Status

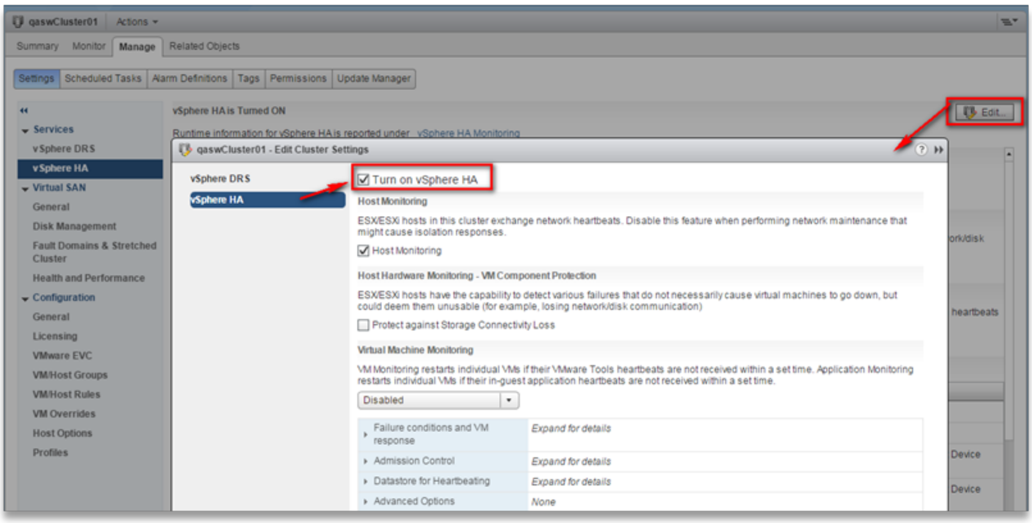
Status	Enabled

General

Name	vmhba33
Model	iSCSI Software Adapter

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

Figure 7-9: Turn On vSphere HA



vSphere HA is Turned ON

Runtime information for vSphere HA is reported under vSphere HA Monitoring

qaswCluster01 - Edit Cluster Settings

vSphere DRS

vSphere HA

☑ Turn on vSphere HA

Host Monitoring

ESX/ESXi hosts in this cluster exchange network heartbeats. Disable this feature when performing network maintenance that might cause isolation responses.

☑ Host Monitoring

Host Hardware Monitoring - VM Component Protection

ESX/ESXi hosts have the capability to detect various failures that do not necessarily cause virtual machines to go down, but could deem them unusable (for example, losing network/disk communication)

□ Protect against Storage Connectivity Loss

Virtual Machine Monitoring

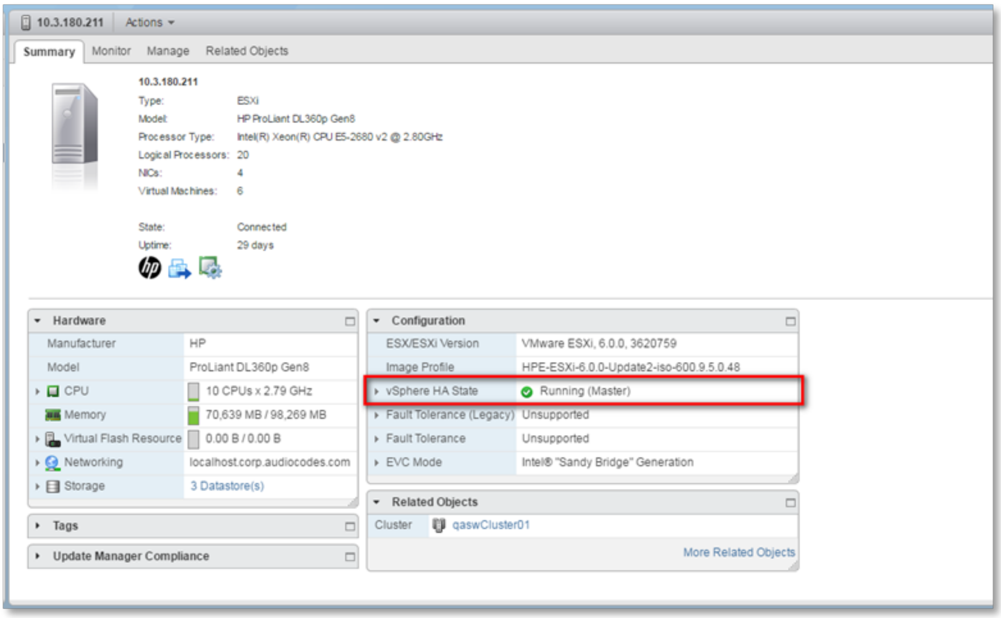
VM Monitoring restarts individual VMs if their VMware Tools heartbeats are not received within a set time. Application Monitoring restarts individual VMs if their in-guest application heartbeats are not received within a set time.

Disabled

Failure conditions and VM response	*Expand for details*
Admission Control	*Expand for details*
Datastore for Heartbeating	*Expand for details*
Advanced Options	*None*

- Ensure that HA is activated on each cluster node:

Figure 7-10: Activate HA on each Cluster Node



10.3.180.211
Type: ESXi
Model: HP ProLiant DL360p Gen8
Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors: 20
NICs: 4
Virtual Machines: 6

State: Connected
Uptime: 29 days

Hardware

Manufacturer	HP
Model	ProLiant DL360p Gen8
CPU	10 CPUs x 2.79 GHz
Memory	70,639 MB / 98,269 MB
Virtual Flash Resource	0.00 B / 0.00 B
Networking	localhost.corp.audiocodes.com
Storage	3 Datastore(s)

Tags

Update Manager Compliance

Configuration

ESX/ESXi Version	VMware ESXi, 6.0.0, 3620759
Image Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5.0.48
vSphere HA State	Running (Master)
Fault Tolerance (Legacy)	Unsupported
Fault Tolerance	Unsupported
EVC Mode	Intel® "Sandy Bridge" Generation

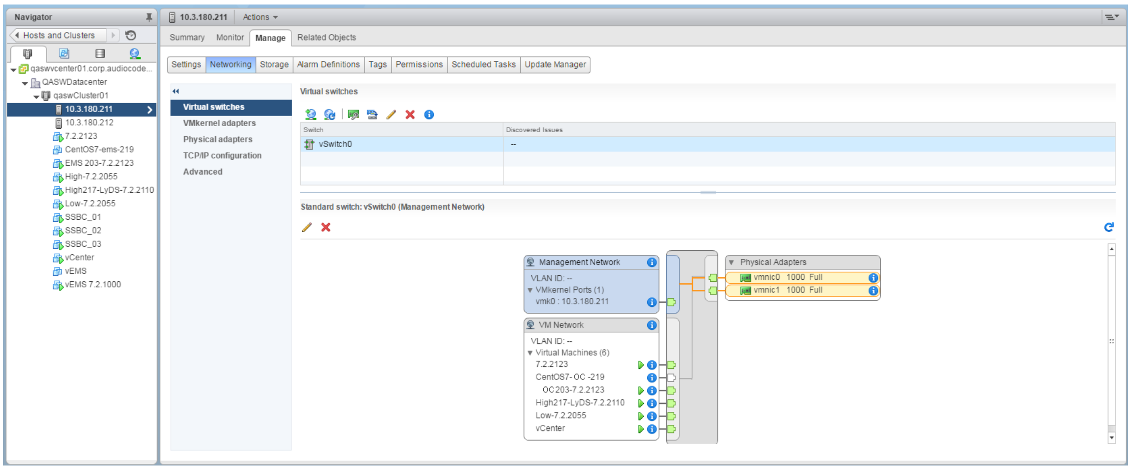
Related Objects

Cluster	qaswCluster01

More Related Objects

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

Figure 7-11: Networking



Virtual switches

Switch	Discovered Issues
vSwitch0	--

Standard switch: vSwitch0 (Management Network)

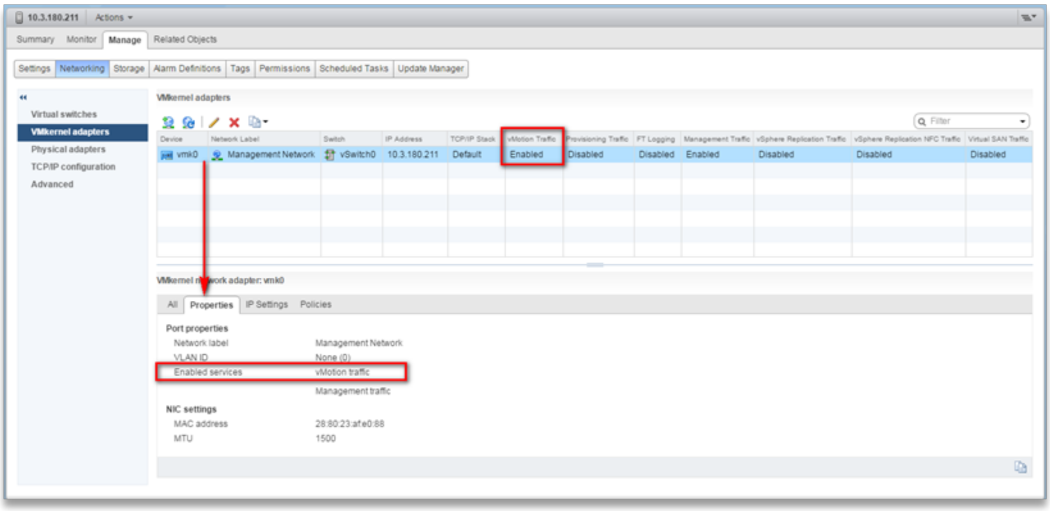
Management Network
VLAN ID: --
VMkernel Ports (1)
vmk0 : 10.3.180.211

VM Network
VLAN ID: --
Virtual Machines (6)
7.2.2123
CentOS7-OC -219
OC203-7.2.2123
High217-LyDS-7.2.2110
Low-7.2.2055
vCenter

Physical Adapters
vmnic0 1000 Full
vmnic1 1000 Full

- 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 7-12: Switch Properties



VMkernel adapters

Device	Network Label	Switch	IP Address	TCP/IP Stack	vMotion Traffic	Provisioning Traffic	FT Logging	Management Traffic	vSphere Replication Traffic	vSphere Replication NFC Traffic	Virtual SAN Traffic
vmk0	Management Network	vSwitch0	10.3.180.211	Default	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

VMkernel network adapter: vmk0

All | Properties | IP Settings | Policies

Port properties

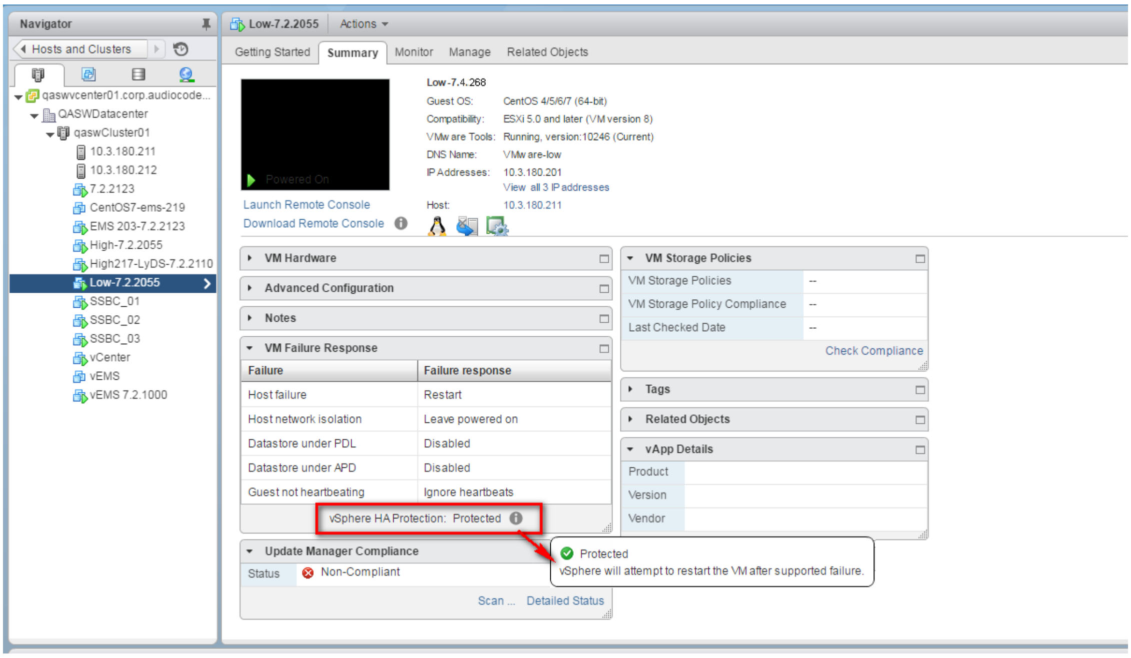
Network label	Management Network
VLAN ID	None (0)
Enabled services	vMotion traffic
	Management traffic

NIC settings

MAC address	28:80:23:af:e0:88
MTU	1500

- 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 7-13: Protected VM



Low-7.4.268

Guest OS:	CentOS 4/5/6/7 (64-bit)
Compatibility:	ESXi 5.0 and later (VM version 8)
VMware Tools:	Running, version:10246 (Current)
DNS Name:	VMware-low
IP Addresses:	10.3.180.201 View all 3 IP addresses
Host:	10.3.180.211

VM Failure Response

Failure	Failure response
Host failure	Restart
Host network isolation	Leave powered on
Datastore under PDL	Disabled
Datastore under APD	Disabled
Guest not heartbeating	Ignore heartbeats

vSphere HA Protection: Protected

Protected
vSphere will attempt to restart the VM after supported failure.

Update Manager Compliance

Status	Non-Compliant

VM Storage Policies

VM Storage Policies	--
VM Storage Policy Compliance	--
Last Checked Date	--

vApp Details

Product	
Version	
Vendor	

If you wish to manually migrate the OVOC VMs to another cluster node, see Managing Clusters on page 278.

Cluster Host Node Failure on VMware

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

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

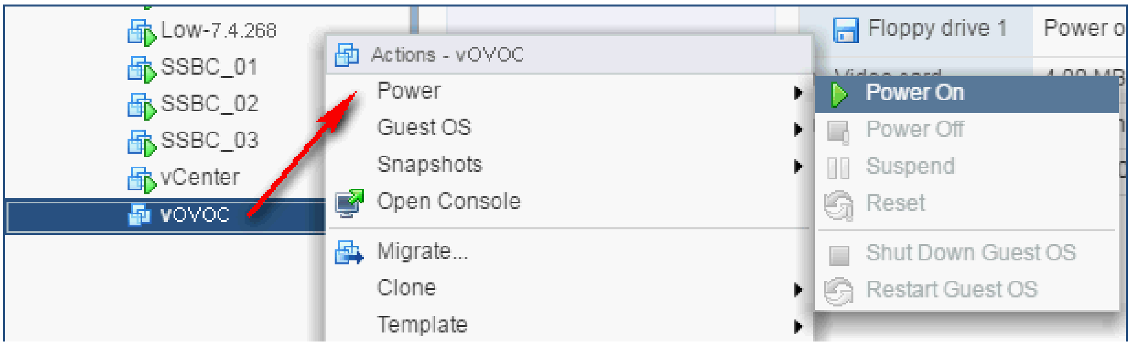
Connecting OVOC Server to Network on VMware

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

➢ To connect to the OVOC server:

1. Power on the machine; in the vCenter tree, right-click the AudioCodes One Voice Operations Center node (vOC) and in the drop-down menu, choose **Power** > **Power On**. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications (Hardware and Software Specifications on page 8).

Figure 7-14: Power On



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

```
su - root
```

5. Proceed to the network configuration using the OVOC Server Manager.
6. Type the following command and press Enter.

```
# EmsServerManager
```

7. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify login to OVOC Web client is successful.

8. Set the OVOC server network IP address to suit your IP addressing scheme (Server IP Address on page 195).

9. If you are installing the Service Provider Cluster mode, see Service Provider Cluster on page 188

10. Perform other configuration actions as required using the OVOC Server Manager (Getting Started on page 163).

This page is intentionally left blank.

8 Installing OVOC Server on Microsoft Hyper-V Virtual Machine

This section describes how to install the OVOC server on a Microsoft Hyper-V virtual machine.

- Before proceeding, ensure that the minimum platform requirements are met (see .Hardware and Software Specifications on page 8). Failure to meet these requirements will lead to the aborting of the installation.
- For obtaining the installation files, see OVOC Software Deliverables on page 15

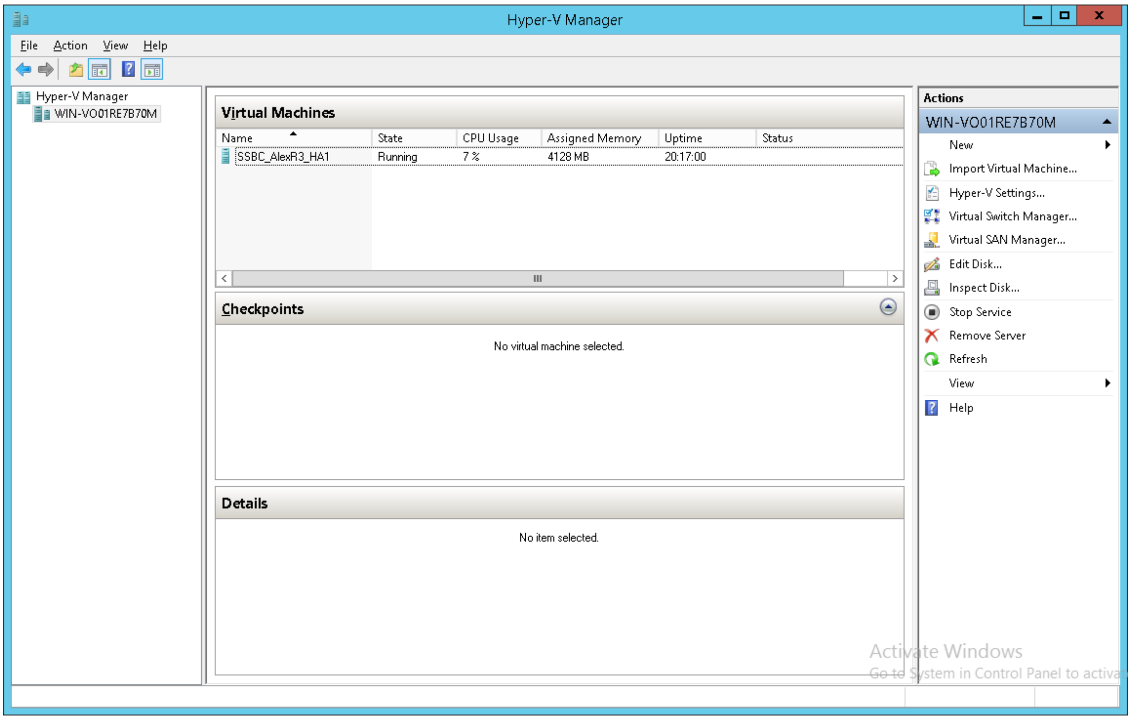
✔ Note that you must also verify the ISO file, see Files Verification on page 18

➢ To install the OVOC server on Microsoft Hyper-V:

1. Transfer the ISO file containing the Microsoft Hyper-V Virtual Machine installation package that you received from AudioCodes to your PC (see Appendix Transferring Files on page 295 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 8-1: Installing the OVOC server on Hyper-V – Hyper-V Manager



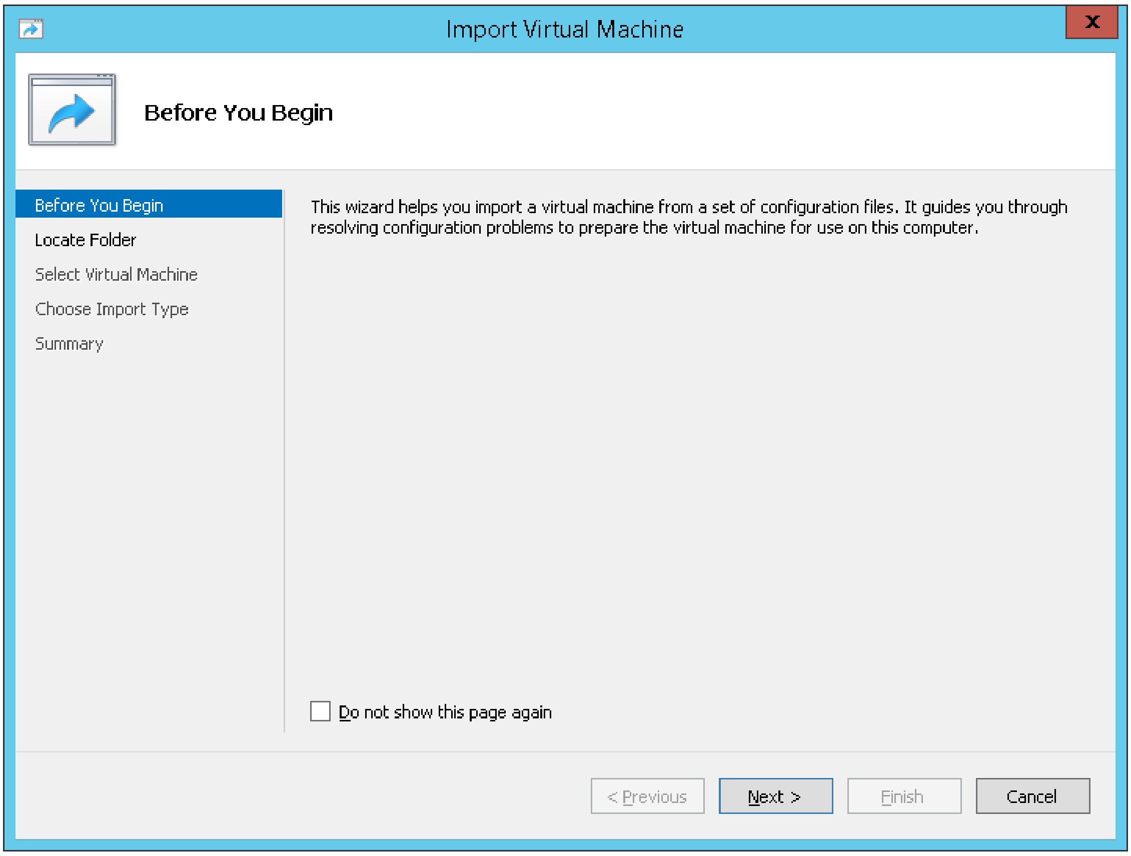
Name	State	CPU Usage	Assigned Memory	Uptime	Status
SSBC_AlexR3_HA1	Running	7 %	4128 MB	20:17:00	

No virtual machine selected.

No item selected.

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 8-2: Installing OVOC server on Hyper-V – Import Virtual Machine Wizard

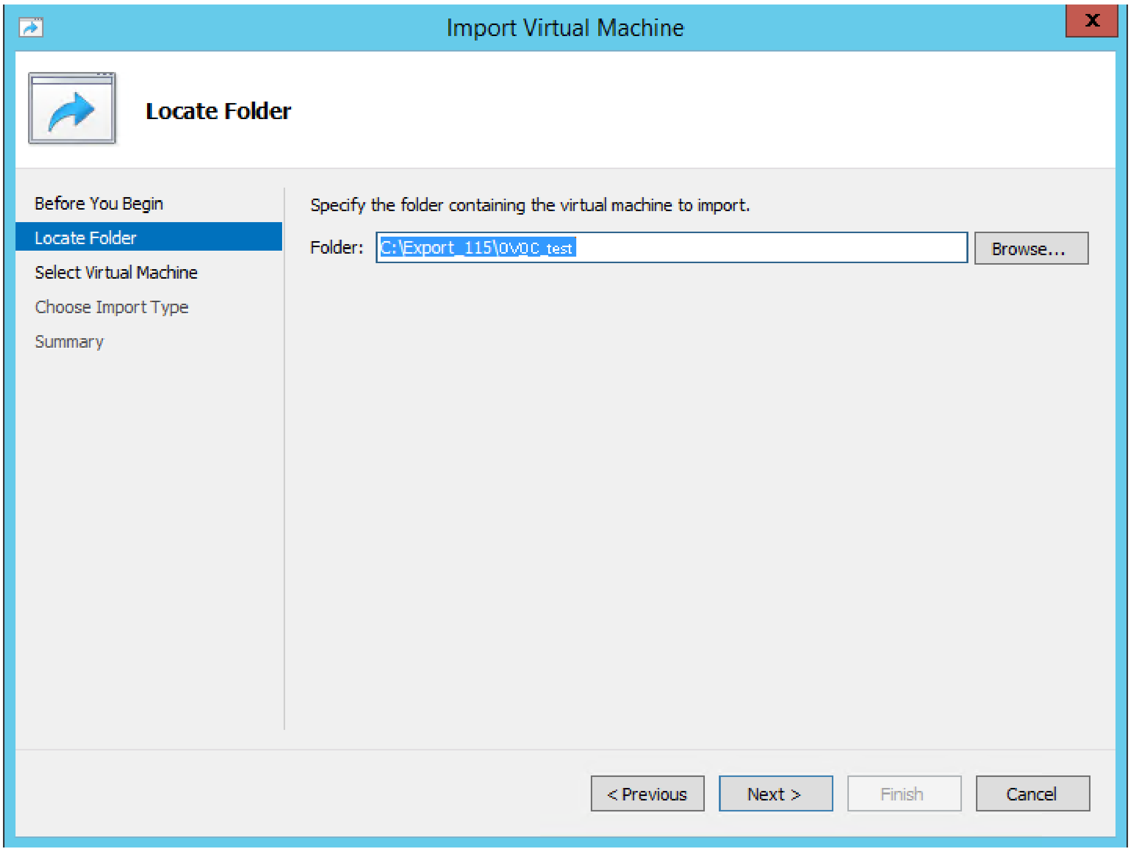


This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

□ Do not show this page again

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

Figure 8-3: Installing OVOC server on Hyper-V – Locate Folder



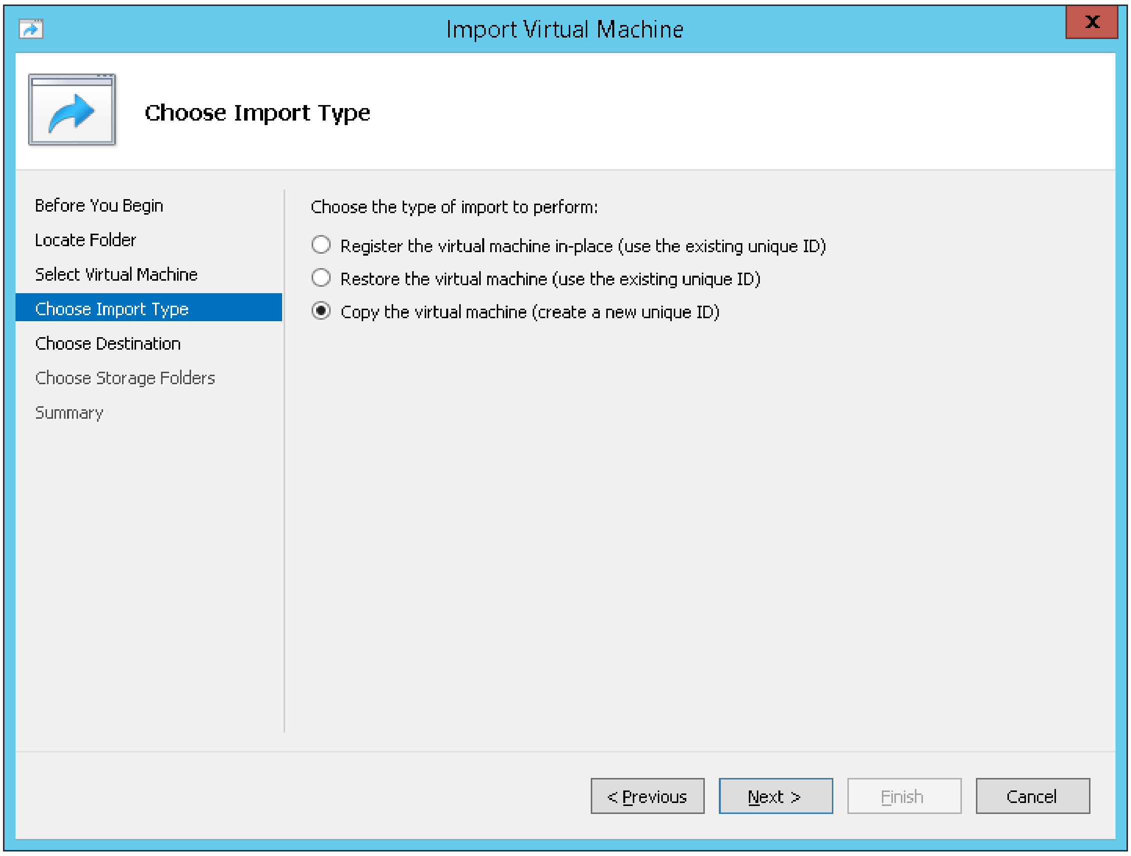
Specify the folder containing the virtual machine to import.

Folder: C:\Export_115\OVOC_test

5. Enter the location of the VM installation folder (extracted from the ISO 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 8-4: Installing OVOC server on Hyper-V – Choose Import Type



Import Virtual Machine

Choose Import Type

Choose the type of import to perform:

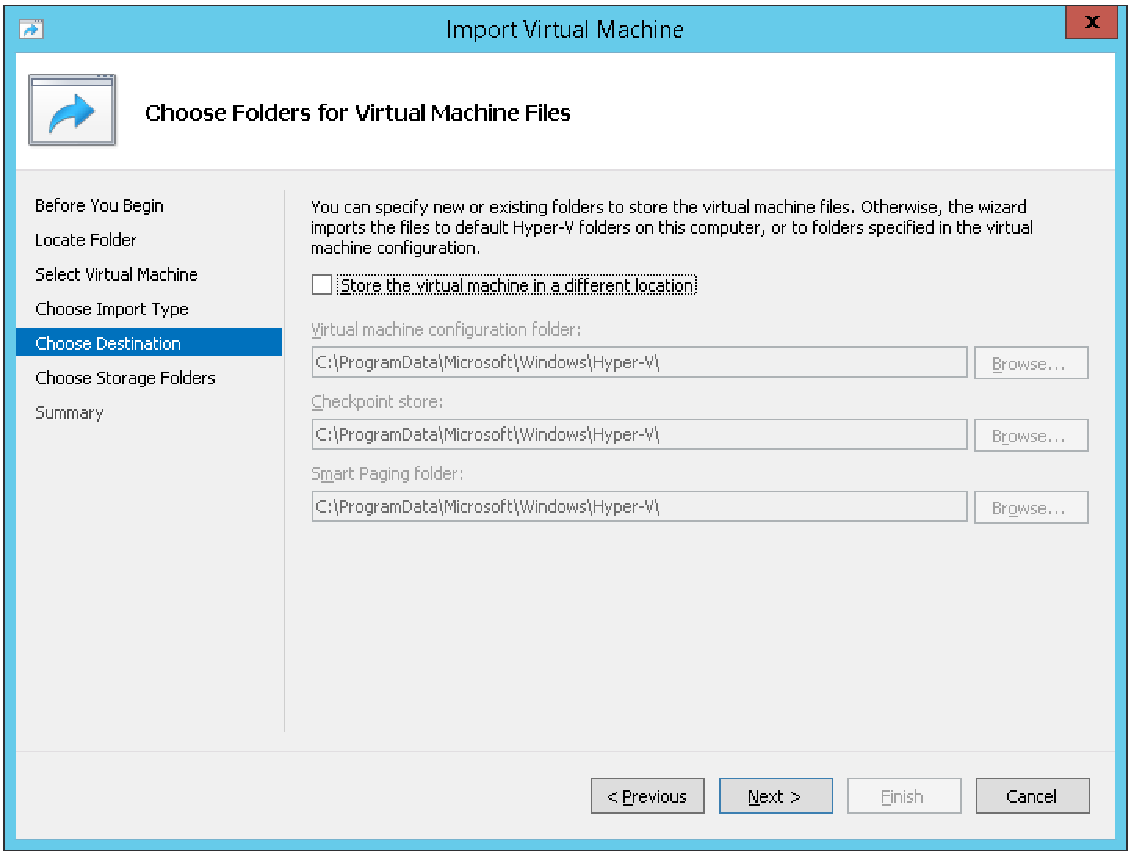
○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

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 8-5: Installing OVOC server on Hyper-V – Choose Destination



Import Virtual Machine

Choose Folders for Virtual Machine Files

- Before You Begin
- Locate Folder
- Select Virtual Machine
- Choose Import Type
- Choose Destination
- Choose Storage Folders
- Summary

You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

□ Store the virtual machine in a different location

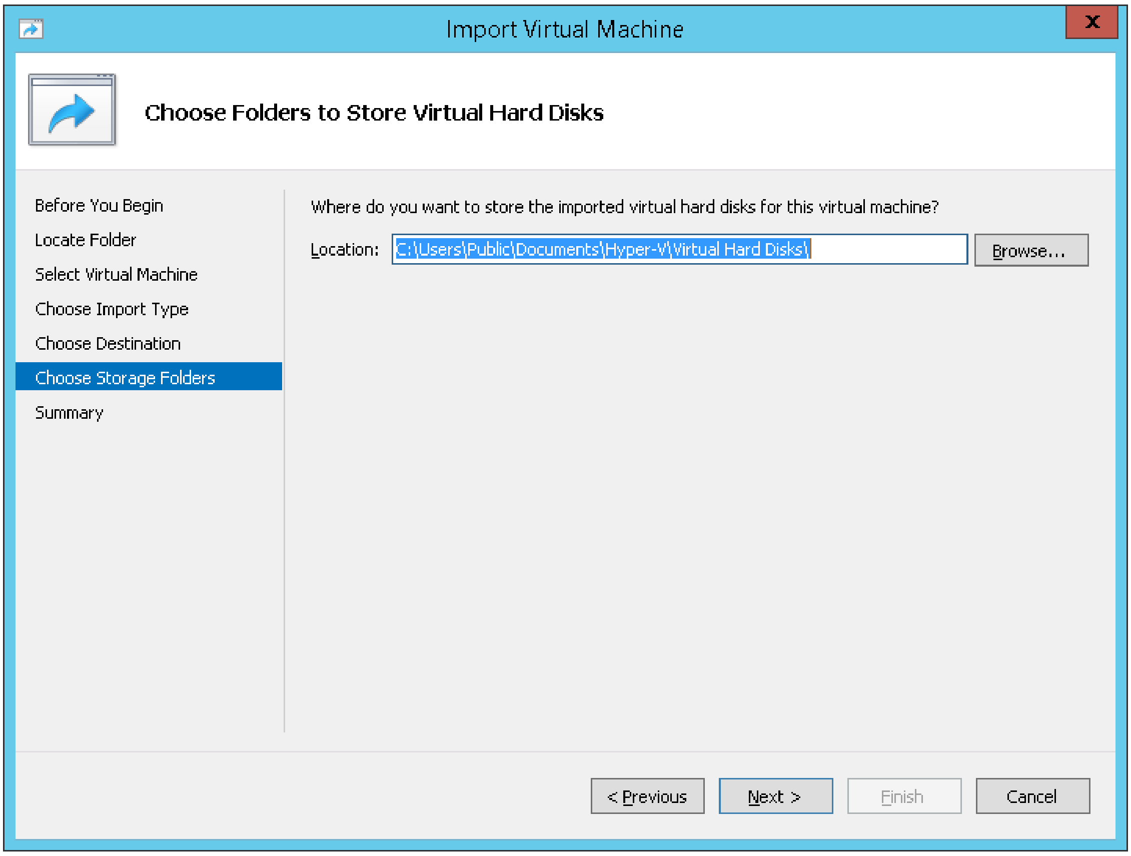
Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Checkpoint store: C:\ProgramData\Microsoft\Windows\Hyper-V\

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

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

Figure 8-6: Installing OVOC server on Hyper-V – Choose Storage Folders



Where do you want to store the imported virtual hard disks for this virtual machine?

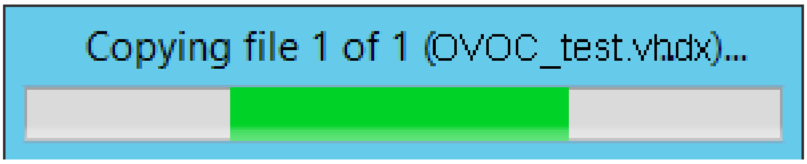
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

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 8-7: File Copy Progress Bar

This process may take approximately 30 minutes to complete.



Copying file 1 of 1 (OVOC_test.vhdx)...

11. Proceed to Configuring the Virtual Machine Hardware Settings below.

Configuring the Virtual Machine Hardware Settings

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

Before starting this procedure, select the required values for your type of installation (high or low profile) and note them in the following table for reference. For the required VMware Disk Space allocation, CPU, and memory, see Hardware and Software Specifications on page 8.

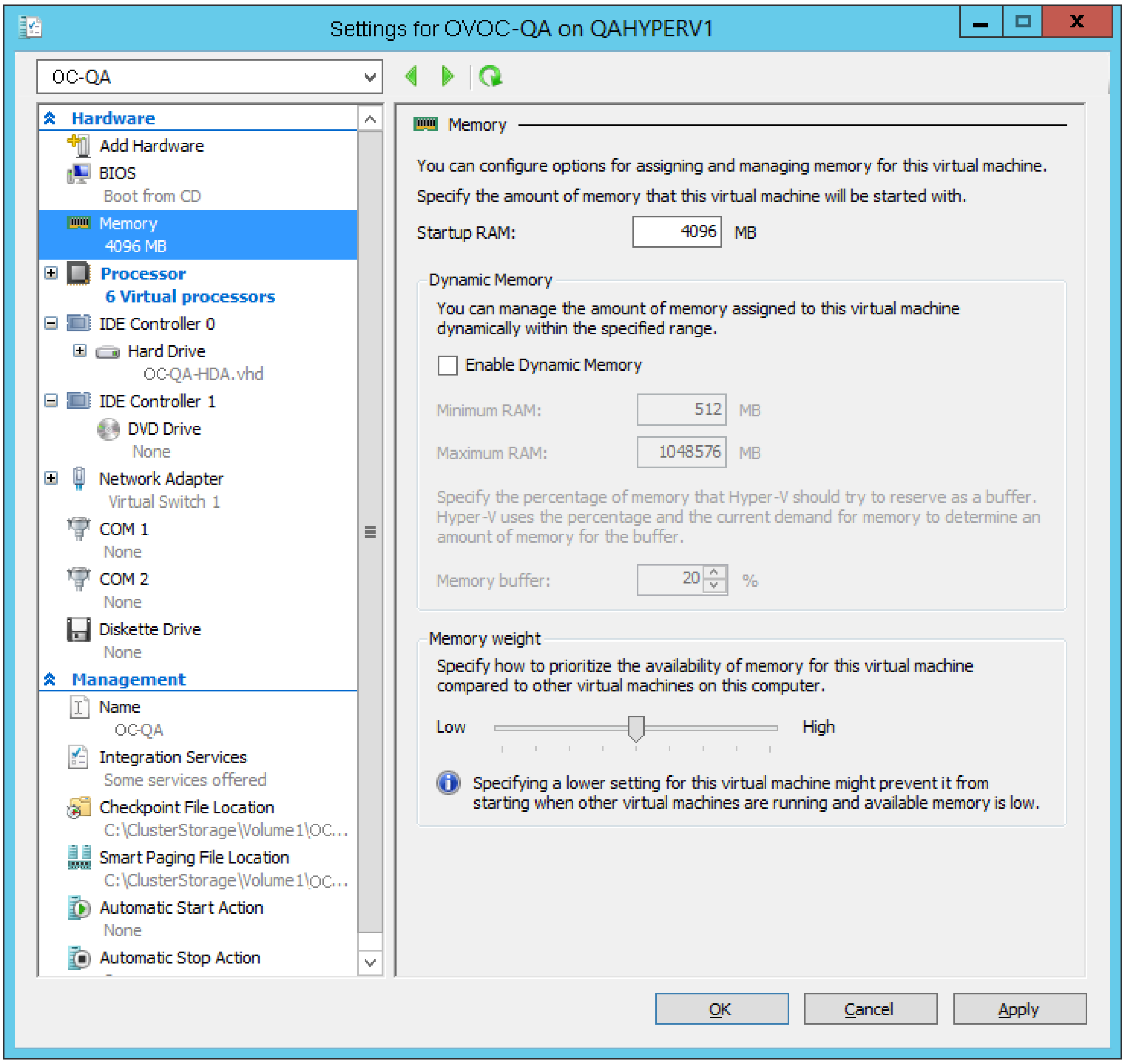
Table 8-1: Virtual Machine Configuration

Required Parameter	Value
Disk size	
Memory size	
CPU cores	

➢ To configure the VM for OVOC server:

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

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



Settings for OVOC-QA on QAHYPERV1

OC-QA

Hardware
- Add Hardware
- BIOS
Boot from CD
- Memory
4096 MB
- Processor
6 Virtual processors
- IDE Controller 0
  - Hard Drive
OC-QA-HDA.vhd
- IDE Controller 1
  - DVD Drive
None
- Network Adapter
Virtual Switch 1
- COM 1
None
- COM 2
None
- Diskette Drive
None

Management
- Name
OC-QA
- Integration Services
Some services offered
- Checkpoint File Location
C:\ClusterStorage\Volume1\OC...
- Smart Paging File Location
C:\ClusterStorage\Volume1\OC...
- Automatic Start Action
None
- Automatic Stop Action

Memory

You can configure options for assigning and managing memory for this virtual machine.

Specify the amount of memory that this virtual machine will be started with.

Startup RAM: 4096 MB

Dynamic Memory

You can manage the amount of memory assigned to this virtual machine dynamically within the specified range.

□ Enable Dynamic Memory

Minimum RAM: 512 MB

Maximum RAM: 1048576 MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

Memory weight

Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

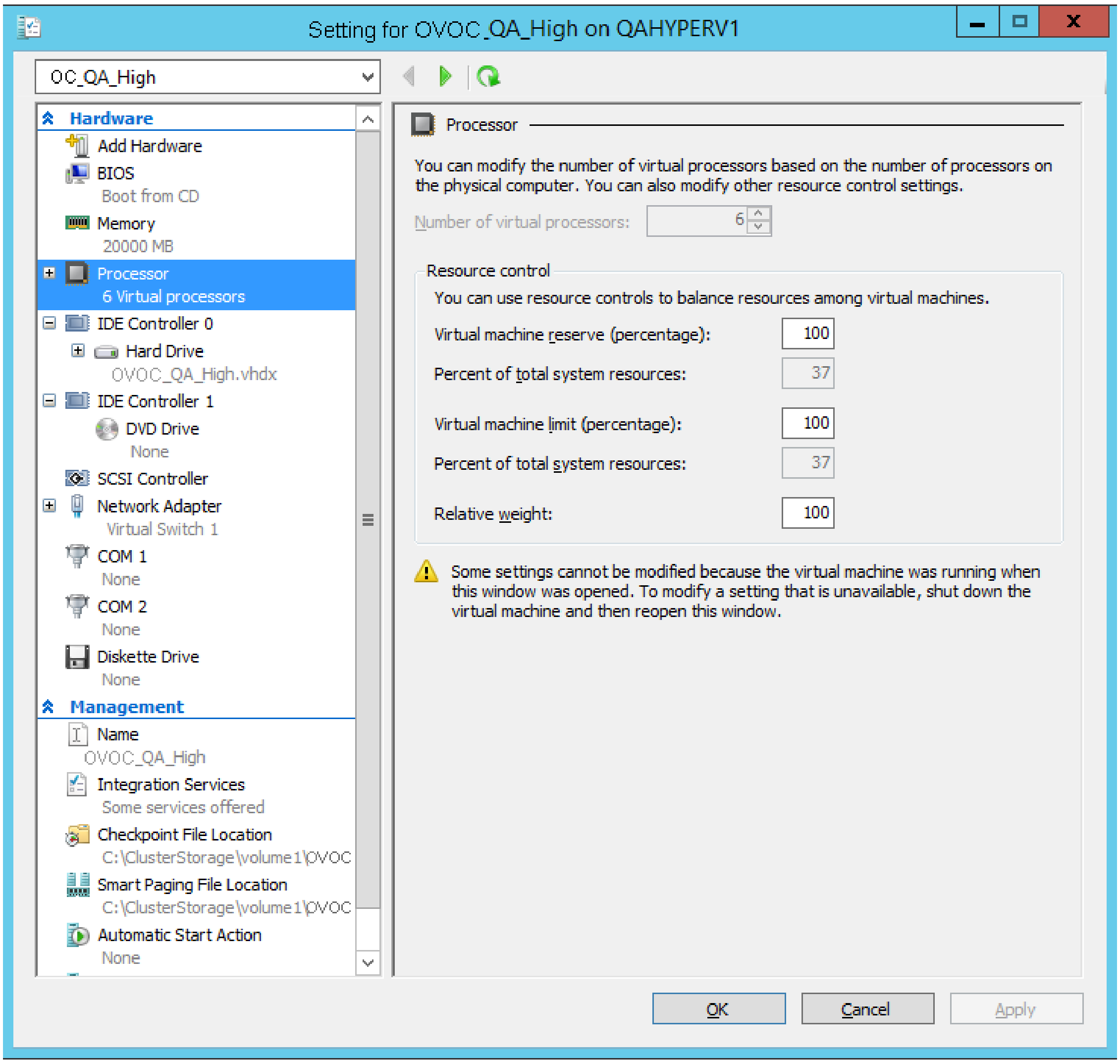
Low — High

Specifying a lower setting for this virtual machine might prevent it from starting when other virtual machines are running and available memory is low.

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 8-9: Adjusting VM for OVOC server - Settings - Processor



Setting for OVOC_QA_High on QAHYPERV1

OC_QA_High

Hardware
Add Hardware
BIOS
Boot from CD
Memory
20000 MB
Processor
6 Virtual processors
IDE Controller 0
Hard Drive
OVOC_QA_High.vhdx
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
Virtual Switch 1
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
OVOC_QA_High
Integration Services
Some services offered
Checkpoint File Location
C:\ClusterStorage\volume1\OVOC
Smart Paging File Location
C:\ClusterStorage\volume1\OVOC
Automatic Start Action
None

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 6

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 100

Percent of total system resources: 37

Virtual machine limit (percentage): 100

Percent of total system resources: 37

Relative weight: 100

⚠ Some settings cannot be modified because the virtual machine was running when this window was opened. To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

4. Set the 'Number of virtual processors' parameters as required.

5. Set the 'Virtual machine reserve (percentage)' parameter to **100%,** and then click **Apply**.

- Once the hard disk space allocation is increased, it cannot be reduced.
- If you wish to create OVOC VMs in a Cluster environment that supports High Availability and you are using shared network storage, then ensure you provision a VM hard drive on the shared network storage on the cluster (Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster on page 93).

Expanding Disk Capacity

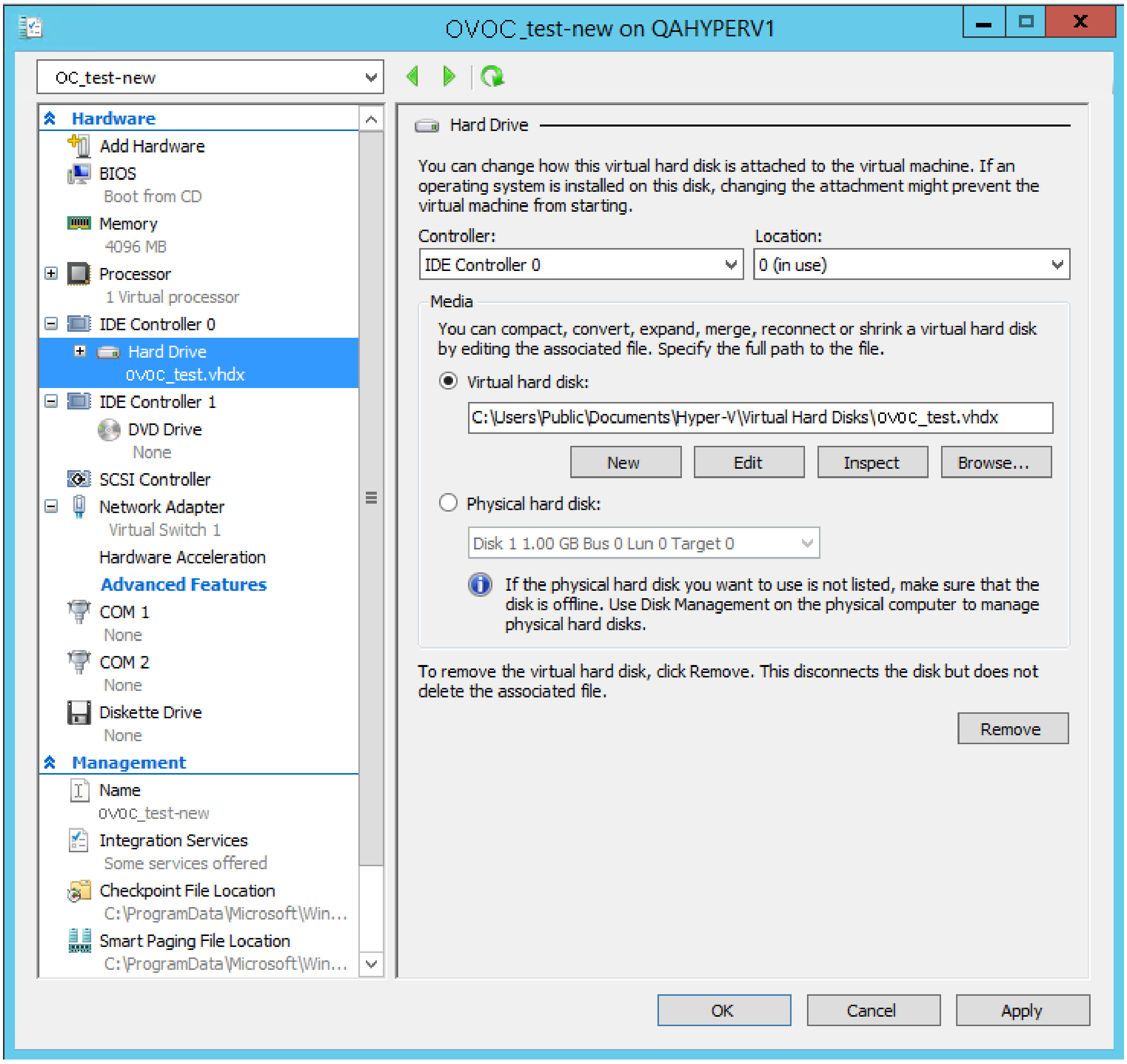
The OVOC server virtual disk is provisioned by default with a minimum volume. In case a higher capacity is required for the target OVOC server then the disk can be expanded.

➢ 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 8-10: Expanding Disk Capacity



OVOC_test-new on QAHYPERV1

OC_test-new

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ovoc_test.vhdx

○ Physical hard disk:

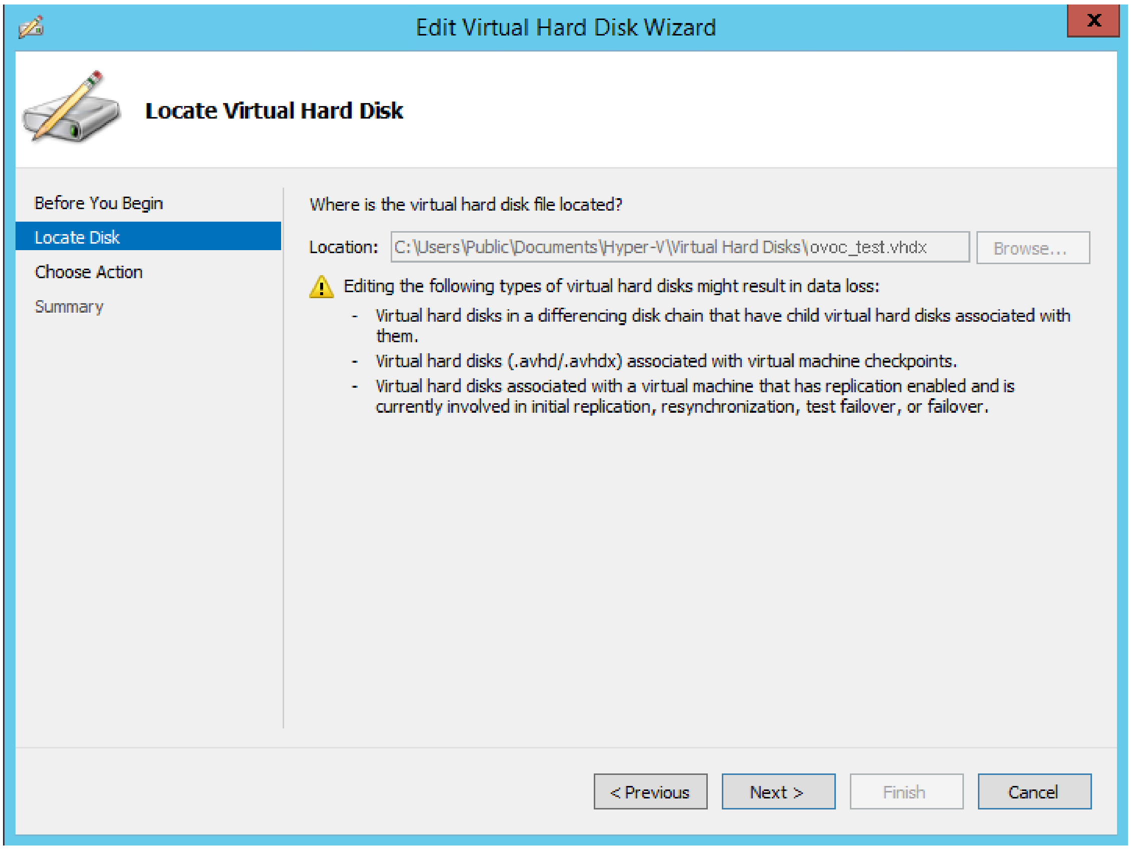
Disk 1 1.00 GB Bus 0 Lun 0 Target 0

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

The Edit Virtual Disk Wizard is displayed as shown below.

Figure 8-11: Edit Virtual Hard Disk Wizard



Where is the virtual hard disk file located?

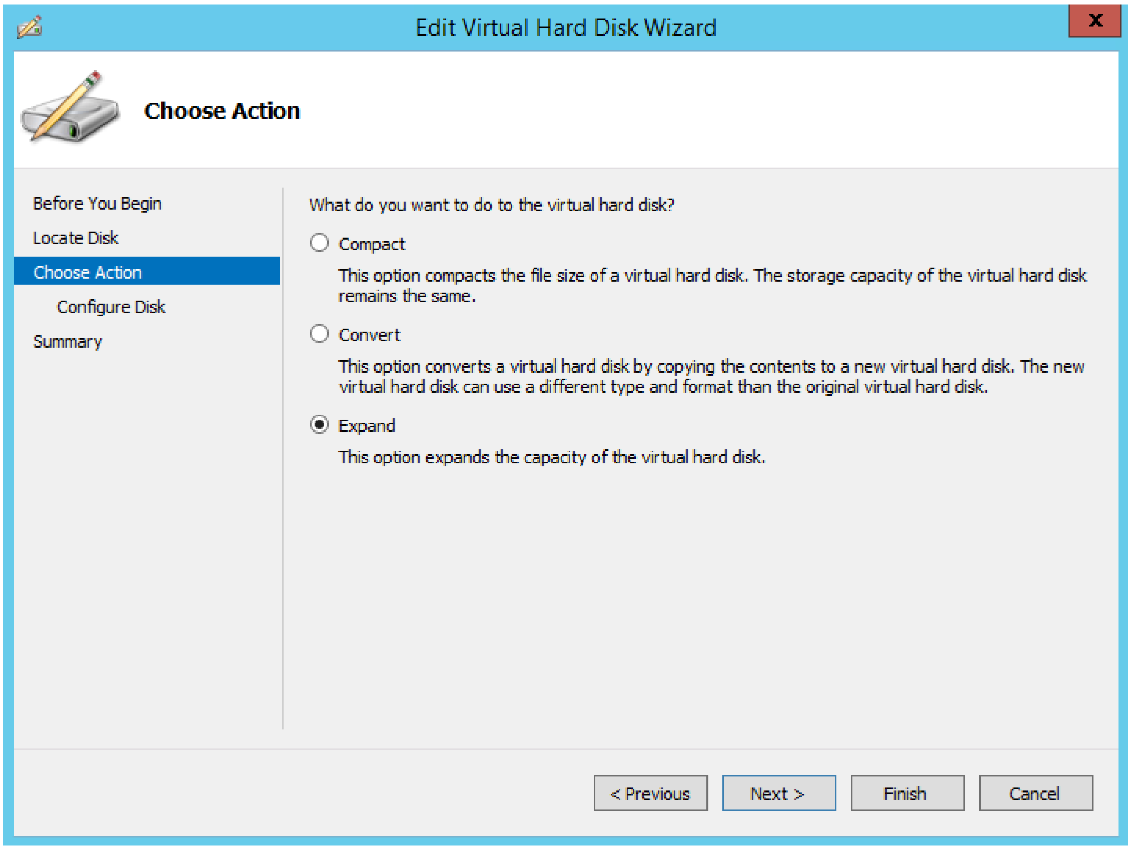
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ovoc_test.vhdx

⚠ Editing the following types of virtual hard disks might result in data loss:

- Virtual hard disks in a differencing disk chain that have child virtual hard disks associated with them.
- Virtual hard disks (.avhd/.avhdx) associated with virtual machine checkpoints.
- Virtual hard disks associated with a virtual machine that has replication enabled and is currently involved in initial replication, resynchronization, test failover, or failover.

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

Figure 8-12: Edit Virtual Hard Disk Wizard-Choose Action



What do you want to do to the virtual hard disk?

○ Compact

This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard disk remains the same.

○ Convert

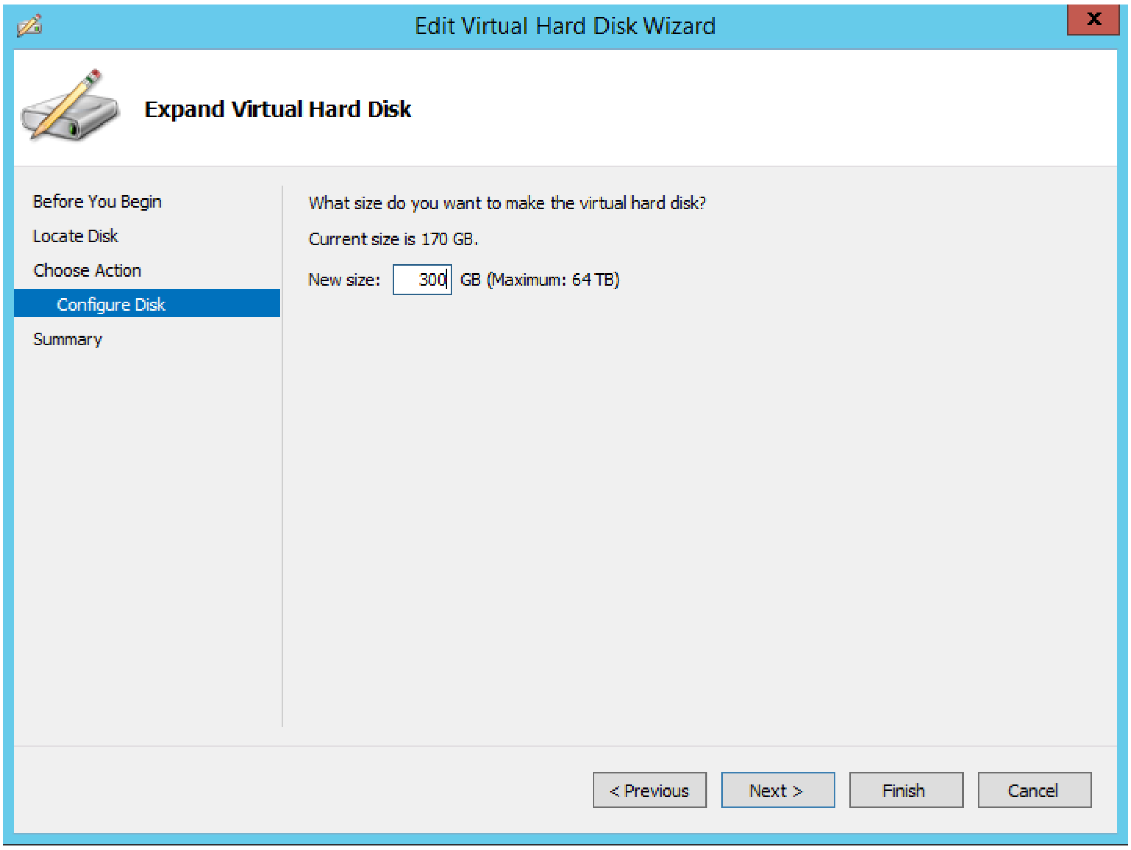
This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk.

● Expand

This option expands the capacity of the virtual hard disk.

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

Figure 8-13: Edit Virtual Hard Disk Wizard-Expand Virtual Hard Disk



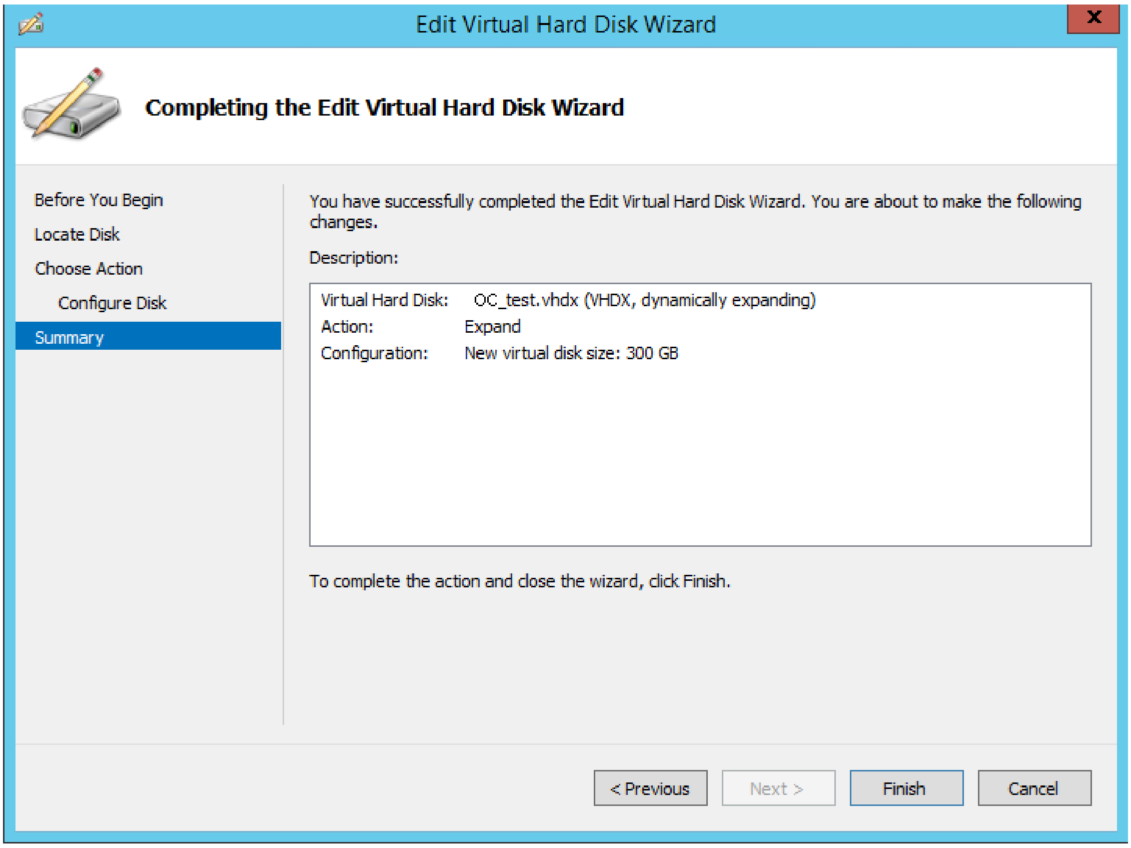
What size do you want to make the virtual hard disk?

Current size is 170 GB.

New size: 300 GB (Maximum: 64 TB)

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

Figure 8-14: Edit Virtual Hard Disk Wizard-Completion



You have successfully completed the Edit Virtual Hard Disk Wizard. You are about to make the following changes.

Description:

Virtual Hard Disk: OC_test.vhdx (VHDX, dynamically expanding)
Action: Expand
Configuration: New virtual disk size: 300 GB

To complete the action and close the wizard, click Finish.

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

7. Click **OK** to close.

Changing MAC Addresses from 'Dynamic' to 'Static'

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

To prevent this from occurring, MAC Addresses should be changed from 'Dynamic' to 'Static'.

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

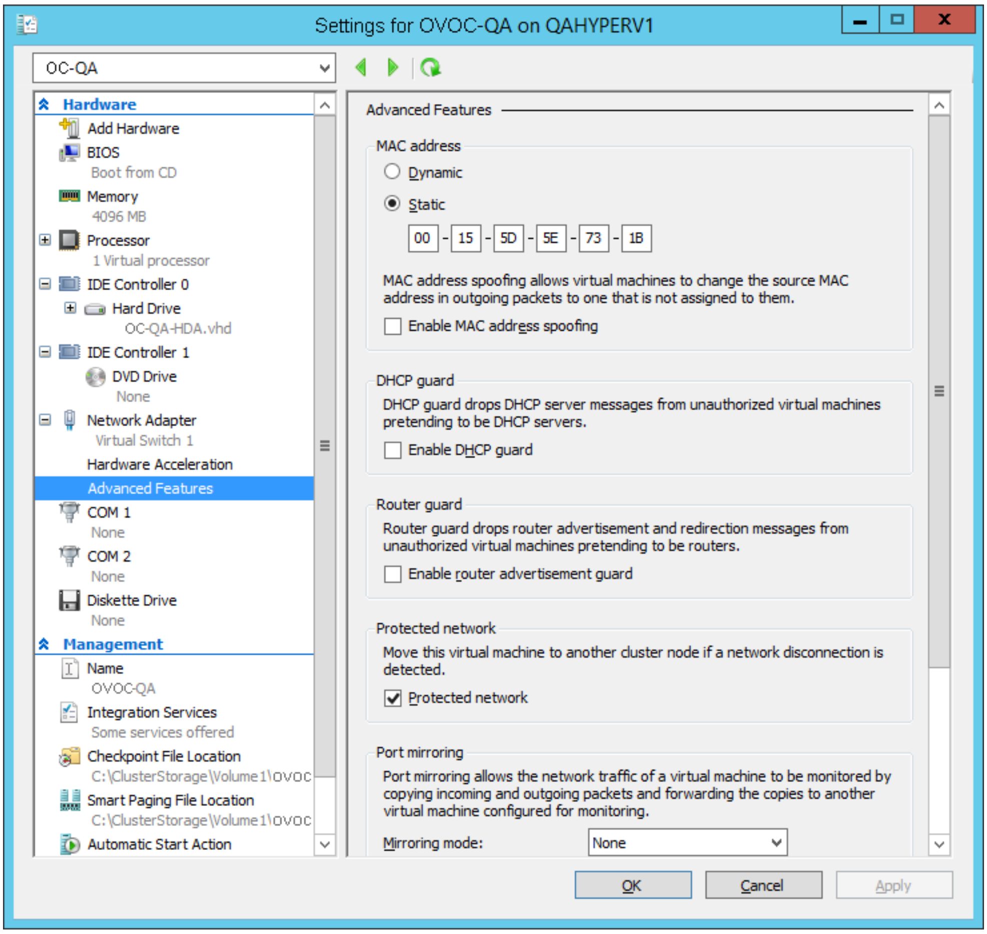
1. Shutdown the OVOC server (Shutdown the OVOC Server Machine on page 193).

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 8-15: Advanced Features - Network Adapter – Static MAC Address



Settings for OVOC-QA on QAHYPERV1

OC-QA

- Hardware
  - Add Hardware
  - BIOS
    Boot from CD
  - Memory
    4096 MB
  - Processor
    1 Virtual processor
  - IDE Controller 0
    - Hard Drive
      OC-QA-HDA.vhd
  - IDE Controller 1
    - DVD Drive
      None
  - Network Adapter
    Virtual Switch 1
    - Hardware Acceleration
    - Advanced Features
  - COM 1
    None
  - COM 2
    None
  - Diskette Drive
    None
- Management
  - Name
    OVOC-QA
  - Integration Services
    Some services offered
  - Checkpoint File Location
    C:\ClusterStorage\Volume1\ovoc
  - Smart Paging File Location
    C:\ClusterStorage\Volume1\ovoc
  - Automatic Start Action

Advanced Features

MAC address

○ Dynamic

● Static

00 - 15 - 5D - 5E - 73 - 1B

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

□ Enable MAC address spoofing

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

□ Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

□ Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

☑ Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: None

Configuring OVOC Virtual Machines in a Microsoft Hyper-V Cluster

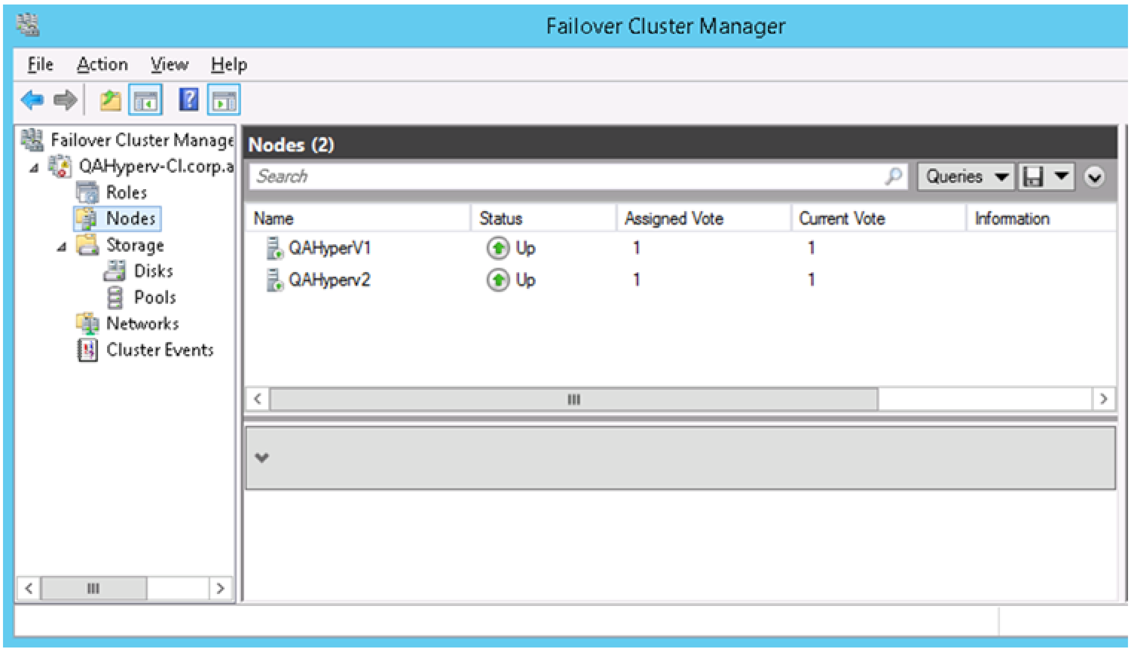
This section describes how to configure OVOC VMs in a Microsoft Hyper-V cluster for HA.

Hyper-V Cluster Site Requirements

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

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

Figure 8-16: Hyper-V-Failover Cluster Manager Nodes



Name	Status	Assigned Vote	Current Vote	Information
QAHyperV1	Up	1	1	
QAHyperv2	Up	1	1	

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

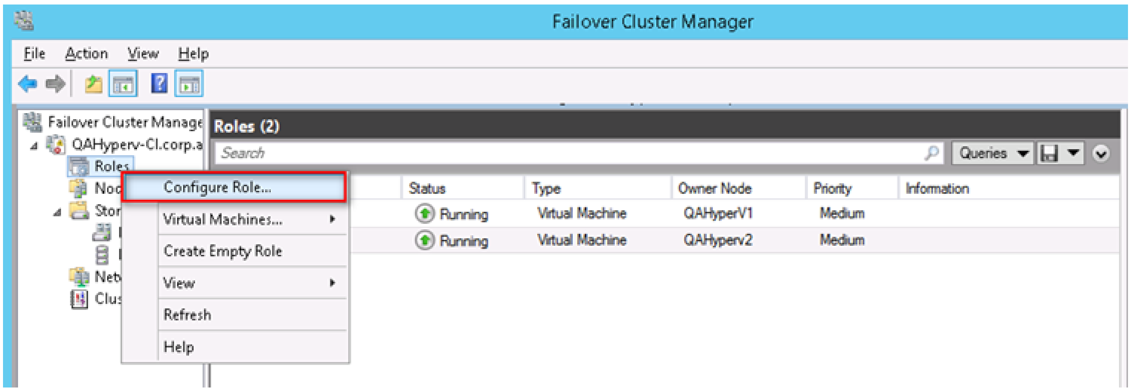
Add the OVOC VM in Failover Cluster Manager

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

➢ To add the OVOC VM in Failover Cluster Manager:

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

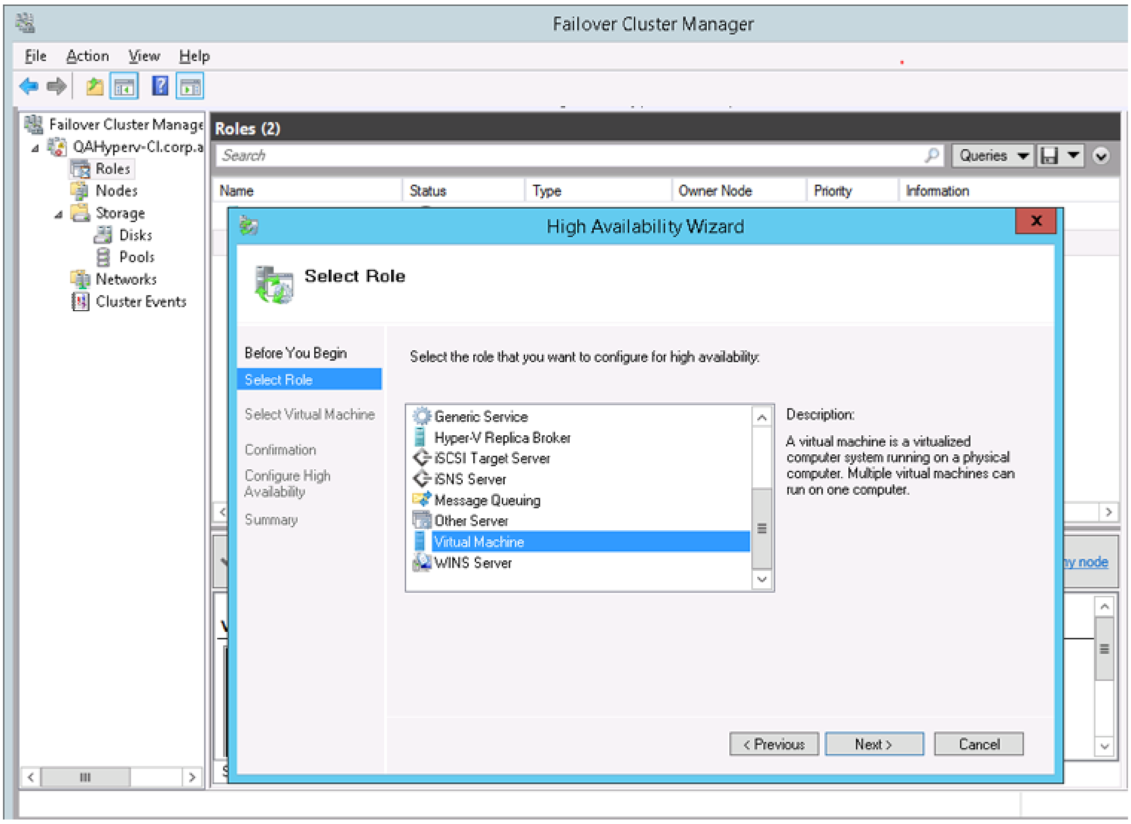
Figure 8-17: Configure Role



Status	Type	Owner Node	Priority	Information
Running	Virtual Machine	QAHyperV1	Medium	
Running	Virtual Machine	QAHyperv2	Medium	

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

Figure 8-18: Choose Virtual Machine



Select the role that you want to configure for high availability:

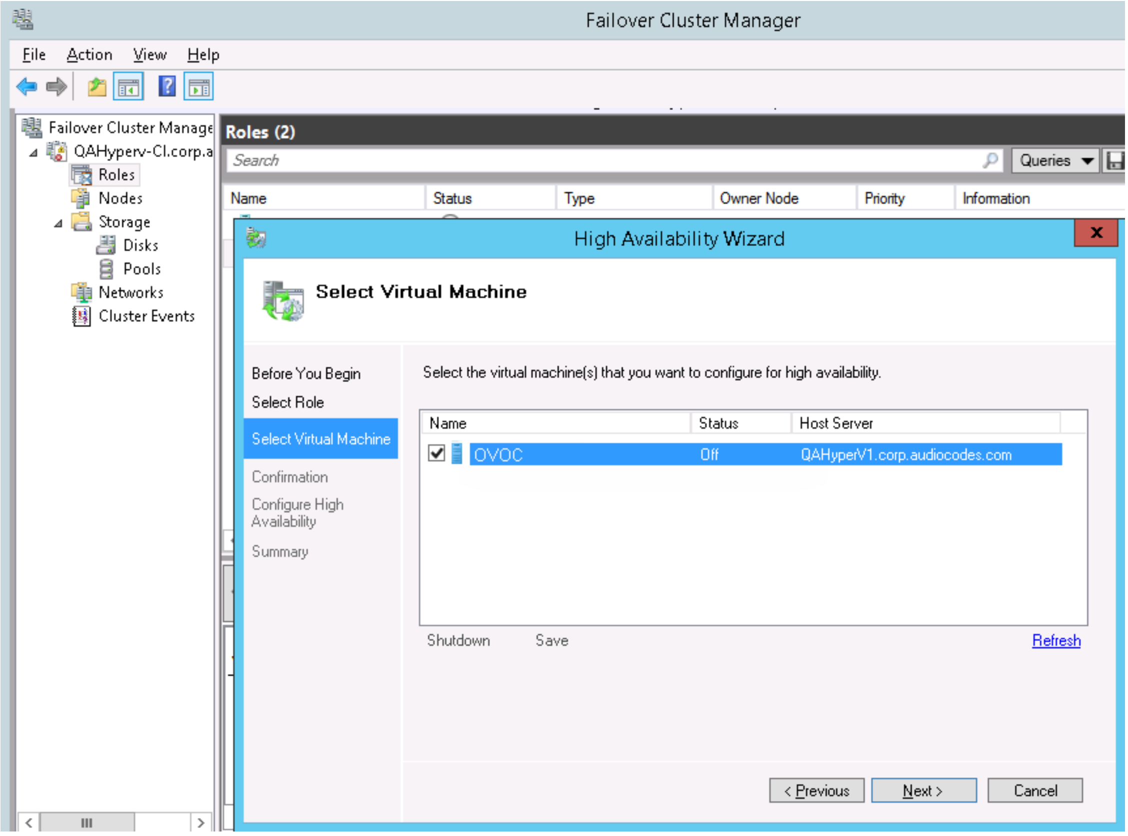
- Generic Service
- Hyper-V Replica Broker
- iSCSI Target Server
- iSNS Server
- Message Queuing
- Other Server
- Virtual Machine
- WINS Server

Description:

A virtual machine is a virtualized computer system running on a physical computer. Multiple virtual machines can run on one computer.

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

Figure 8-19: Confirm Virtual Machine



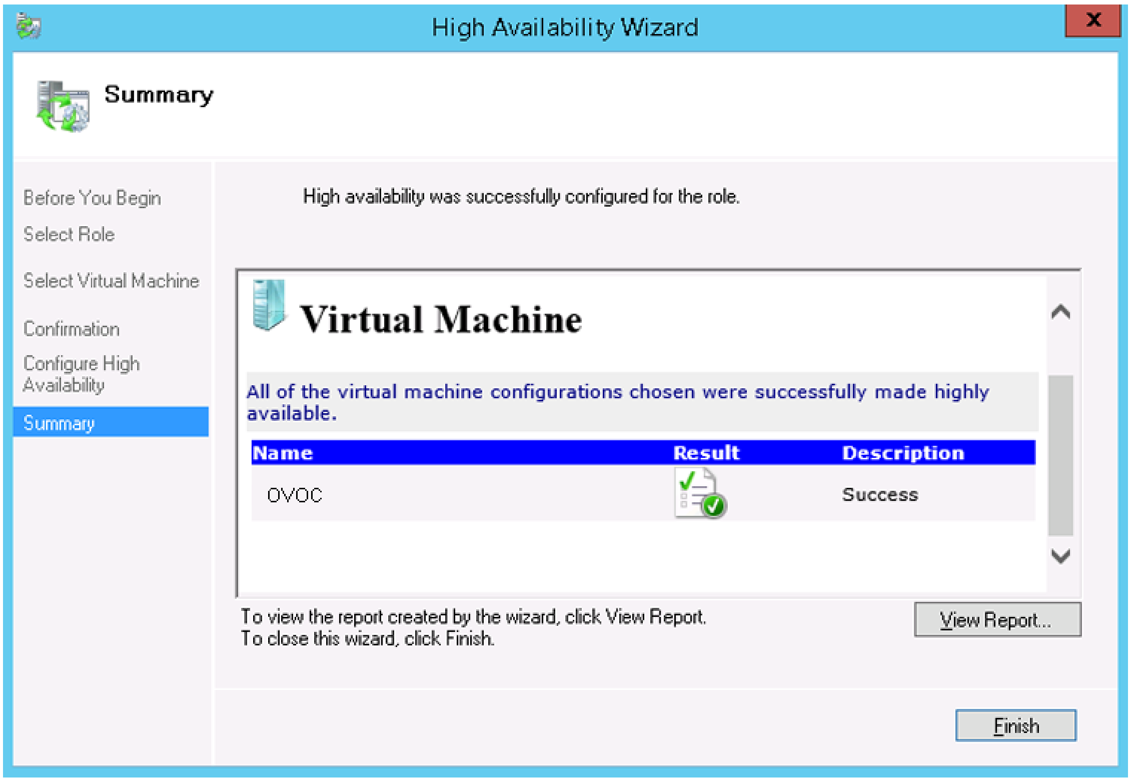
Select the virtual machine(s) that you want to configure for high availability.

Name	Status	Host Server
☑ OVOC	Off	QAHyperV1.corp.audiocodes.com

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

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

Figure 8-20: Virtual Machine Successfully Added



High availability was successfully configured for the role.

Virtual Machine

All of the virtual machine configurations chosen were successfully made highly available.

Name	Result	Description
OVOC	✓	Success

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

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

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

If you wish to manually move the OVOC VMs to another cluster node, see Appendix Managing Clusters on page 278.

Cluster Host Node Failure on Hyper-V

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

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

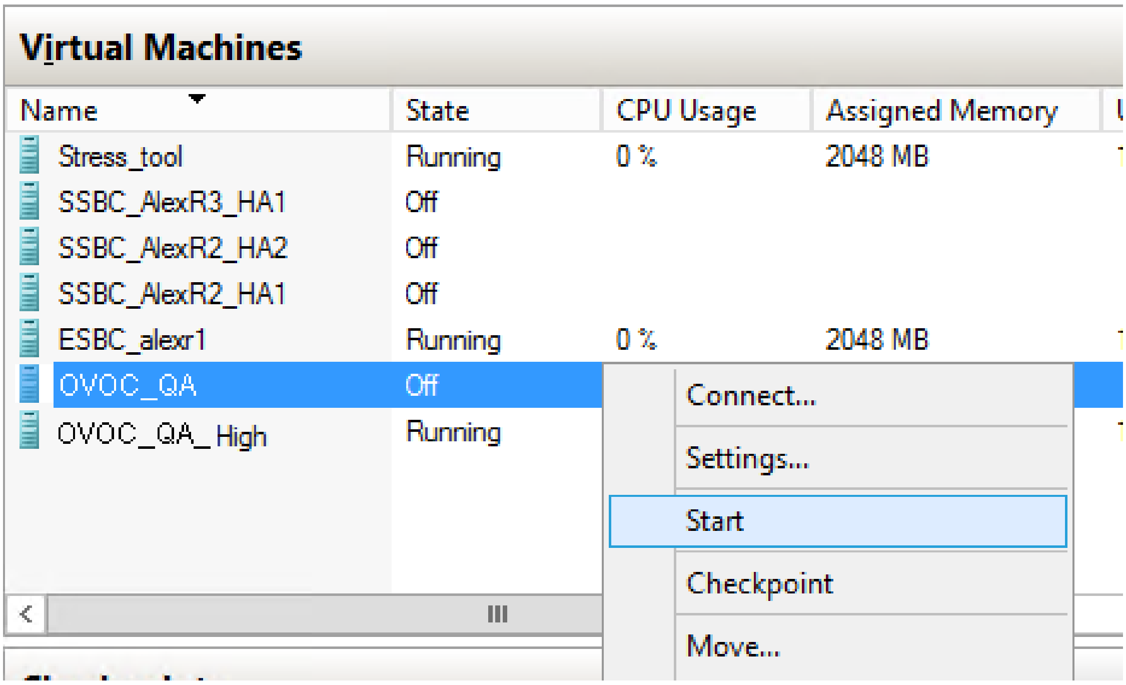
Connecting OVOC Server to Network on HyperV

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

➢ To reconfigure the OVOC server IP address:

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

Figure 8-21: Power On Virtual Machine

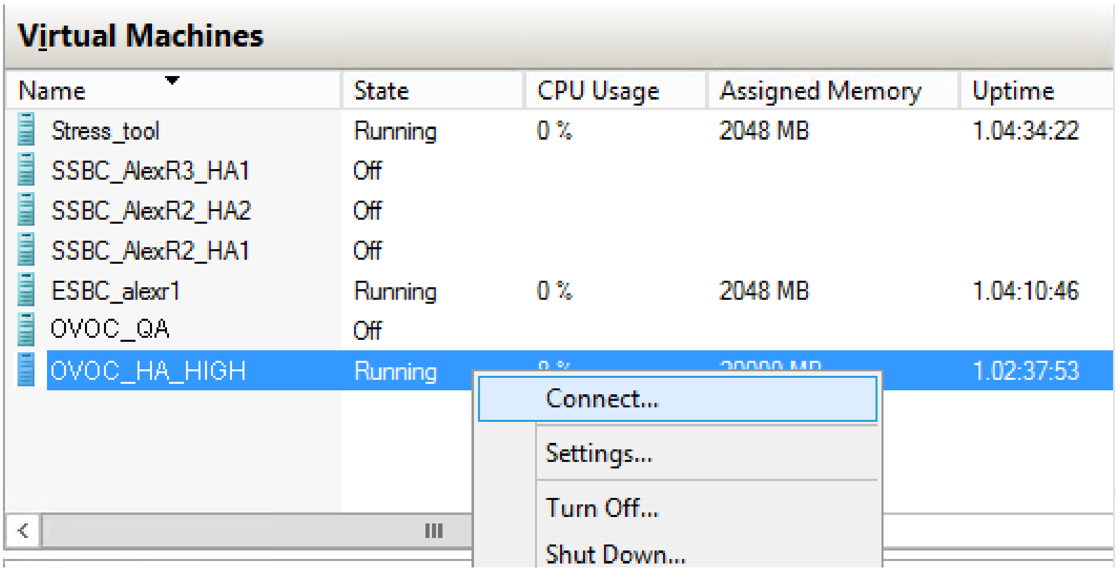


Virtual Machines

Name	State	CPU Usage	Assigned Memory
Stress_tool	Running	0 %	2048 MB
SSBC_AlexR3_HA1	Off		
SSBC_AlexR2_HA2	Off		
SSBC_AlexR2_HA1	Off		
ESBC_alexr1	Running	0 %	2048 MB
OVOC_QA	Off		
OVOC_QA_ High	Running		

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 8-22: 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 %	20000 MB	1.02:37:53

3. Login into the OVOC server by SSH, as ‘acems’ user and enter password *acems*.

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

```
su - root
```

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

```
# EmsServerManager
```

6. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify login to OVOC Web client is successful.

7. Set the OVOC server network IP address to suit your IP addressing scheme (Server IP Address on page 195).

8. Perform other configuration actions as required using the OVOC Server Manager (Getting Started on page 163).

9 Installing OVOC Server on Dedicated Hardware

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

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

⚠

- Ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8). Failure to meet these requirements will lead to the aborting of the installation.
- Installation of OVOC Version 7.8 and later must be performed on HP DL Gen10 machines. Installation on HP DL G8 machines is not supported.
- For obtaining the installation files, see OVOC Software Deliverables on page 15
  - ✓ Note that you must verify this file, see Files Verification on page 18

DVD1: Linux CentOS

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

⚠ Before commencing the installation, you must configure RAID-0 (see Appendix Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen10 Servers on page 275).

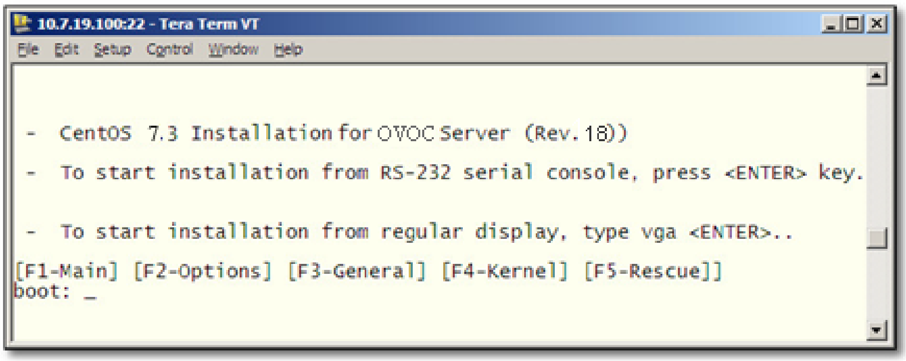
➢ **To perform DVD1 installation:**

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

```
reboot
```

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

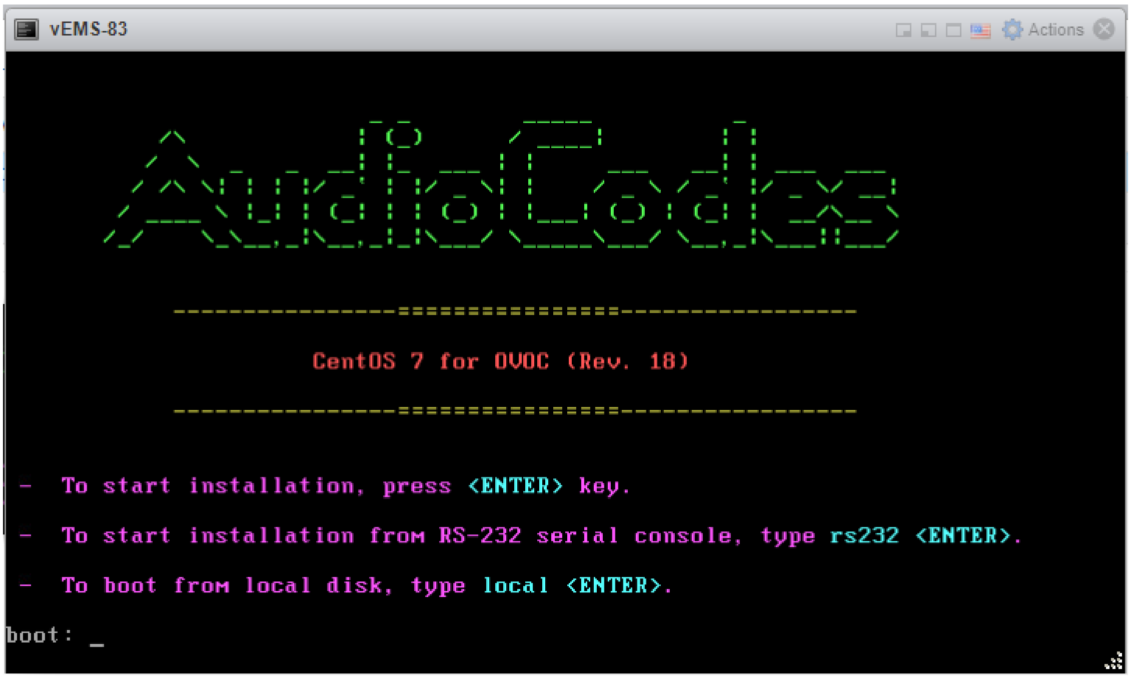
Figure 9-1: Linux CentOS Installation



10.7.19.100:22 - Tera Term VT
File Edit Setup Control Window Help

```
 -  CentOS  7.3 Installation for OVOC Server  (Rev. 18))
 -  To start installation from RS-232 serial console, press <ENTER> key.

 -  To start installation from regular display, type vga <ENTER>..
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]]
boot: _
```

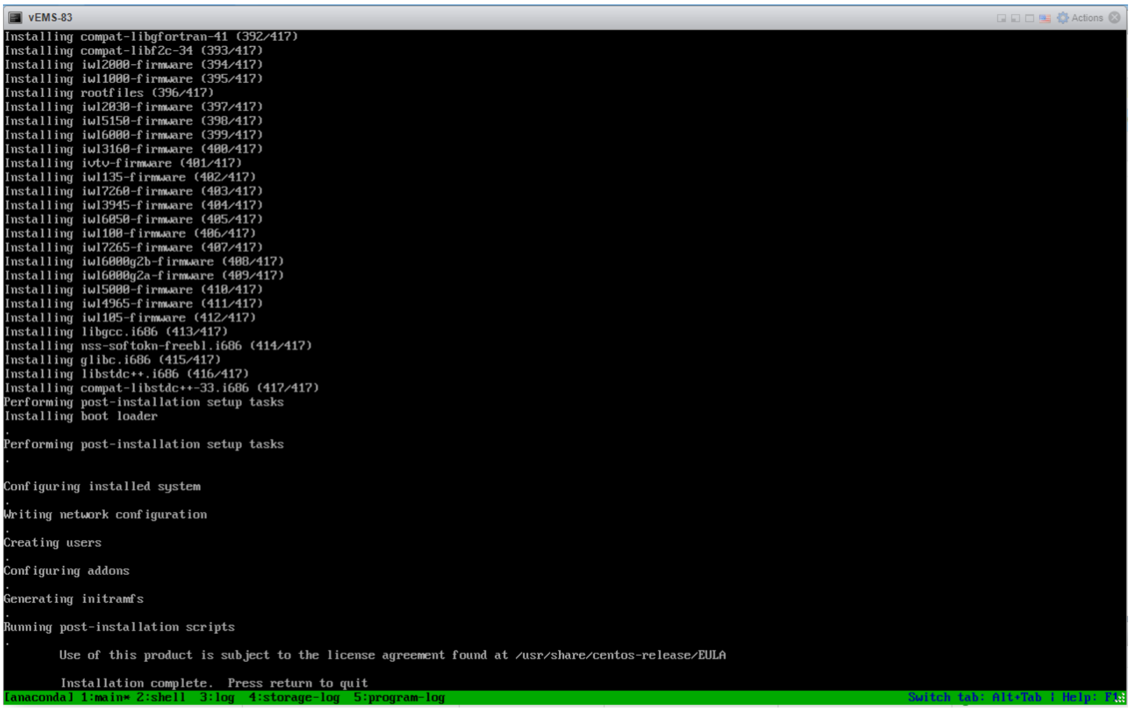
Figure 9-2: CentOS



```
         -----------------================----------------

                    CentOS 7 for OVOC (Rev. 18)

         -----------------================----------------


 -  To start installation, press <ENTER> key.

 -  To start installation from RS-232 serial console, type rs232 <ENTER>.

 -  To boot from local disk, type local <ENTER>.

boot: _
```

6. Wait for the installation to complete.

Figure 9-3: CentOS Installation

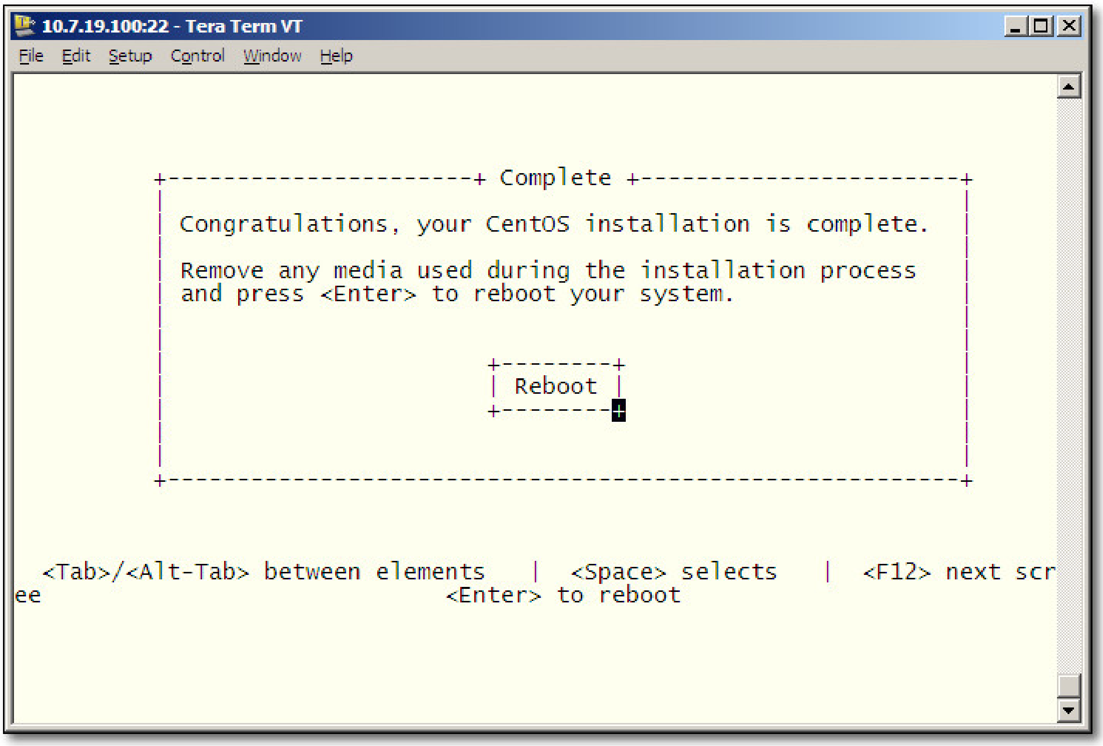


```
Installing compat-libgfortran-41 (392/417)
Installing compat-libf2c-34 (393/417)
Installing iwl2000-firmware (394/417)
Installing iwl1000-firmware (395/417)
Installing rootfiles (396/417)
Installing iwl2030-firmware (397/417)
Installing iwl5150-firmware (398/417)
Installing iwl6000-firmware (399/417)
Installing iwl3160-firmware (400/417)
Installing ivtv-firmware (401/417)
Installing iwl135-firmware (402/417)
Installing iwl7260-firmware (403/417)
Installing iwl3945-firmware (404/417)
Installing iwl6050-firmware (405/417)
Installing iwl100-firmware (406/417)
Installing iwl7265-firmware (407/417)
Installing iwl6000g2b-firmware (408/417)
Installing iwl6000g2a-firmware (409/417)
Installing iwl5000-firmware (410/417)
Installing iwl4965-firmware (411/417)
Installing iwl105-firmware (412/417)
Installing libgcc.i686 (413/417)
Installing nss-softokn-freebl.i686 (414/417)
Installing glibc.i686 (415/417)
Installing libstdc++.i686 (416/417)
Installing compat-libstdc++-33.i686 (417/417)
Performing post-installation setup tasks
Installing boot loader
.
Performing post-installation setup tasks
.

Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
.
        Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA

        Installation complete.  Press return to quit
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log                    Switch tab: Alt+Tab | Help: F1
```

7. Reboot your machine by pressing **Enter**.

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

Figure 9-4: Linux CentOS Installation Complete

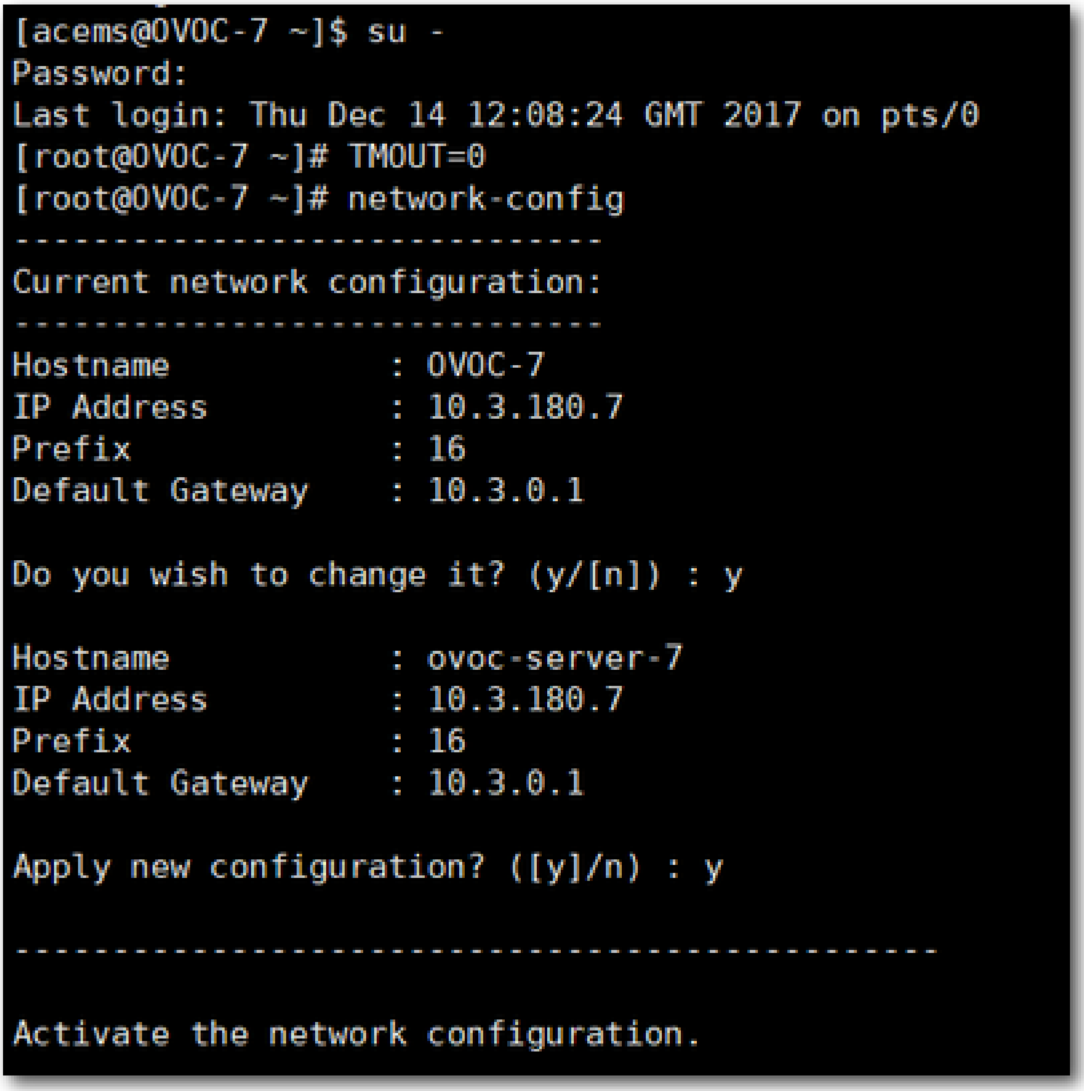


```
          +---------------------+ Complete +-----------------------+
          |                                                        |
          | Congratulations, your CentOS installation is complete. |
          |                                                        |
          | Remove any media used during the installation process  |
          | and press <Enter> to reboot your system.               |
          |                                                        |
          |                                                        |
          |                       +--------+                       |
          |                       | Reboot |                       |
          |                       +--------+                       |
          |                                                        |
          |                                                        |
          +--------------------------------------------------------+



  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next scr
ee                              <Enter> to reboot
```

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

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

Figure 9-5: Linux CentOS Network Configuration



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

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

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

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

-----------------------------------------------

Activate the network configuration.
```

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

10. You are prompted to change the configuration; enter **y**.

11. Enter your Hostname, IP Address, Subnet Mask and Default Gateway.

12. Confirm the changes; enter **y**.

13. You are prompted to reboot; enter **y**.

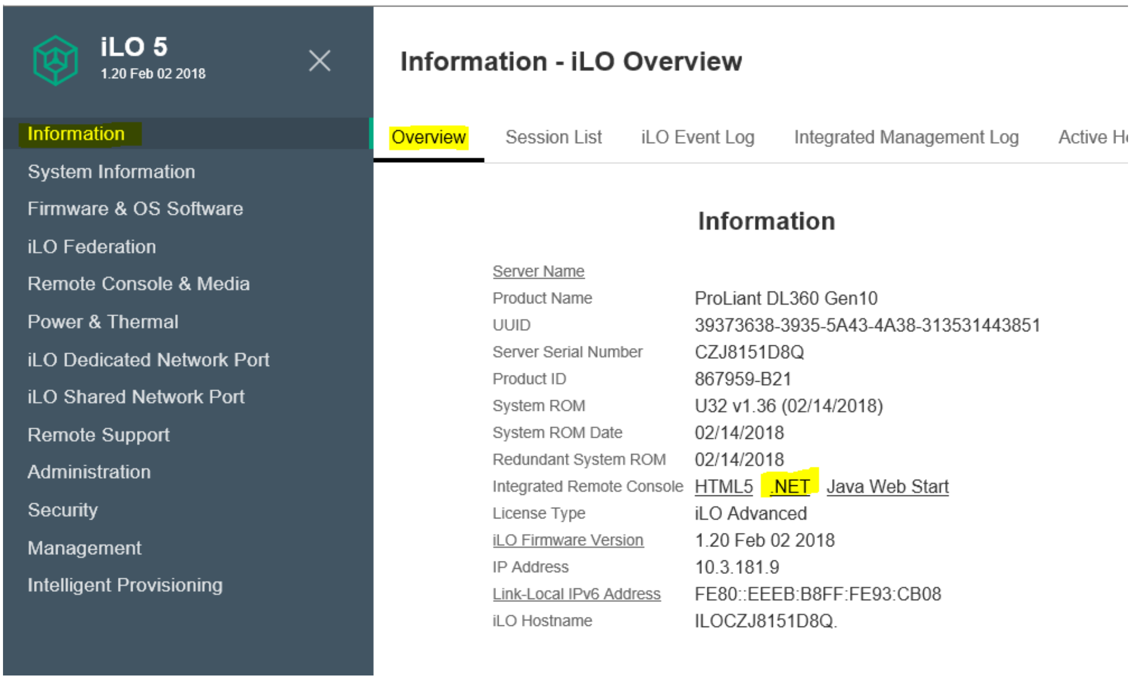
Installing DVD1 without a CD-ROM

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

➢ To install DVD1 without a CD-ROM:

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

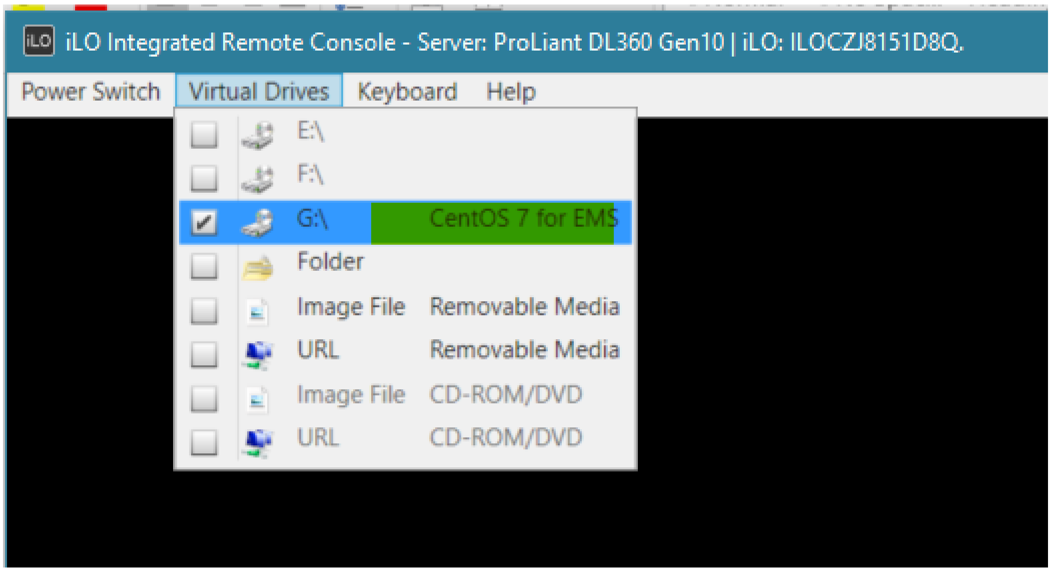
Figure 9-6: Information-iLO Overview



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

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

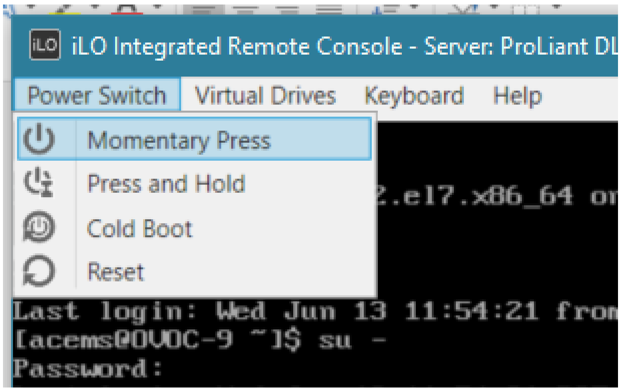
Figure 9-7: iLO Integrated Remote Console


iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.
Power Switch
Virtual Drives
Keyboard
Help

- □ E:\
- □ F:\
- ☑ G:\ CentOS 7 for EMS
- □ Folder
- □ Image File Removable Media
- □ URL Removable Media
- □ Image File CD-ROM/DVD
- □ URL CD-ROM/DVD

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

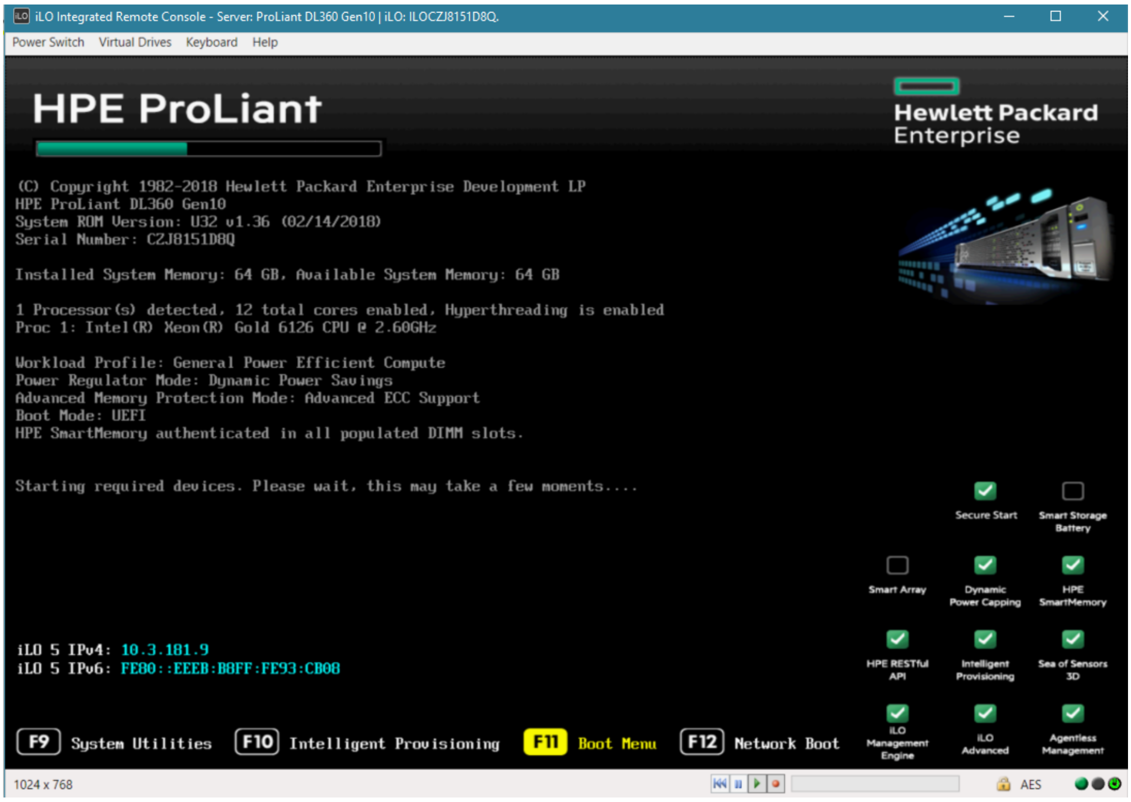
Figure 9-8: Momentary Press



```
2.el7.x86_64 on
Last login: Wed Jun 13 11:54:21 from
[acems@OVOC-9 ~]$ su -
Password:
```

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

Figure 9-9: Boot Menu

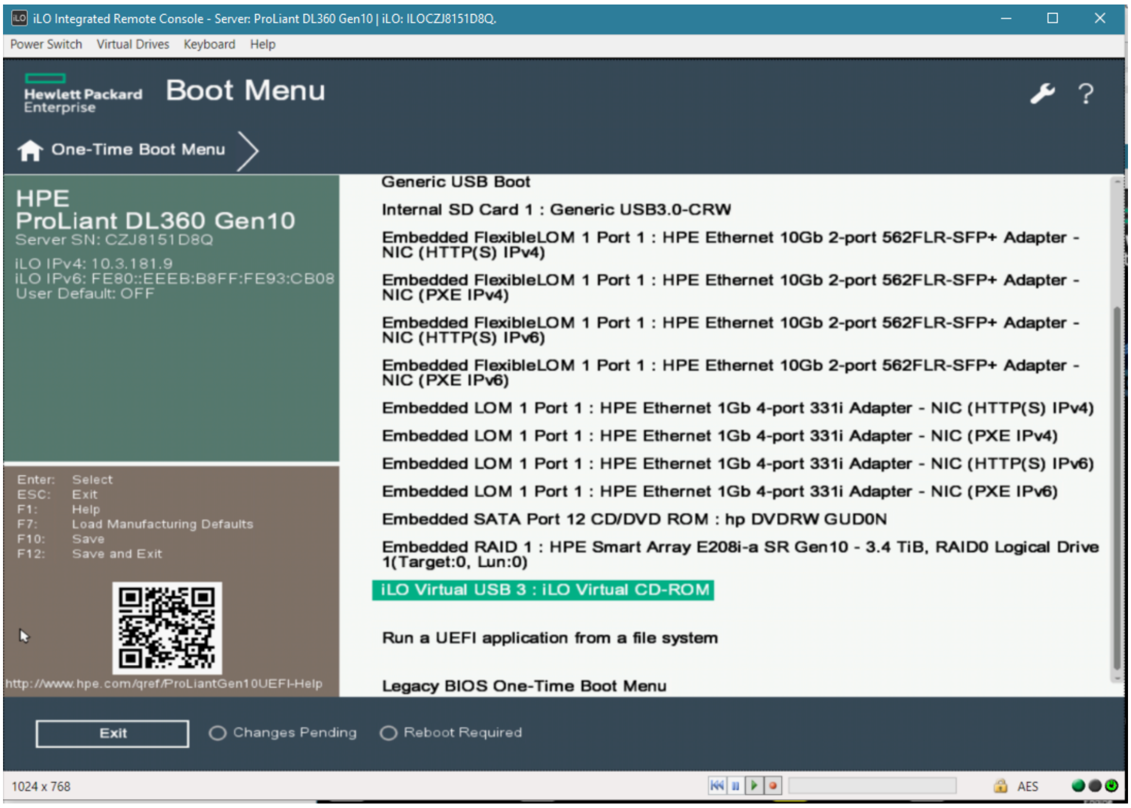


iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.
Power Switch
Virtual Drives
Keyboard
Help
HPE ProLiant
Hewlett Packard Enterprise

```
(C) Copyright 1982-2018 Hewlett Packard Enterprise Development LP
HPE ProLiant DL360 Gen10
System ROM Version: U32 v1.36 (02/14/2018)
Serial Number: CZJ8151D8Q

Installed System Memory: 64 GB, Available System Memory: 64 GB

1 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz

Workload Profile: General Power Efficient Compute
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Boot Mode: UEFI
HPE SmartMemory authenticated in all populated DIMM slots.

Starting required devices. Please wait, this may take a few moments....

iLO 5 IPv4: 10.3.181.9
iLO 5 IPv6: FE80::EEEB:B8FF:FE93:CB08

F9 System Utilities   F10 Intelligent Provisioning   F11 Boot Menu   F12 Network Boot
```

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

Figure 9-10: Boot Sequence



iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.

Power Switch Virtual Drives Keyboard Help

Hewlett Packard Enterprise Boot Menu

One-Time Boot Menu

HPE
ProLiant DL360 Gen10
Server SN: CZJ8151D8Q
iLO IPv4: 10.3.181.9
iLO IPv6: FE80::EEEB:B8FF:FE93:CB08
User Default: OFF

Enter: Select
ESC: Exit
F1: Help
F7: Load Manufacturing Defaults
F10: Save
F12: Save and Exit

http://www.hpe.com/qref/ProLiantGen10UEFI-Help

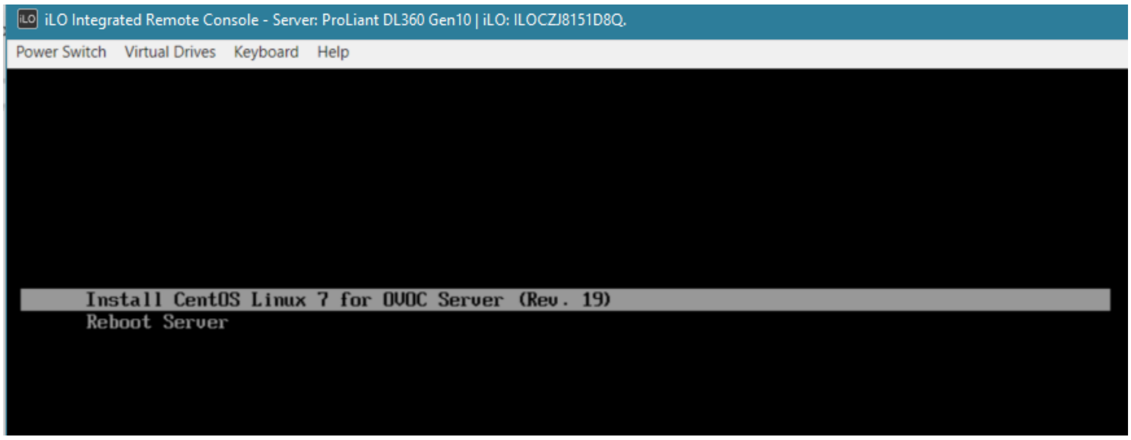
Generic USB Boot
Internal SD Card 1 : Generic USB3.0-CRW
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (HTTP(S) IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (PXE IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (HTTP(S) IPv6)
Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC (PXE IPv6)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (HTTP(S) IPv4)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (PXE IPv4)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (HTTP(S) IPv6)
Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adapter - NIC (PXE IPv6)
Embedded SATA Port 12 CD/DVD ROM : hp DVDRW GUD0N
Embedded RAID 1 : HPE Smart Array E208i-a SR Gen10 - 3.4 TiB, RAID0 Logical Drive 1(Target:0, Lun:0)
iLO Virtual USB 3 : iLO Virtual CD-ROM
Run a UEFI application from a file system
Legacy BIOS One-Time Boot Menu

Exit ○ Changes Pending ○ Reboot Required

1024 x 768 AES

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

Figure 9-11: Install CentOS



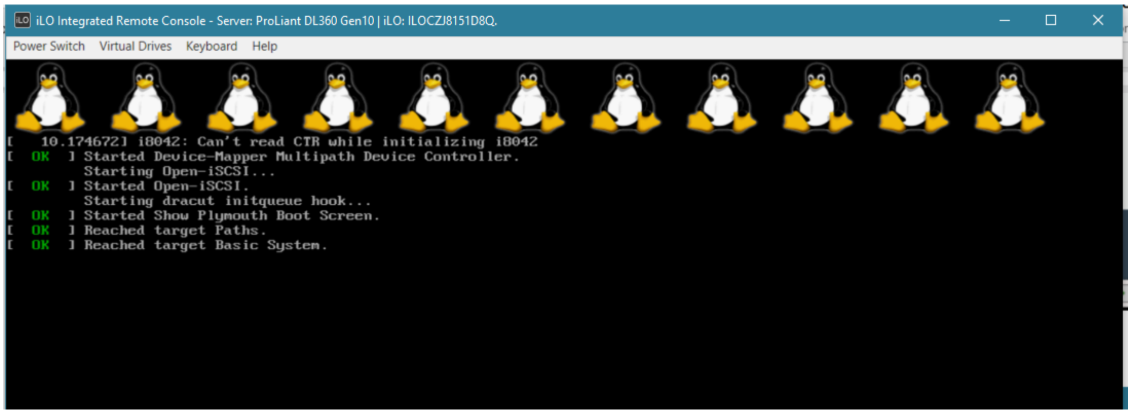
iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.

Power Switch Virtual Drives Keyboard Help

```
Install CentOS Linux 7 for OVOC Server (Rev. 19)
Reboot Server
```

8. After a while the CentOS installation commences:

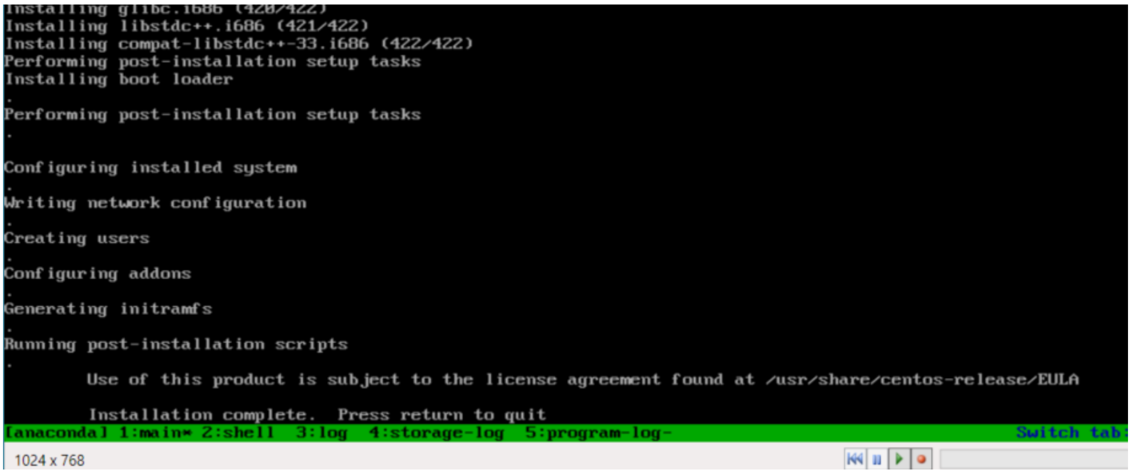
Figure 9-12: Start CentOS


iLO Integrated Remote Console - Server: ProLiant DL360 Gen10 | iLO: ILOCZJ8151D8Q.
Power Switch
Virtual Drives
Keyboard
Help

```
[   10.174672] i8042: Can't read CTR while initializing i8042
[  OK  ] Started Device-Mapper Multipath Device Controller.
         Starting Open-iSCSI...
[  OK  ] Started Open-iSCSI.
         Starting dracut initqueue hook...
[  OK  ] Started Show Plymouth Boot Screen.
[  OK  ] Reached target Paths.
[  OK  ] Reached target Basic System.
```

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

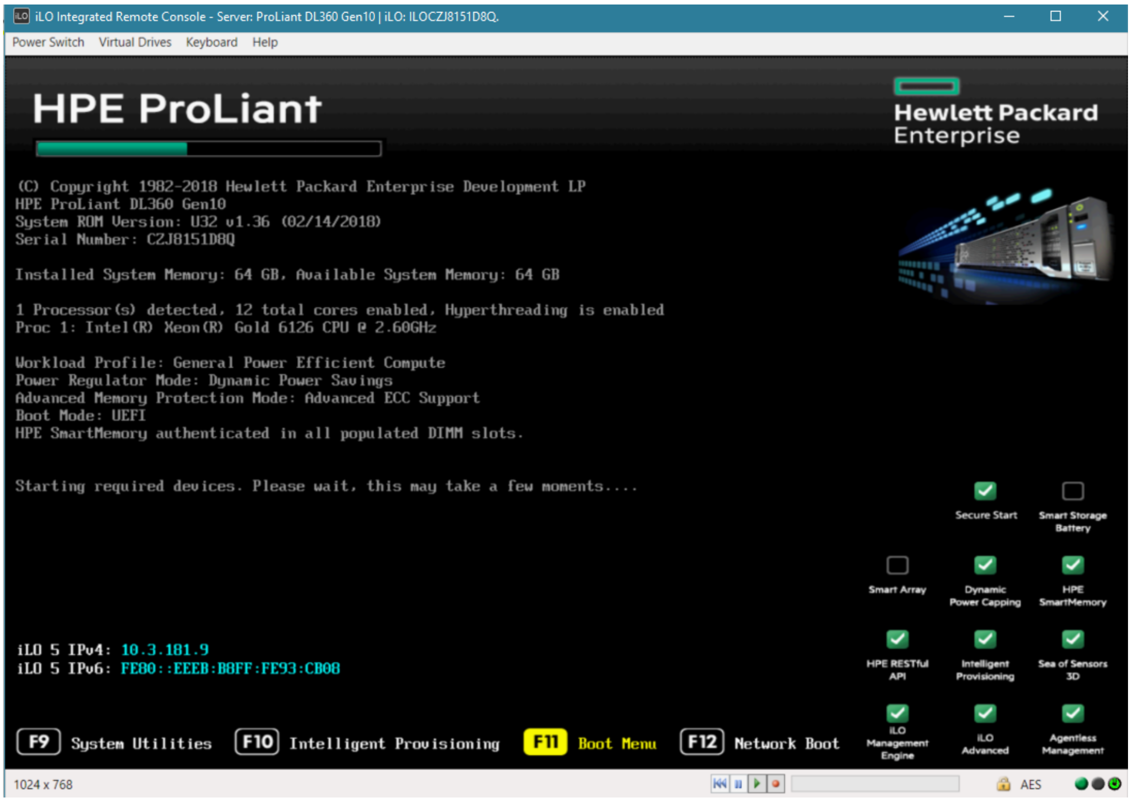
Figure 9-13: Server Rebooted



```
Installing glibc.i686 (420/422)
Installing libstdc++.i686 (421/422)
Installing compat-libstdc++-33.i686 (422/422)
Performing post-installation setup tasks
Installing boot loader
.
Performing post-installation setup tasks
.

Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
.
        Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA

        Installation complete.  Press return to quit
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log-                          Switch tab:
```

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

Figure 9-14: Boot Menu



```
(C) Copyright 1982-2018 Hewlett Packard Enterprise Development LP
HPE ProLiant DL360 Gen10
System ROM Version: U32 v1.36 (02/14/2018)
Serial Number: CZJ8151D8Q

Installed System Memory: 64 GB, Available System Memory: 64 GB

1 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz

Workload Profile: General Power Efficient Compute
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Boot Mode: UEFI
HPE SmartMemory authenticated in all populated DIMM slots.

Starting required devices. Please wait, this may take a few moments....

iLO 5 IPv4: 10.3.181.9
iLO 5 IPv6: FE80::EEEB:B8FF:FE93:CB08
```

DVD2: Oracle DB Installation

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

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

➢ To perform DVD2 installation:

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

```
su - root
```

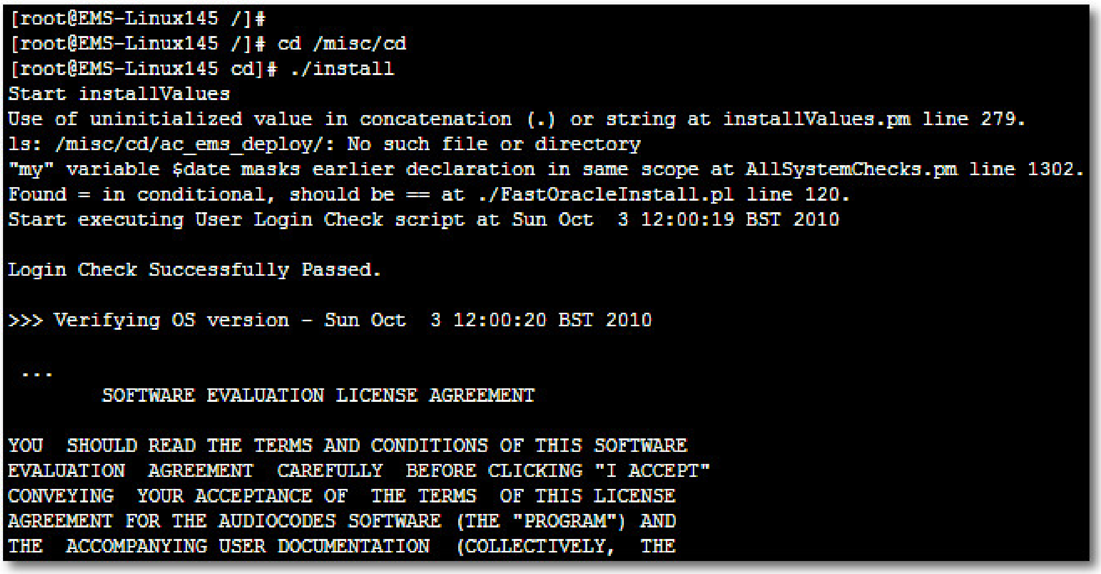
4. Mount the CDROM to make it available:

```
mount /home/acems/DVD2_EMS_.iso /mnt
```

5. Run the installation script from its location:

```
./install
```

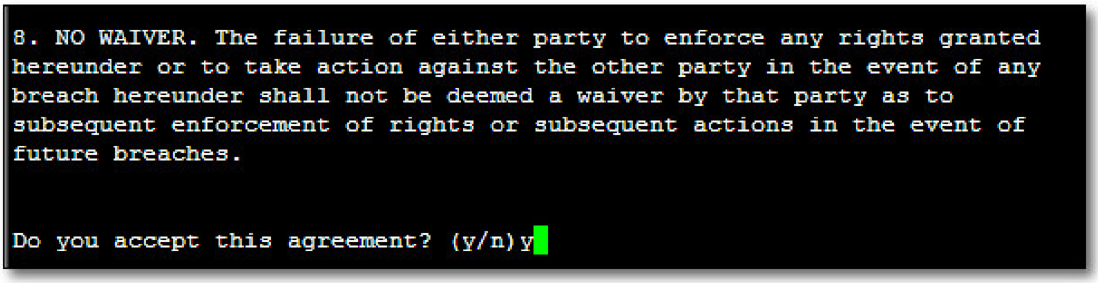
Figure 9-15: Oracle DB Installation



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

Login Check Successfully Passed.

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

 ...
        SOFTWARE EVALUATION LICENSE AGREEMENT

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

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

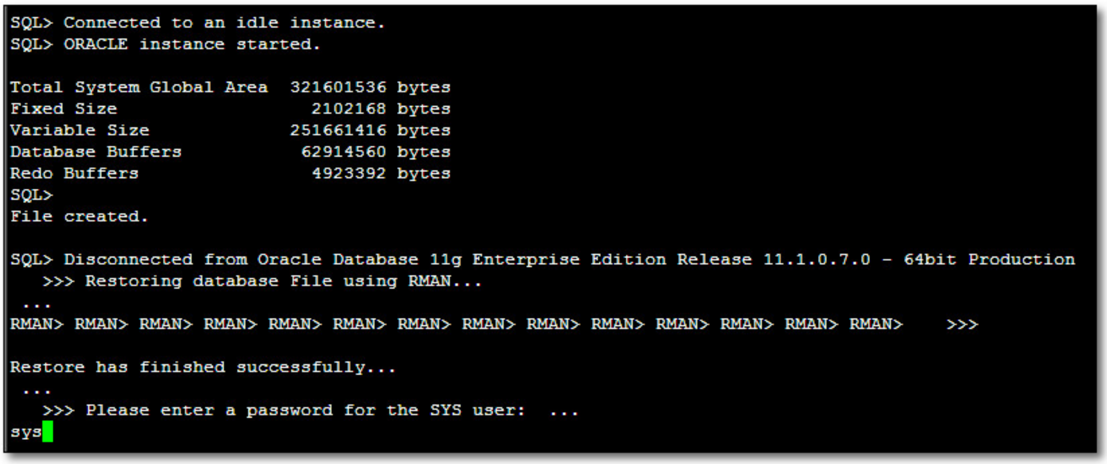
Figure 9-16: Oracle DB Installation - License Agreement



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


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

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

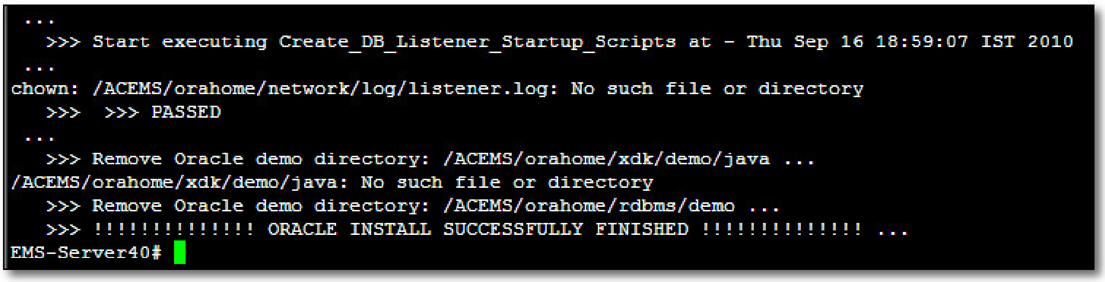
Figure 9-17: Oracle DB Installation (cont)



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

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

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

Restore has finished successfully...
 ...
   >>> Please enter a password for the SYS user:  ...
sys
```

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

Figure 9-18: Oracle DB Installation



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

DVD3: OVOC Server Application Installation

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

➢ To perform DVD3 installation:

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

```
su - root
```

4. Mount the CDROM to make it available:

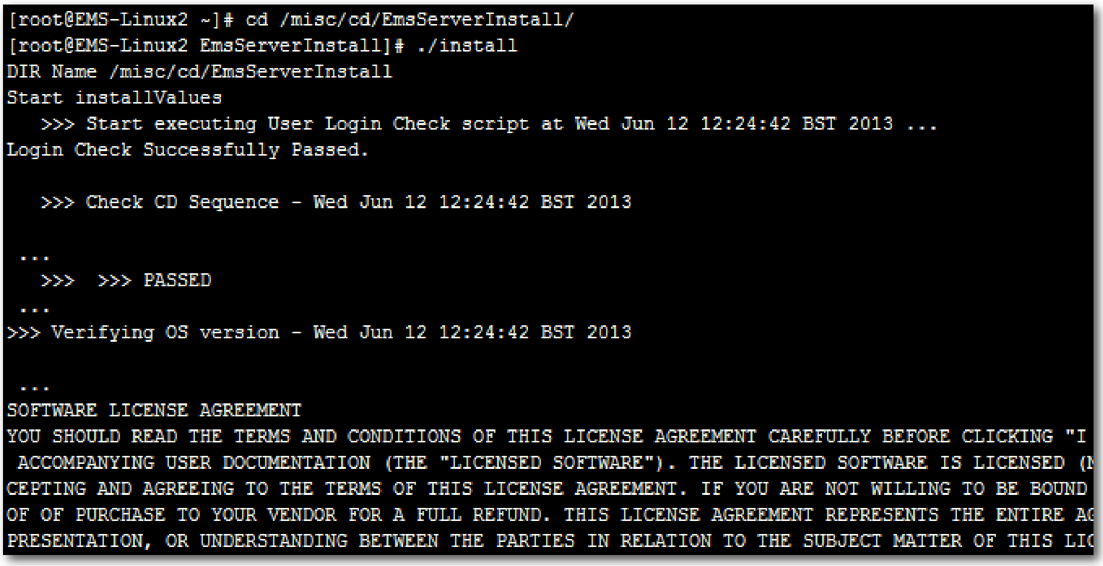
```
mount /home/acems/DVD3_EMS_.iso /mnt/EmsServerInstall/
```

```
cd /mnt/EmsServerInstall/
```

5. Run the installation script from its location:

```
./install
```

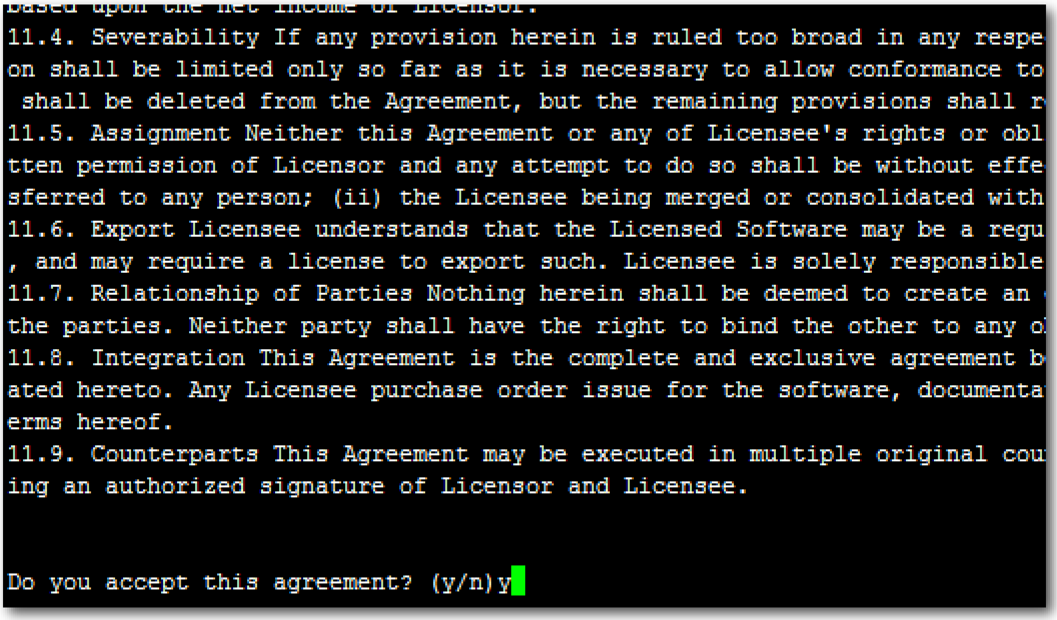
Figure 9-19: OVOC server Application Installation



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

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

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

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

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

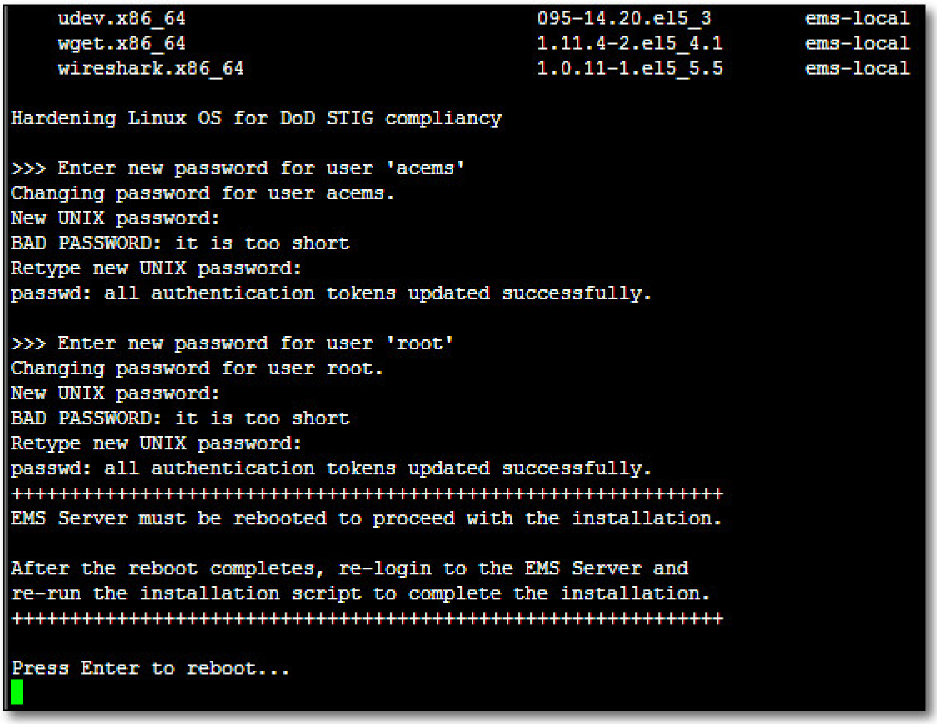
   Figure 9-20: OVOC server Application Installation – License Agreement



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


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

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

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

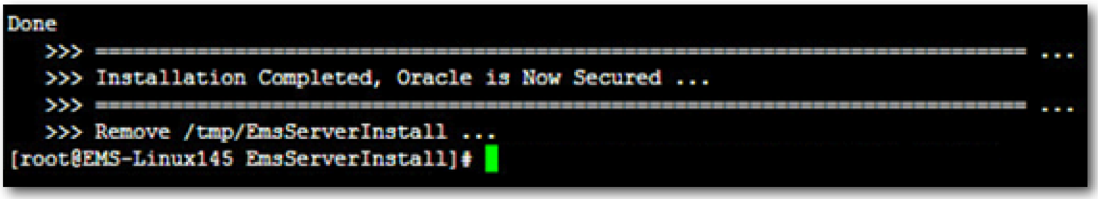


```
    udev.x86_64                                       095-14.20.el5_3       ems-local
    wget.x86_64                                       1.11.4-2.el5_4.1      ems-local
    wireshark.x86_64                                  1.0.11-1.el5_5.5      ems-local

Hardening Linux OS for DoD STIG compliancy

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

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

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

Press Enter to reboot...
```

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

After the OVOC server has rebooted, repeat steps Login into the OVOC server by SSH, as 'acems' user and enter password acems (or customer defined password). on page 147 to Enter y, and then press Enter to accept the License agreement. on page 148.

Figure 9-22: OVOC server Installation Complete



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

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

```
su - root
```

12. Type the following command:

```
# EmsServerManager
```

13. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify login to the OVOC Web client is successful.

14. Verify that the Date and Time are set correctly (Date and Time Settings on page 216).

15. Configure other settings as required (Getting Started on page 163).

10 Managing Device Connections

When the connections between the OVOC server and the managed devices traverse a NAT or firewall, direct connections cannot be established (both for OVOC > Device connections and for Device > OVOC connections). OVOC provides methods for overcoming this issue. These methods can be used for both initial setup and Second-Day management:

- Establishing OVOC-Devices Connections below
- Establishing Devices - OVOC Connections on the next page

The table below describes the different connection scenarios.

Table 10-1: Device Connection Scenarios

Configuration Option/Deployment Scenario	OVOC				Devices		
	AWS Cloud	Azure Cloud	On-Premises	Over Public Network	AWS Cloud	Azure Cloud	On-Premises
AudioCodes SBC Devices							
Cloud Architecture Mode	√	√		-	√	√	√
OVOC Server Configured with Public IP	√	√	√	√	√	√	√
Phones							
Device Manager Agent	-	-	√	-	-	-	√

- For OVOC Managed devices: All remote connections for OVOC managed devices require a configured WAN interface on the managed device.
- For more information for phone and Jabra/Third-party vendor device connections, refer to the *OVOC Security Guidelines* and to the *Device Manager Agent Installation and Configuration Guide/Device Manager for Third-Party Vendor Products Administrator's Manual.*

Establishing OVOC-Devices Connections

When OVOC is deployed behind a firewall or NAT in the cloud or in a remote network, it cannot establish a direct connection with managed devices using its private IP address. Consequently, you must configure the OVOC Server IP address as follows:

- For OVOC Cloud deployments: Configure the OVOC server public IP address.

- For OVOC deployments in a remote public network: Configure the IP address of the NAT router.

See Configure OVOC Server with Public or NAT IP Address below

Configure OVOC Server with Public or NAT IP Address

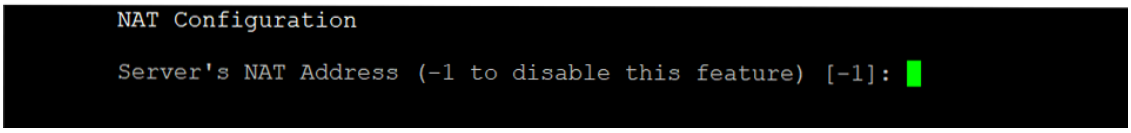
This option lets you configure the OVOC server with a public IP address which enables devices that are deployed behind a NAT in a remote Enterprise or Cloud network to connect to OVOC.

When the "Cloud Architecture" mode is enabled, this option is removed from the OVOC Server Manager " Network Configuration" menu.

➢ To configure OVOC Server with Public IP address:

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

Figure 10-1: Configure NAT IP



```
NAT Configuration

Server's NAT Address (-1 to disable this feature) [-1]:
```

2. Enter the NAT IP address, and then press Enter.
3. Type **y** to confirm the changes.
4. Stop and start the OVOC server for the changes to take effect.

➢ To remove NAT configuration:

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

Establishing Devices - OVOC Connections

When devices are deployed behind a firewall or NAT in the cloud or in a remote network, they cannot connect establish a direct connection with the OVOC server. Consequently, the following methods can be used to overcome this issue:

- **Automatic Detection:** devices are connected automatically to OVOC through sending SNMP Keep-alive messages. See Automatic Detection on the next page.
- **OVOC Cloud Architecture Mode:** Communication between OVOC deployed in the AWS Cloud and devices deployed either in the AWS Cloud or in a remote network are secured over an HTTP/S tunnel overlay network. See Configure OVOC Cloud Architecture Mode on the next page

- This mode is only supported for OVOC deployment on Amazon AWS.
- Single Sign-on from OVOC Web to managed device's Web interface is only supported for the "Cloud Architecture Mode" option.

Automatic Detection

The Automatic Detection feature enables devices to be automatically connected to OVOC over SNMP. When devices are connected to the power supply in the enterprise network and/or are rebooted and initialized, they're automatically detected by the OVOC and added by default to the AutoDetection region. For this feature to function, devices must be configured with the OVOC server's IP address and configured to send keep-alive messages. OVOC then connects to the devices and automatically determines their firmware version and subnet. Devices are then added to the appropriate tenant/region according to the best match for subnet address. When a default tenant exists, devices that cannot be successfully matched with a subnet are added to an automatically created AutoDetection Region under the default tenant. When a default tenant does not exist and the device cannot be matched with a subnet, the device isn't added to OVOC.

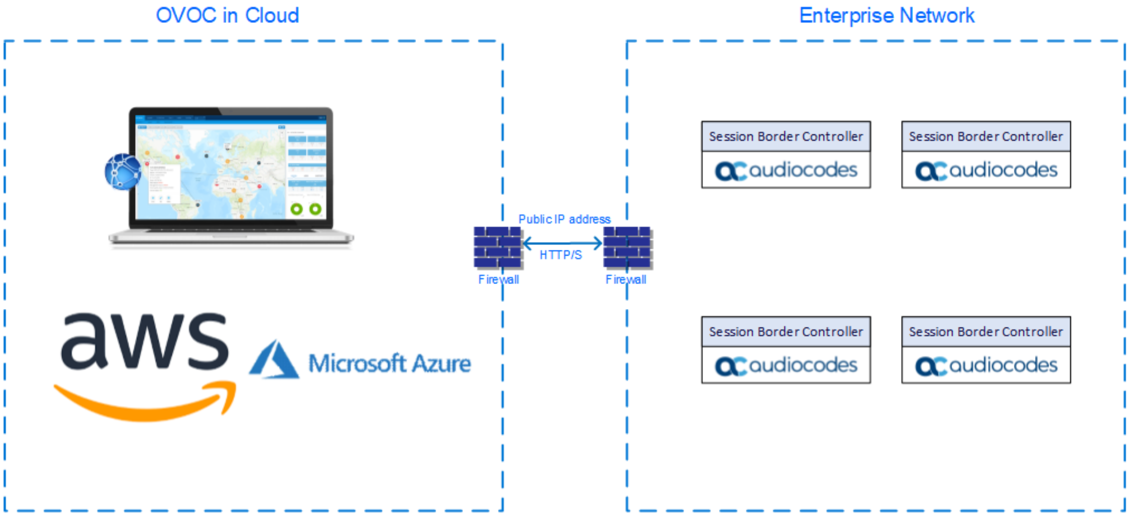
For more information, refer to Section "Adding AudioCodes Devices Automatically" in the *OVOC User's Manual*.

Configure OVOC Cloud Architecture Mode

When OVOC is deployed in a public cloud and managed devices are either deployed in the Cloud or in an enterprise network, an automatic mechanism can be enabled to secure the OVOC server and SBC device communication through binding to a dedicated HTTP/S tunnel through a generic WebSocket server connection. This mechanism binds several different port connections including SNMP, HTTP, syslog and debug recording into an HTTP/S tunnel overlay network. This eliminates the need for administrators to manually manage firewall rules for these connections and to lease third-party VPN services. When operating in this mode, Single Sign-on can also be performed from the Devices Page link in the OVOC Web interface to SBC devices deployed behind a NAT. The figure below illustrates the OVOC Cloud Architecture.

This mode is supported for both Microsoft Azure and Amazon AWS deployments for all SBC devices released in Version 7.2.256.

Figure 10-2: Cloud Architecture



This section includes the following:

- Before Enabling Cloud Architecture Mode below
- Configuring Cloud Architecture Mode on the next page

Before Enabling Cloud Architecture Mode

Before enabling Cloud Architecture mode, ensure the following:

- Ensure HTTPS port 80 or HTTPS port 443 are open on the Enterprise firewall.

> - For maximum security, its advised to implement this connection over HTTPS port 443 with One-way authentication. Mutual authentication is not supported for this mode.
> - This connection can be secured using either AudioCodes certificates or custom certificates.

- Ensure that all managed devices have been upgraded to the software version that supports this feature (refer to *SBC-Gateway Series Release Notes for Latest Release Versions 7.2*)

> If devices are not appropriately upgraded then they cannot be managed in OVOC.

- Ensure that the following parameters have been configured for the managed devices (for more information, refer to the relevant SBC User's Manual):
  - WSTunServerAddress; WSTunServerPath; WSTunUsername; WSTunPassword; WSTunSecured; WSTunVerifyPeer
- In the OVOC Web interface, the SBC Devices Communication parameter **must** be set to **IP Based** in the Configuration screen (**System** tab > **Administration** menu > **OVOC Server** folder > Configuration); **do not** use an FQDN when working in Cloud Architecture mode.

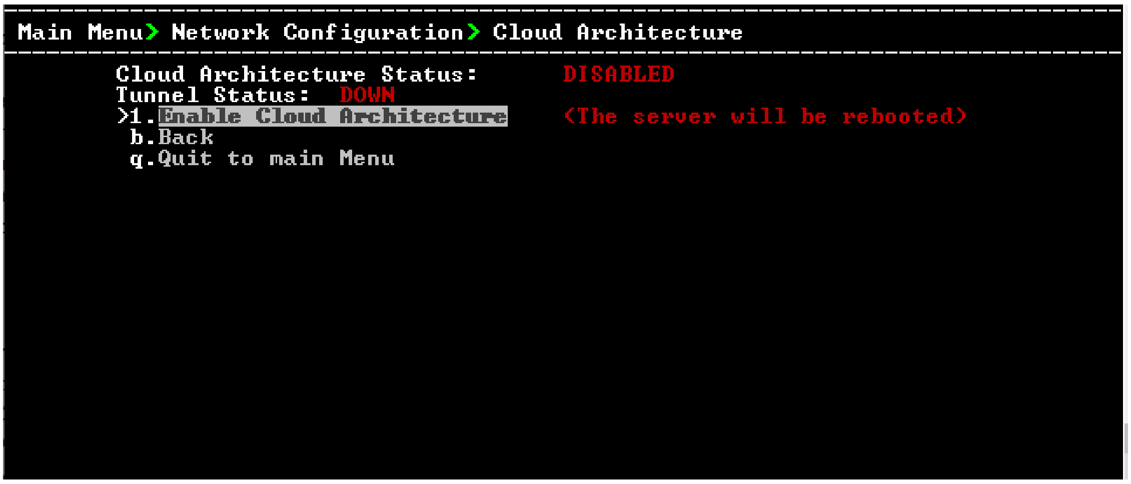
Configuring Cloud Architecture Mode

This option configures the OVOC server in a cloud topology. When configured, a "secure tunnel“ overlay network” is established between the connected devices and the OVOC server. This connection is secured over a WebSocket connection. The Tunnel Status indicates the status for all sub-processes running for this architecture.

➢ To setup cloud architecture:

1. From the Network Configuration menu, choose **Cloud Architecture.**

Figure 10-3: Cloud Architecture



```
Main Menu> Network Configuration> Cloud Architecture

        Cloud Architecture Status:       DISABLED
        Tunnel Status:   DOWN
        >1.Enable Cloud Architecture     (The server will be rebooted)
         b.Back
         q.Quit to main Menu
```

2. Select option **Enable Cloud Architecture**. The OVOC server is restarted.

> ⚠ When this option is configured, the NAT configuration option is disabled.

Part III

OVOC Server Upgrade

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

11 Upgrading OVOC Server on Amazon AWS and Microsoft Azure

This section describes how to upgrade the OVOC server on the Amazon AWS and Microsoft Azure platforms.

- Before proceeding, it is highly recommended to backup the OVOC server files to an external location (see OVOC server Backup).
- Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8). Failure to meet these requirements will lead to the aborting of the upgrade.
- For obtaining the upgrade file, see OVOC Software Deliverables on page 15
  - ✔ Note that you must verify this file, see Files Verification on page 18
- For before upgrade actions, see Before Upgrading on Microsoft Azure on page 121
- For after upgrade actions, see After Upgrading on AWS on page 121

➢ To upgrade the OVOC server on Cloud platforms:

1. Copy the **DVD3** ISO file that you received from AudioCodes to your PC.
2. Using WinSCP utility (see Transferring Files on page 295), copy the .ISO file to the OVOC server acems user home directory: /home/acems
3. Open an SSH connection.
4. Login into the OVOC server as *acems* user with password *acems* (or customer defined password).
5. Switch to 'root' user

```
su - root
```

6. Mount the DVD3.iso file to the /mnt directory:

```
mount /home/acems/DVD3_EMS_ 8.0.110.iso /mnt
```

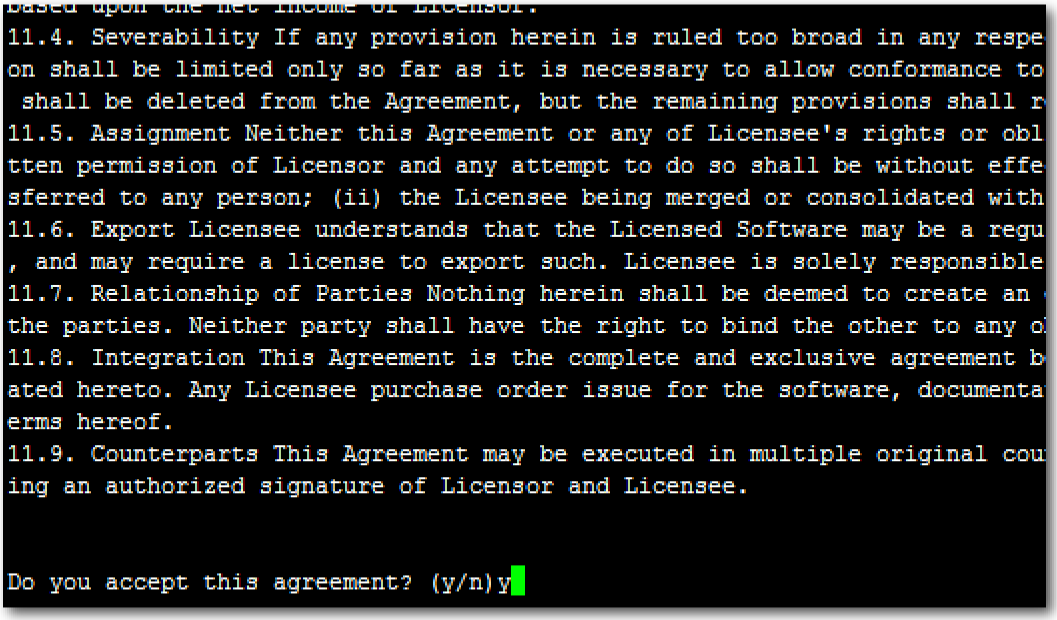
```
cd /mnt/EmsServerInstall
```

7. Run the installation script:

```
./install
```

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

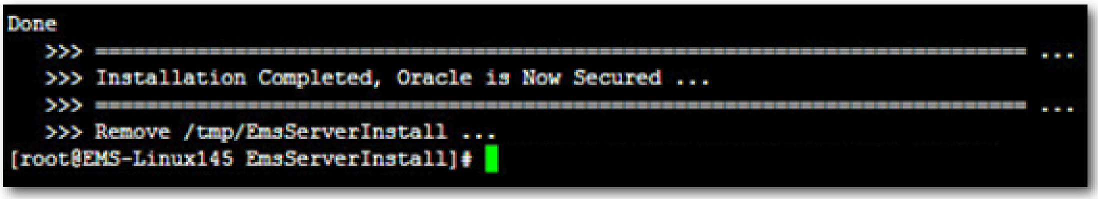
Figure 11-1: OVOC server Upgrade – License Agreement



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


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

9. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:
   - If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 4-9 (inclusive).
   - If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 11-2: OVOC server Installation Complete



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

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

```
su - root
```

13. Type the following command:

```
# EmsServerManager
```

14. Verify that all processes are up and running (see Viewing Process Statuses on page 169) and that you can login to OVOC Web client.

Before Upgrading on Microsoft Azure

This procedure describes the actions required before upgrading to OVOC version 8.0 instance with updated memory requirements.

➢ **Do the following:**

1. Stop your OVOC instance (see Stop the Application on page 182
2. Change Instance type to the following:
   - Low Profile: D8ds_v4
   - High Profile: D16ds_v4
3. Start new OVOC instance.
4. Upgrade OVOC Software to the new OVOC software version as described in Upgrading OVOC Server on Amazon AWS and Microsoft Azure on page 119.

After Upgrading on AWS

This procedure below describes the required actions on AWS following the upgrade to version OVOC Version 8.0.

➢ **Do the following:**

1. Run full OVOC backup (see OVOC Server Backup Processes on page 156
2. Create new AWS instance on m5.4xlarge (High Profile) machine with OVOC Software version 8.0.
3. Restore OVOC data from the backup (see OVOC Server Restore on page 158

⚠ The OVOC version from where the backup is taken must be identical to the OVOC version on which the restore is run.

12 Upgrading OVOC Server on VMware and Microsoft Hyper-V Virtual Machines

This chapter describes how to upgrade the OVOC server on VMware and Microsoft Hyper-V Virtual machines.

- Before proceeding, it is highly recommended to backup the OVOC server files to an external location (OVOC server Backup).
- If you are upgrading from Version 7.2.3000, you can optionally migrate OVOC topology to Version 7.4 and later (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center*).
- Ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8). Failure to meet these requirements will lead to the aborting of the upgrade.
- For obtaining the upgrade file, see OVOC Software Deliverables on page 15
  - ✔ Note that you must verify this file, see Files Verification on page 18
- VMware platform only: If you are installing the Service Provider Cluster mode, a separate upgrade image is provided for each of the following components: Management server, VQM server and PM server. Therefore, you must run the upgrade script separately for each of these images.

The upgrade includes the following steps:

1. Setup the Virtual Machine (Step 1: Setup the Virtual Machine below)
2. Run the upgrade script (Option 1: Standard Upgrade Script on page 135)
3. Connect the OVOC server to the network (Step 3: Connect the OVOC Server to Network on page 144)

Step 1: Setup the Virtual Machine

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

- Setting up VMware Platform for Upgrade below
- Setting Up Microsoft Hyper-V Platform for Upgrade on page 129

Setting up VMware Platform for Upgrade

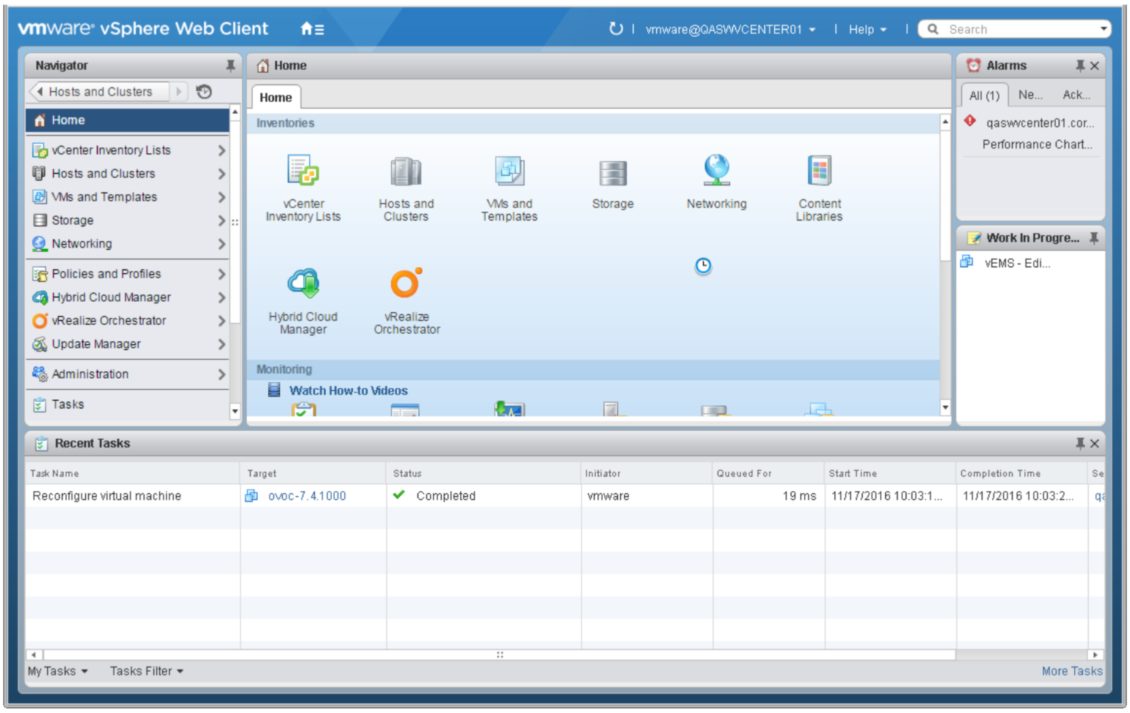
The upgrade on the VMware platform can be run using either the Upgrade media CD/DVD or ISO file using either the VMware Remote Console Application (VMRC) or the VMware Server Host.

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

➢ To setup the VMware machine:

1. Transfer the OVA file containing the VMware Virtual Machine installation package from **DVD3-OVOC server Application Installation** to your PC (see Transferring Files on page 295 for instructions on how to transfer files).
2. Login to the VMware vSphere Web client.

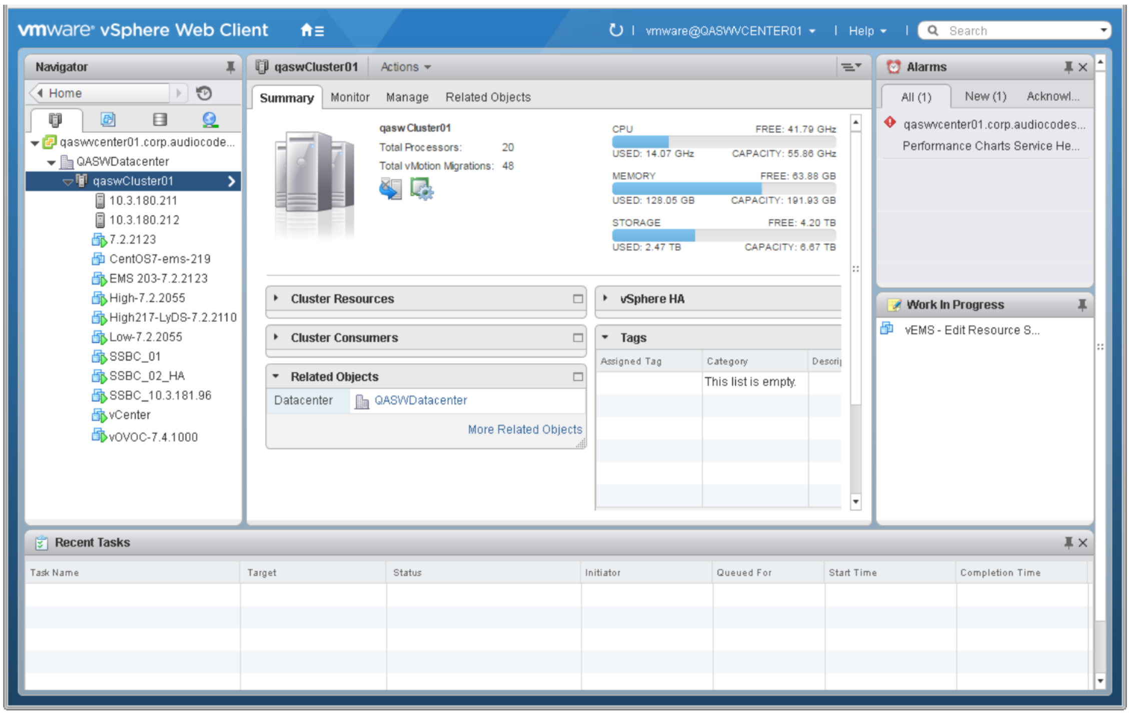
Figure 12-1: VMware vSphere Web Client



Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Se
Reconfigure virtual machine	ovoc-7.4.1000	✓ Completed	vmware	19 ms	11/17/2016 10:03:1...	11/17/2016 10:03:2...	qa

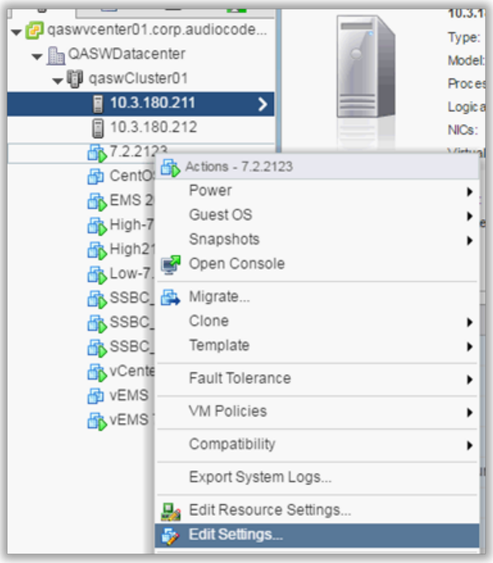
3. In the vCenter Navigator, select **Hosts and Clusters**. A list of Hosts and Clusters is displayed.

Figure 12-2: Hosts and Clusters



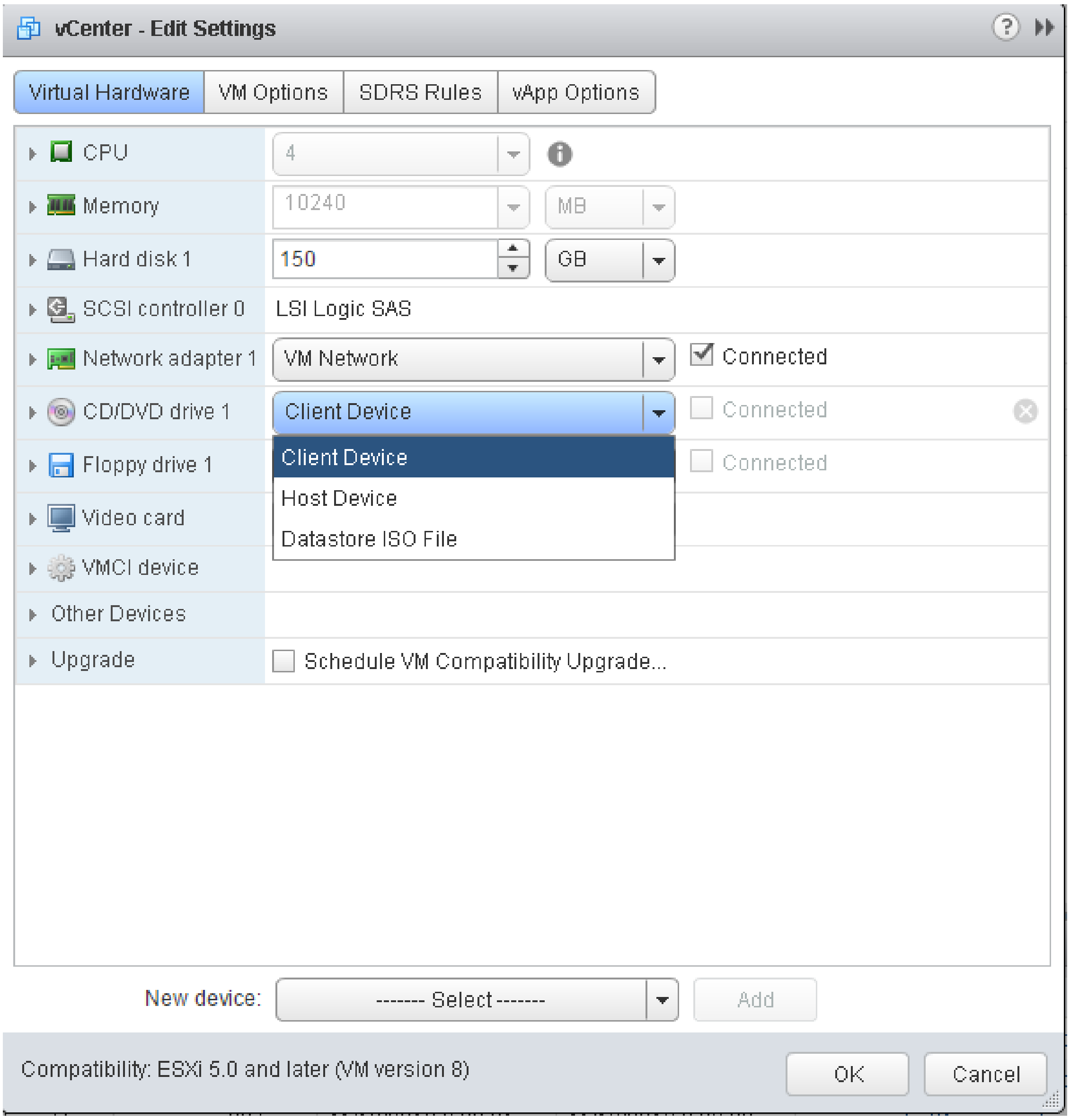
4. Right-click the AudioCodes OVOC node that you wish to upgrade and choose the **Edit Settings** option.

Figure 12-3: Edit Settings Option



The vCenter Edit Settings screen is displayed.

Figure 12-4: Connection Options



vCenter - Edit Settings

Virtual Hardware | VM Options | SDRS Rules | vApp Options

CPU	4		
Memory	10240	MB	
Hard disk 1	150	GB	
SCSI controller 0	LSI Logic SAS		
Network adapter 1	VM Network		☑ Connected
CD/DVD drive 1	Client Device		□ Connected
Floppy drive 1			□ Connected
Video card			
VMCI device			
Other Devices			
Upgrade	□ Schedule VM Compatibility Upgrade...		

New device: ------- Select ------- Add

Compatibility: ESXi 5.0 and later (VM version 8)

5. In the **Virtual Hardware** tab, select the CD/DVD drive item, and from the drop-down list, select the relevant option according to where you placed the Upgrade Media (CD/DVD or ISO image file):

   - **Client Device:** This option enables you to run the upgrade from the PC running the remote console (Setting up Using VMware Remote Console Application (VMRC) on the next page.
   - **Host Device:** This option enables you to run the upgrade from the CD/DVD drive of the VMware server host (Setting up Using VMware Server Host for Upgrade on page 128).
   - **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 (Setting up Using VMware Server Host for Upgrade on page 128).

Setting up Using VMware Remote Console Application (VMRC)

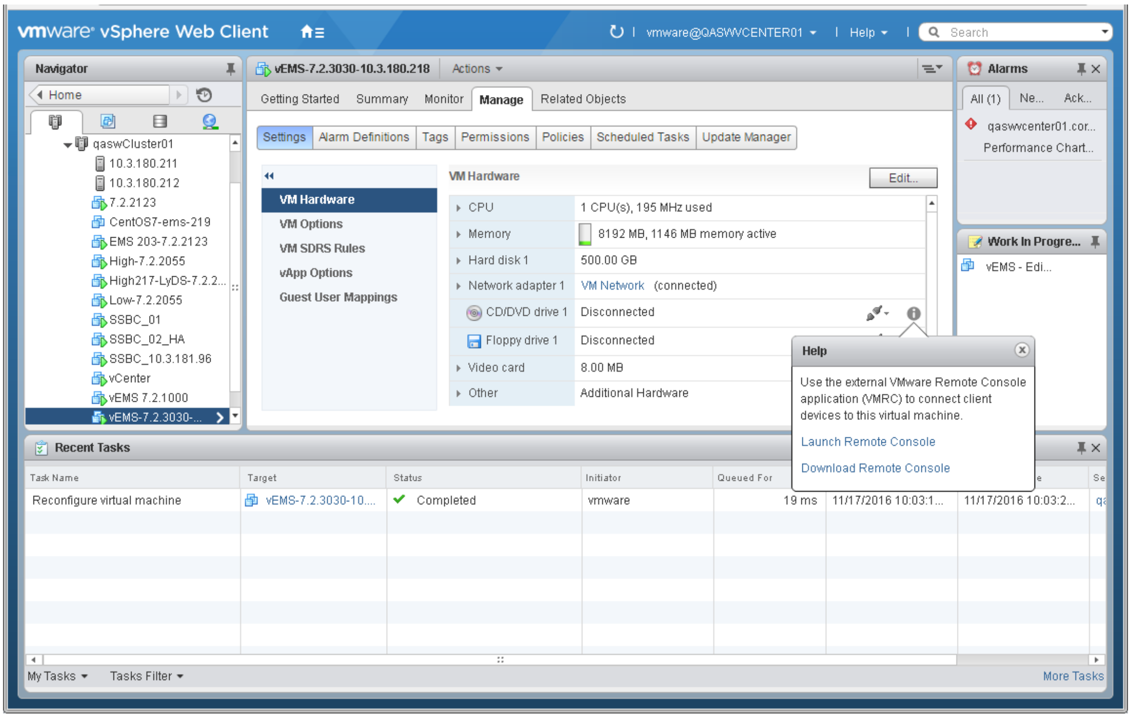
This section describes how to run the upgrade from the VMware host. This procedure requires connecting to the VMware host using the VMware Remote Console application (VMRC).

➢ To run the upgrade using VMRC:

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

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

Figure 12-5: Help Link to Launch Remote Console



VM Hardware

CPU	1 CPU(s), 195 MHz used
Memory	8192 MB, 1146 MB memory active
Hard disk 1	500.00 GB
Network adapter 1	VM Network (connected)
CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	8.00 MB
Other	Additional Hardware

Help

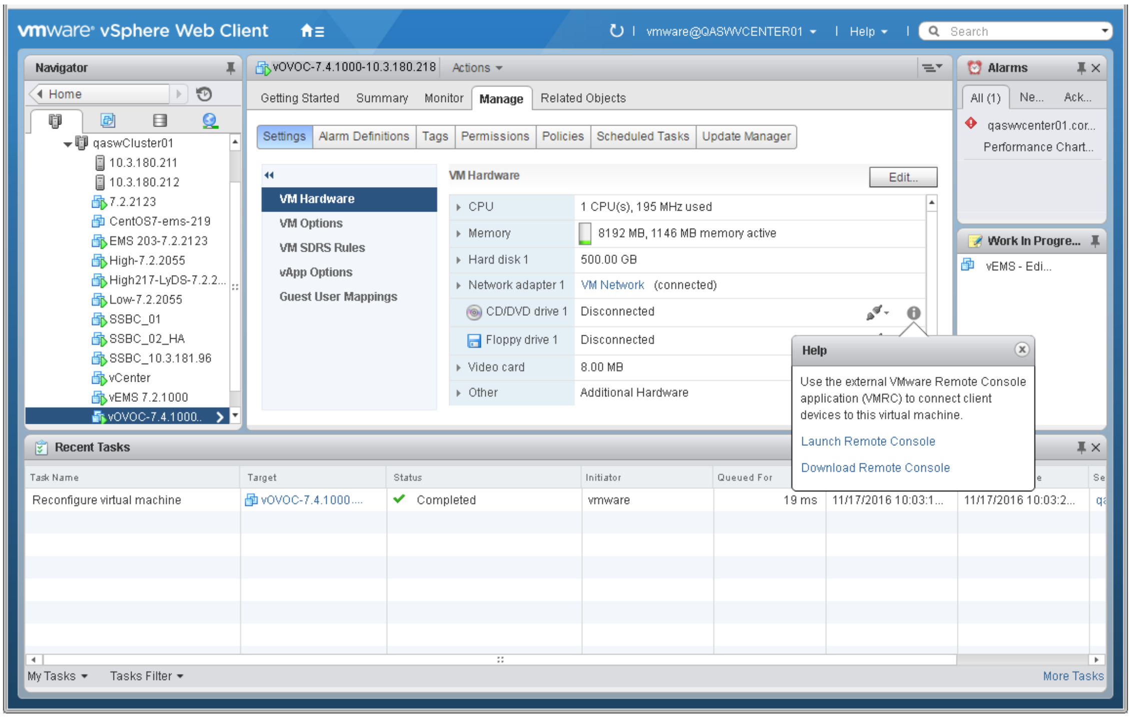
Use the external VMware Remote Console application (VMRC) to connect client devices to this virtual machine.

Launch Remote Console

Download Remote Console

Task Name	Target	Status	Initiator	Queued For		e	Se
Reconfigure virtual machine	vEMS-7.2.3030-10....	✓ Completed	vmware	19 ms	11/17/2016 10:03:1...	11/17/2016 10:03:2...	qa

Figure 12-6: VMware Web Client



VM Hardware

CPU	1 CPU(s), 195 MHz used
Memory	8192 MB, 1146 MB memory active
Hard disk 1	500.00 GB
Network adapter 1	VM Network (connected)
CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	8.00 MB
Other	Additional Hardware

Help

Use the external VMware Remote Console application (VMRC) to connect client devices to this virtual machine.

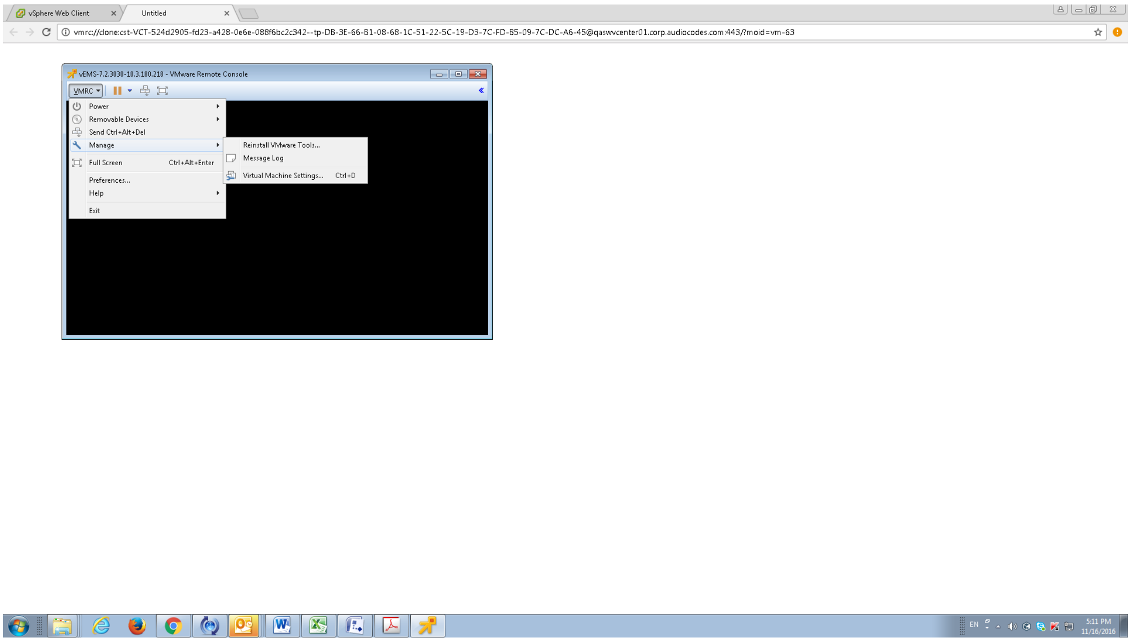
Launch Remote Console

Download Remote Console

Task Name	Target	Status	Initiator	Queued For			Se
Reconfigure virtual machine	vOVOC-7.4.1000....	✓ Completed	vmware	19 ms	11/17/2016 10:03:1...	11/17/2016 10:03:2...	qa

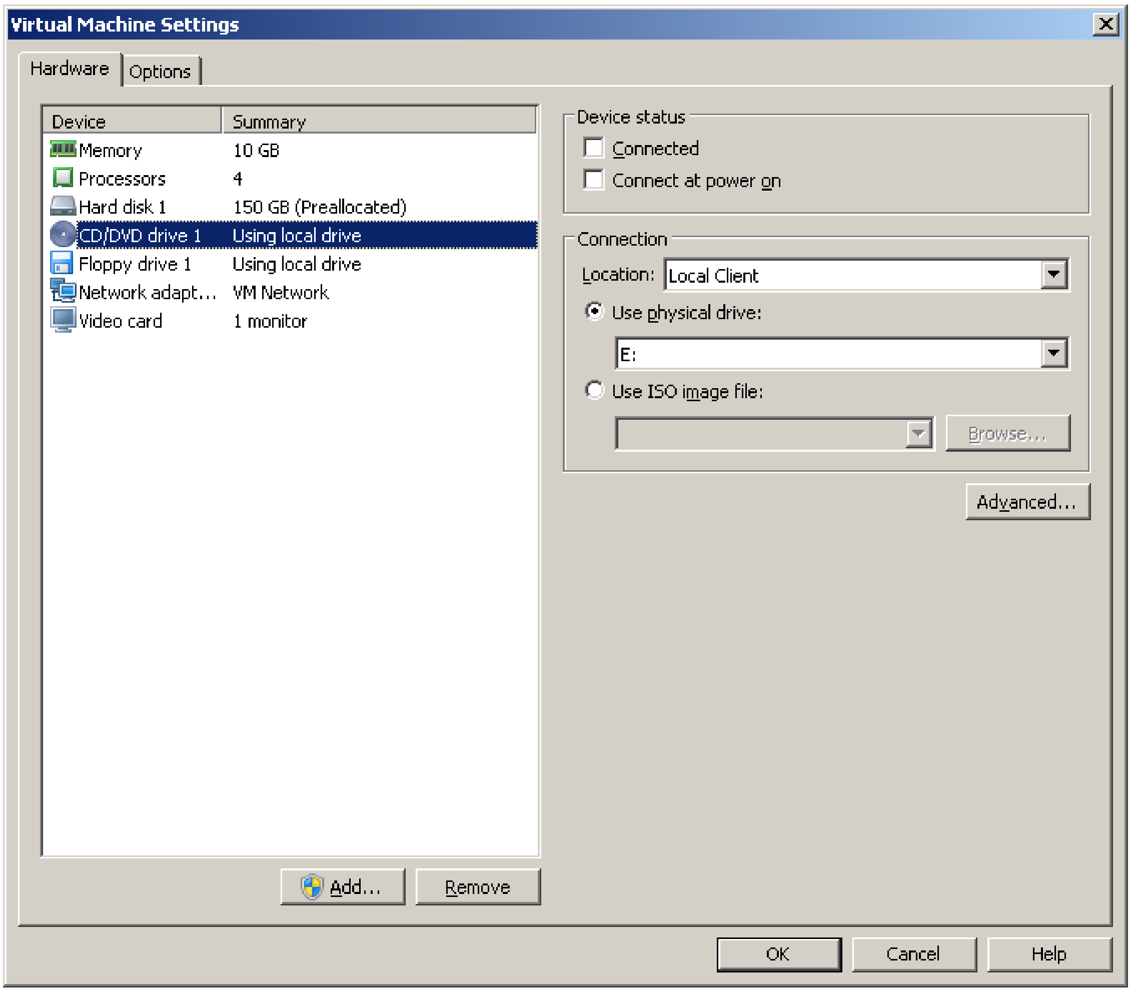
The remote console application is displayed.

Figure 12-7: Remote Console Application


vSphere Web Client
Untitled
vmrc://clone:cst-VCT-524d2905-fd23-a428-0e6e-088f6bc2c342--tp-DB-3E-66-B1-08-68-1C-51-22-5C-19-D3-7C-FD-B5-09-7C-DC-A6-45@qaswvcenter01.corp.audiocodes.com:443/?moid=vm-63
vEMS-7.2.3030-10.3.180.218 - VMware Remote Console
VMRC
Power
Removable Devices
Send Ctrl+Alt+Del
Manage
Full Screen Ctrl+Alt+Enter
Preferences...
Help
Exit
Reinstall VMware Tools...
Message Log
Virtual Machine Settings... Ctrl+D

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

Figure 12-8: Virtual Machine Settings



Device	Summary
Memory	10 GB
Processors	4
Hard disk 1	150 GB (Preallocated)
CD/DVD drive 1	Using local drive
Floppy drive 1	Using local drive
Network adapt...	VM Network
Video card	1 monitor

□ Connected

□ Connect at power on

Location: Local Client

● Use physical drive: E:

○ Use ISO image file:

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**.

Setting up Using VMware Server Host for Upgrade

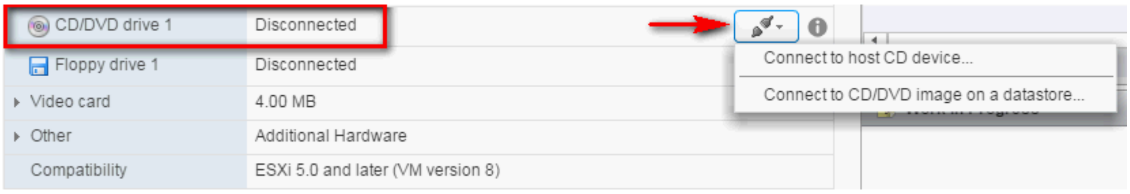
This section describes how to run the upgrade using the VMware server host.

➢ To run the upgrade using the VMware Server host:

1. Select the **Manage** tab, right-click the Connect icon and select one of the following options:

   - Connect to host CD device
   - Connect to CD/DVD image on a datastore

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

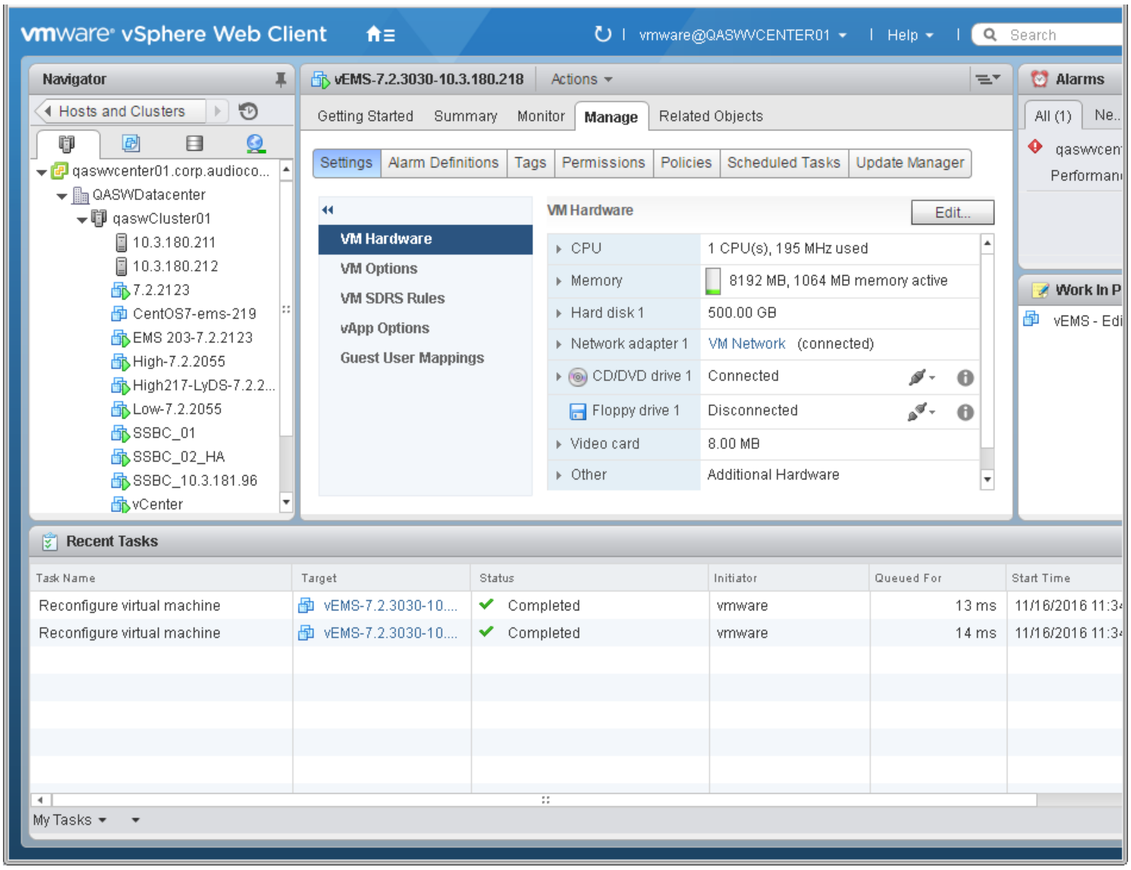


CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	4.00 MB
Other	Additional Hardware
Compatibility	ESXi 5.0 and later (VM version 8)

Connect to host CD device...
Connect to CD/DVD image on a datastore...

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

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



VM Hardware

CPU	1 CPU(s), 195 MHz used
Memory	8192 MB, 1064 MB memory active
Hard disk 1	500.00 GB
Network adapter 1	VM Network (connected)
CD/DVD drive 1	Connected
Floppy drive 1	Disconnected
Video card	8.00 MB
Other	Additional Hardware

Recent Tasks

Task Name	Target	Status	Initiator	Queued For	Start Time
Reconfigure virtual machine	vEMS-7.2.3030-10....	✓ Completed	vmware	13 ms	11/16/2016 11:3
Reconfigure virtual machine	vEMS-7.2.3030-10....	✓ Completed	vmware	14 ms	11/16/2016 11:3

Setting Up Microsoft Hyper-V Platform for Upgrade

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

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

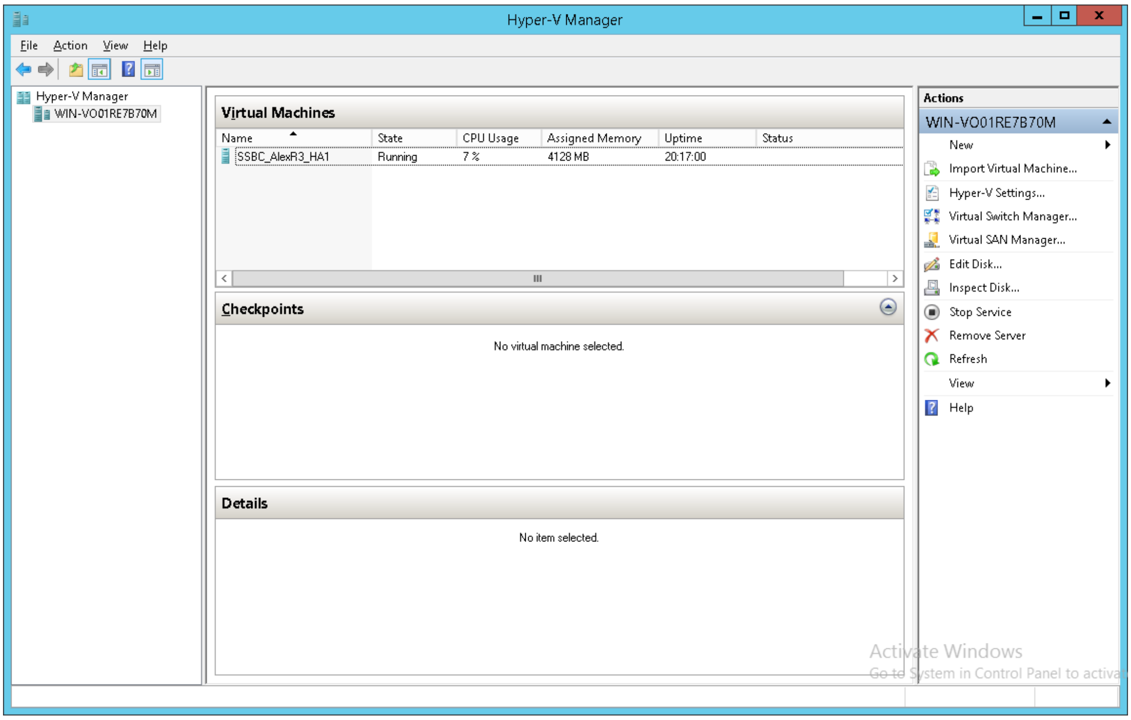
- Upgrade the Virtual Machine (VM) (Installing the Microsoft Hyper-V Virtual Machine).
- Configure the Virtual machine hardware settings (Configuring the Virtual Machine Hardware Settings on page 85).
- Change MAC addresses from 'Dynamic' to 'Static' (Changing MAC Addresses from 'Dynamic' to 'Static' on page 92).

➢ To setup the Microsoft Hyper-V machine:

1. Transfer the ISO file containing the Microsoft Hyper-V Virtual Machine installation package from the AudioCodes **DVD3-OVOC server Application Installation** to your PC (see AppendixTransferring Files on page 295 for instructions on how to transfer files).

2. Open Hyper-V Manager by clicking **Start** > **Administrative Tools** > **Hyper-V Manager**; the following screen opens:

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



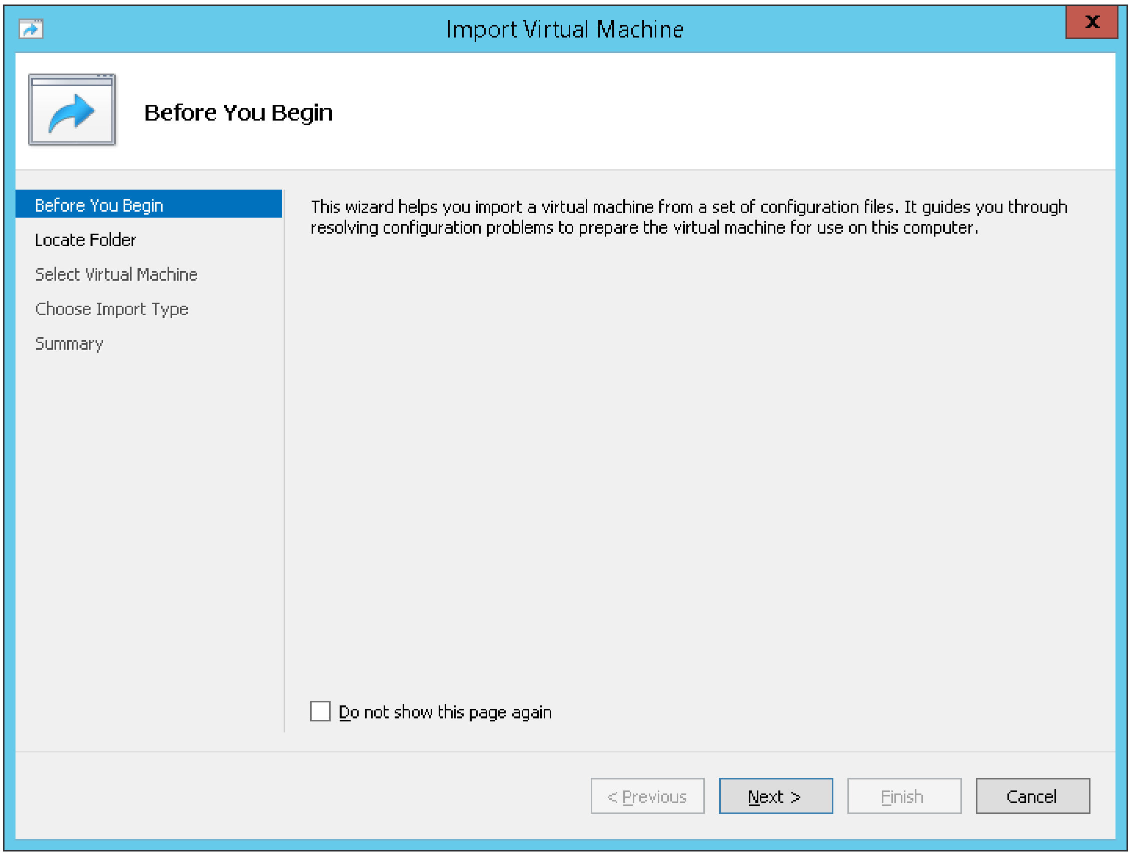
Name	State	CPU Usage	Assigned Memory	Uptime	Status
SSBC_AlexR3_HA1	Running	7 %	4128 MB	20:17:00	

No virtual machine selected.

No item selected.

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

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



Import Virtual Machine

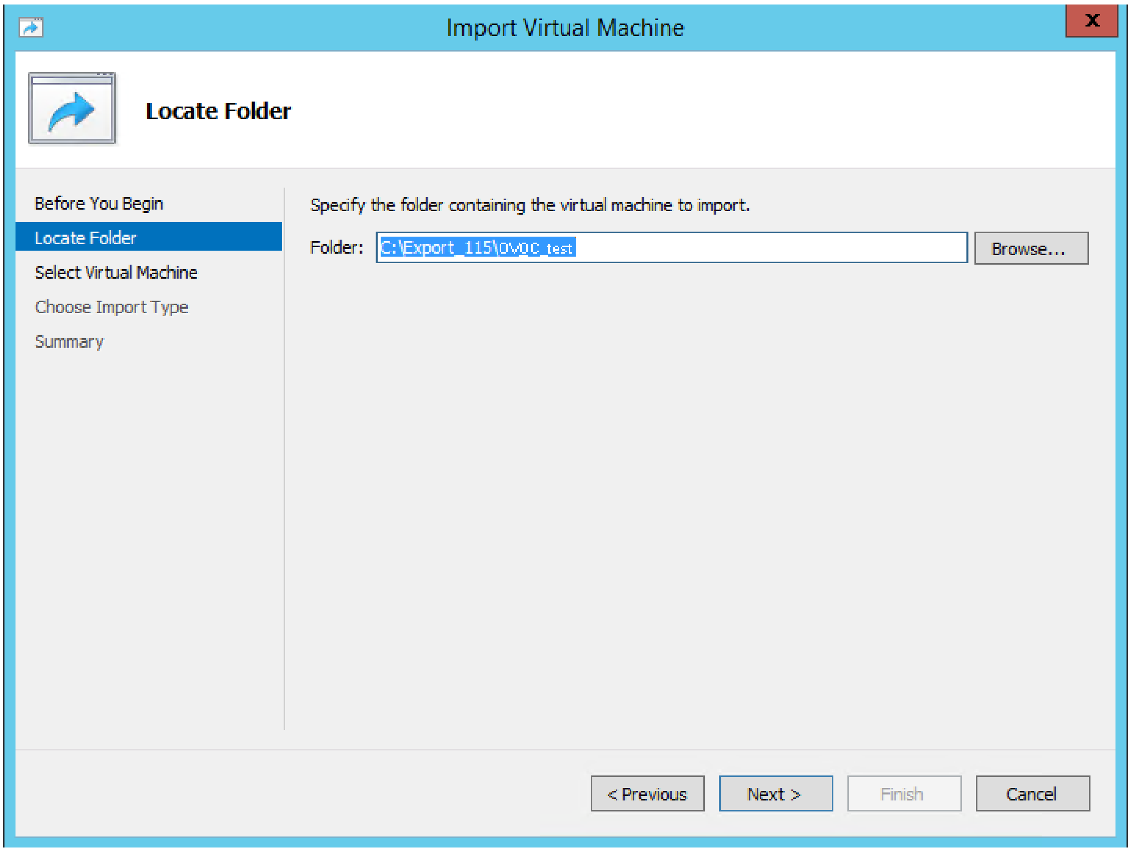
Before You Begin

This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

□ Do not show this page again

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

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



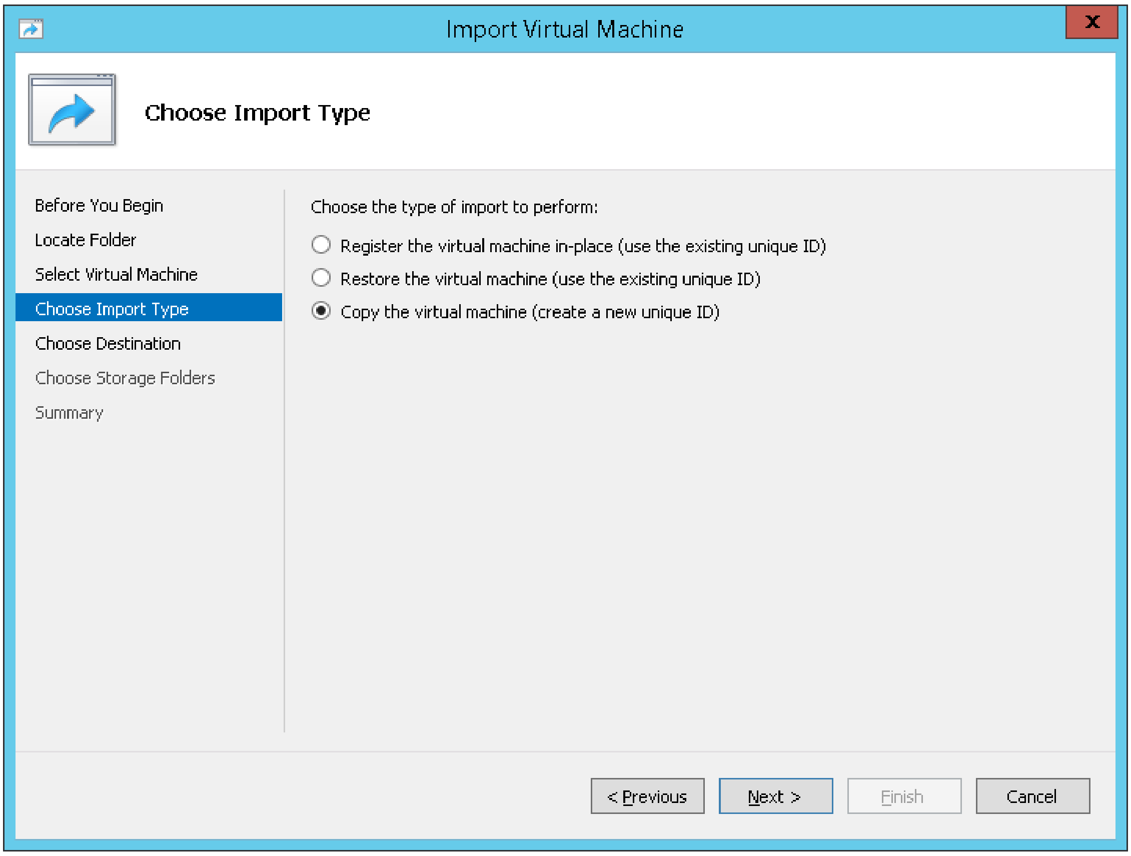
Specify the folder containing the virtual machine to import.

Folder: C:\Export_115\OVOC_test

5. Enter the location of the VM installation folder, which was previously extracted, from the ISO file as shown in the figure above, and then click **Next**; the Select Virtual Machine screen opens.

6. Select the virtual machine to import, and then click **Next**; the Choose Import Type screen opens:

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



Choose the type of import to perform:

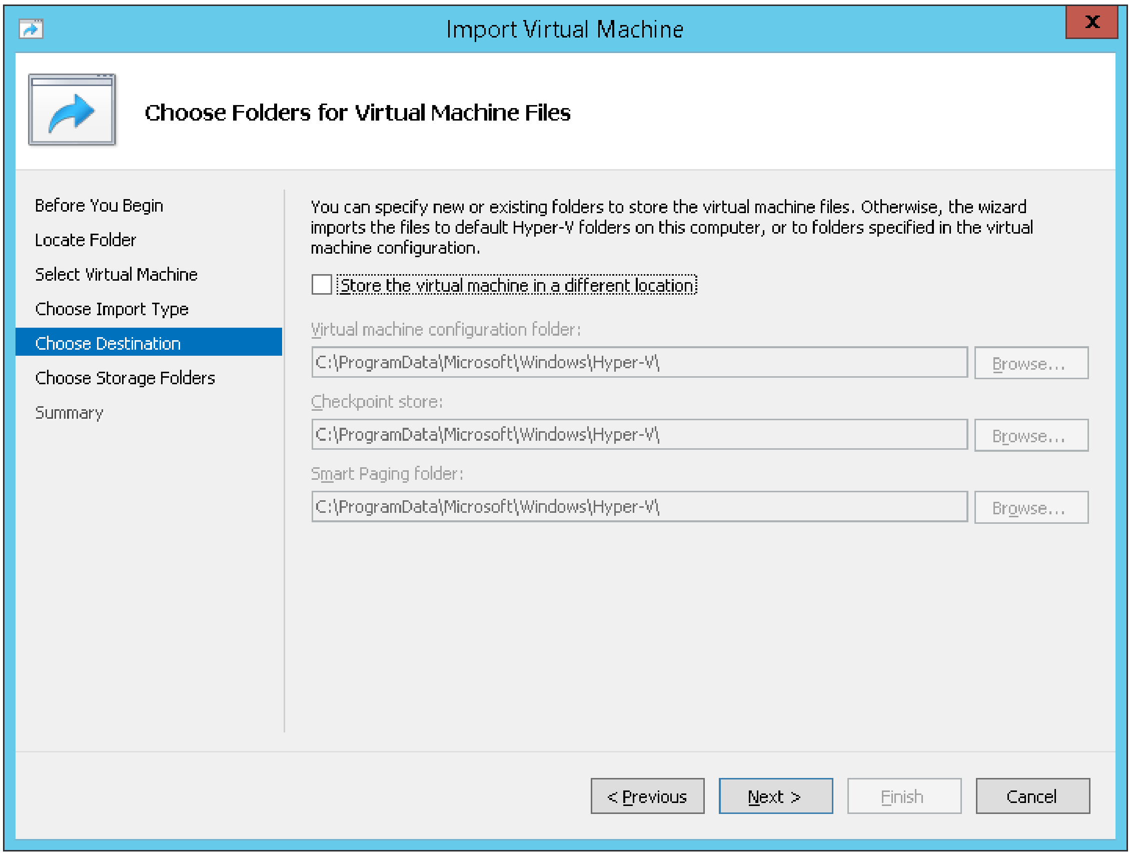
○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

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

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



You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

☐ Store the virtual machine in a different location

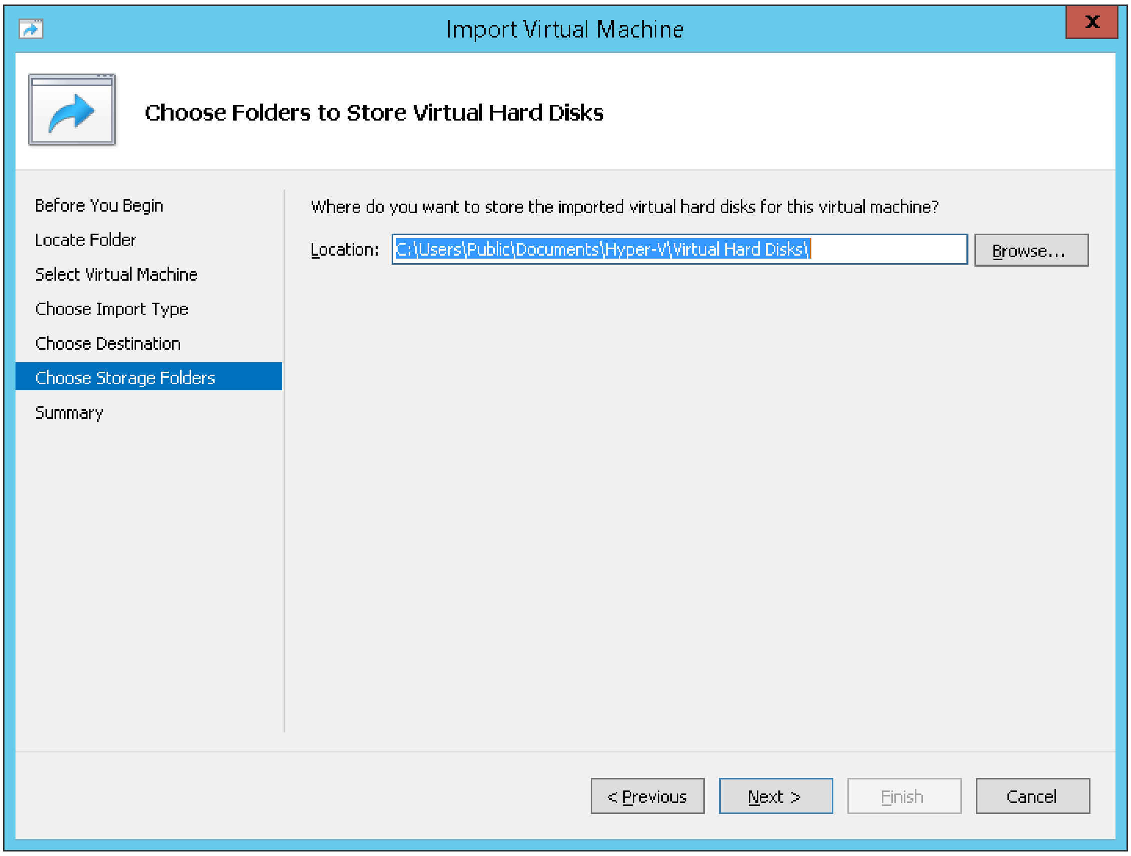
Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Checkpoint store: C:\ProgramData\Microsoft\Windows\Hyper-V\

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

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

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



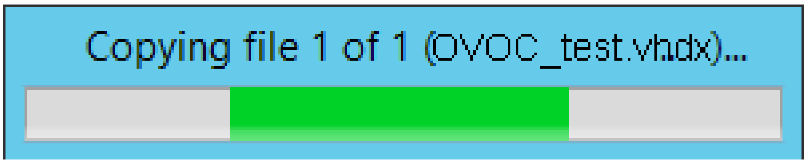
Where do you want to store the imported virtual hard disks for this virtual machine?

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

9. Select the Storage Folder for the Virtual Hard Disk, and then click **Next**; the Summary screen opens.

10. Click **Finish** to start the creation of the VM; a similar installation progress indicator is shown:

Figure 12-17: File Copy Progress Bar



Copying file 1 of 1 (OVOC_test.vhdx)...

This step may take approximately 30 minutes to complete.

Step 2: Run the Server Upgrade Script

This section describes how to run the OVOC server upgrade script:

- Option 1: Standard Upgrade Script below
- Option 2: Service Provider Cluster Upgrade Scripts on page 137

Option 1: Standard Upgrade Script

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

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

➢ To run the OVOC Server upgrade:

1. Using the WinSCP utility (see Transferring Files on page 295), copy the **DVD3** .ISO file that you saved to your PC in Step 1: Setup the Virtual Machine on page 122 to the OVOC server acems user home directory: /home/acems
2. Open an SSH connection or the VM console.
3. Login into the OVOC server as ‘acems’ user with password *acems* (or customer defined password).
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Mount the CDROM to make it available:

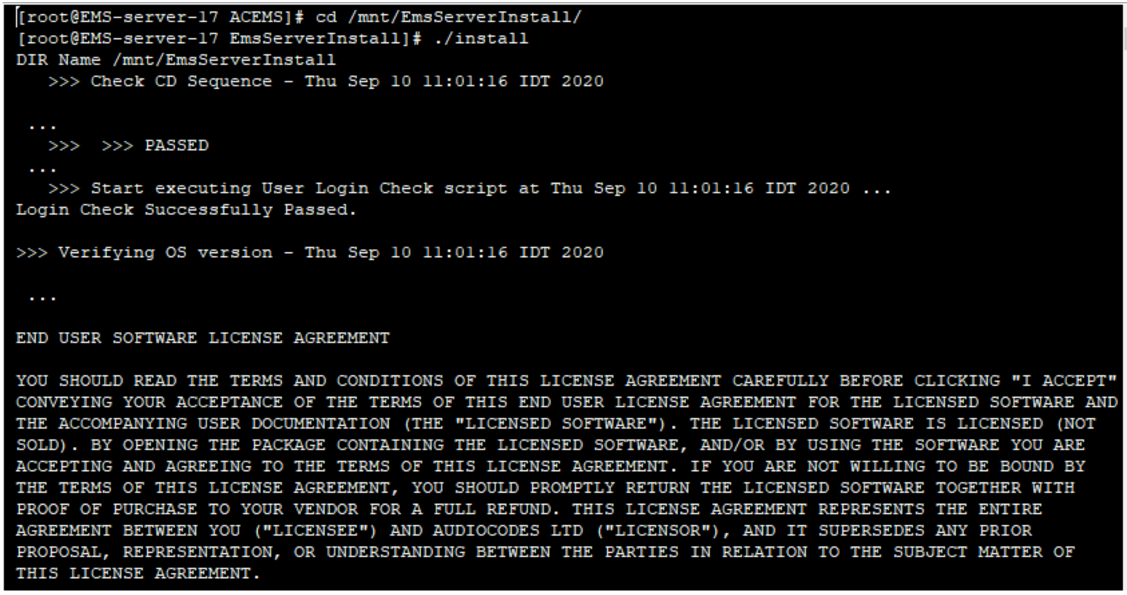
```
mount /home/acems/DVD3_OVOC_ 8.0.110.iso /mnt
```

```
cd /mnt/EmsServerInstall/
```

6. Run the installation script from its location:

```
./install
```

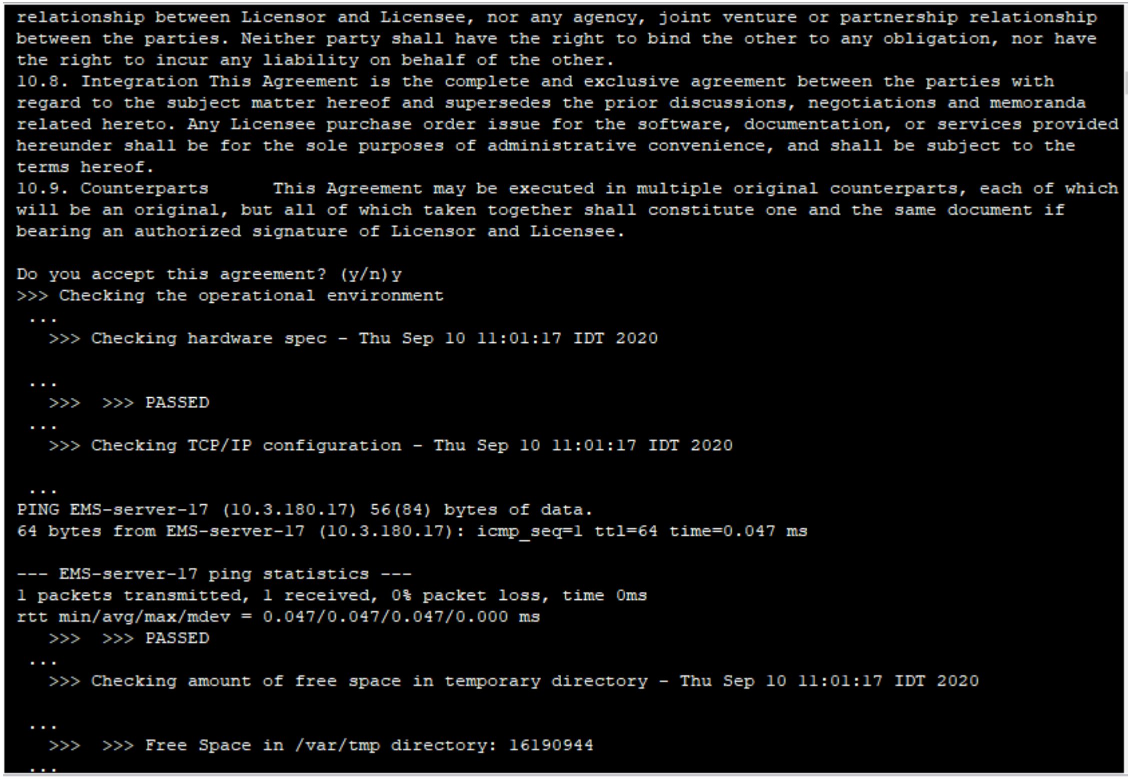
Figure 12-18: OVOC server Installation Script



```
[root@EMS-server-17 ACEMS]# cd /mnt/EmsServerInstall/
[root@EMS-server-17 EmsServerInstall]# ./install
DIR Name /mnt/EmsServerInstall
   >>> Check CD Sequence - Thu Sep 10 11:01:16 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Start executing User Login Check script at Thu Sep 10 11:01:16 IDT 2020 ...
Login Check Successfully Passed.

>>> Verifying OS version - Thu Sep 10 11:01:16 IDT 2020

 ...

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS END USER LICENSE AGREEMENT FOR THE LICENSED SOFTWARE AND
THE ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (NOT
SOLD). BY OPENING THE PACKAGE CONTAINING THE LICENSED SOFTWARE, AND/OR BY USING THE SOFTWARE YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY
THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE LICENSED SOFTWARE TOGETHER WITH
PROOF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE
AGREEMENT BETWEEN YOU ("LICENSEE") AND AUDIOCODES LTD ("LICENSOR"), AND IT SUPERSEDES ANY PRIOR
PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF
THIS LICENSE AGREEMENT.
```

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

Figure 12-19: OVOC server Upgrade – License Agreement



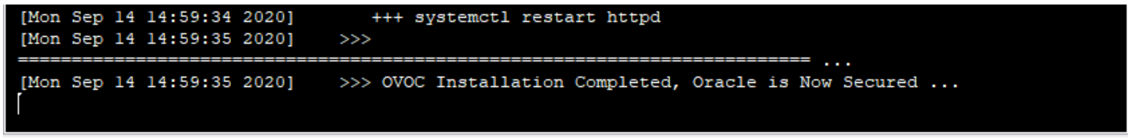
```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```

8. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

   - If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).

   - If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 12-20: OVOC server Installation Complete



```
[Mon Sep 14 14:59:34 2020]      +++ systemctl restart httpd
[Mon Sep 14 14:59:35 2020]    >>>
======================================================================== ...
[Mon Sep 14 14:59:35 2020]    >>> OVOC Installation Completed, Oracle is Now Secured ...
```

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

Option 2: Service Provider Cluster Upgrade Scripts

Once you have setup the virtual machines, you can run the OVOC server upgrade scripts for the Management, VQM and PM servers; a separate script file for each of these cluster nodes is provided on DVD3-OVOC Server Application ISO file. Do the following:

1. Upgrade Management server (see Upgrade Management Server on the next page)

2. Upgrade PM and VQM servers:

   - Upgrade VQM Server on page 140

- Upgrade PM Server on page 142

> - 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.
> - Upgrade the Management server prior to upgrading the VQM and PM servers.

Upgrade Management Server

This section describes how to upgrade the Management server cluster node.

➢ To upgrade the Management Server cluster node:

1. Using the WinSCP utility (see Transferring Files on page 295), copy the **DVD3** .ISO file that you saved to your PC in Step 1: Setup the Virtual Machine on page 122to the OVOC server acems user home directory: /home/acems
2. Open an SSH connection or the VM console.
3. Login into the OVOC server as ‘acems’ user with password *acems* (or customer defined password).
4. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

5. Mount the CDROM to make it available:

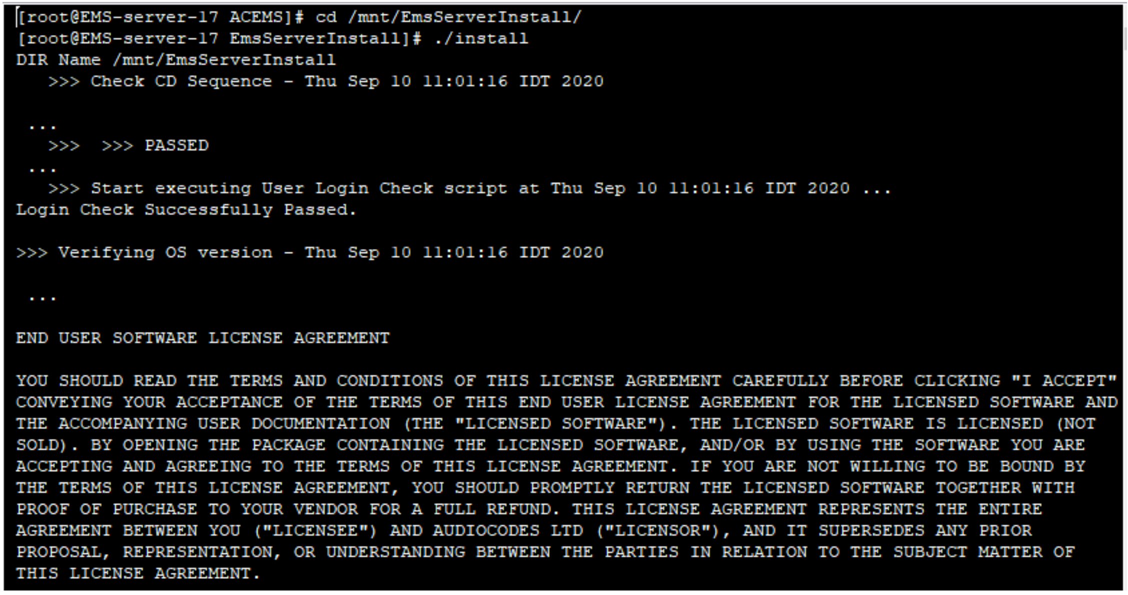
```
mount /home/acems/DVD3_OVOC_ 8.0.110.iso /mnt
```

```
cd /mnt/EmsServerInstall/
```

6. Run the installation script from its location:

```
./install
```

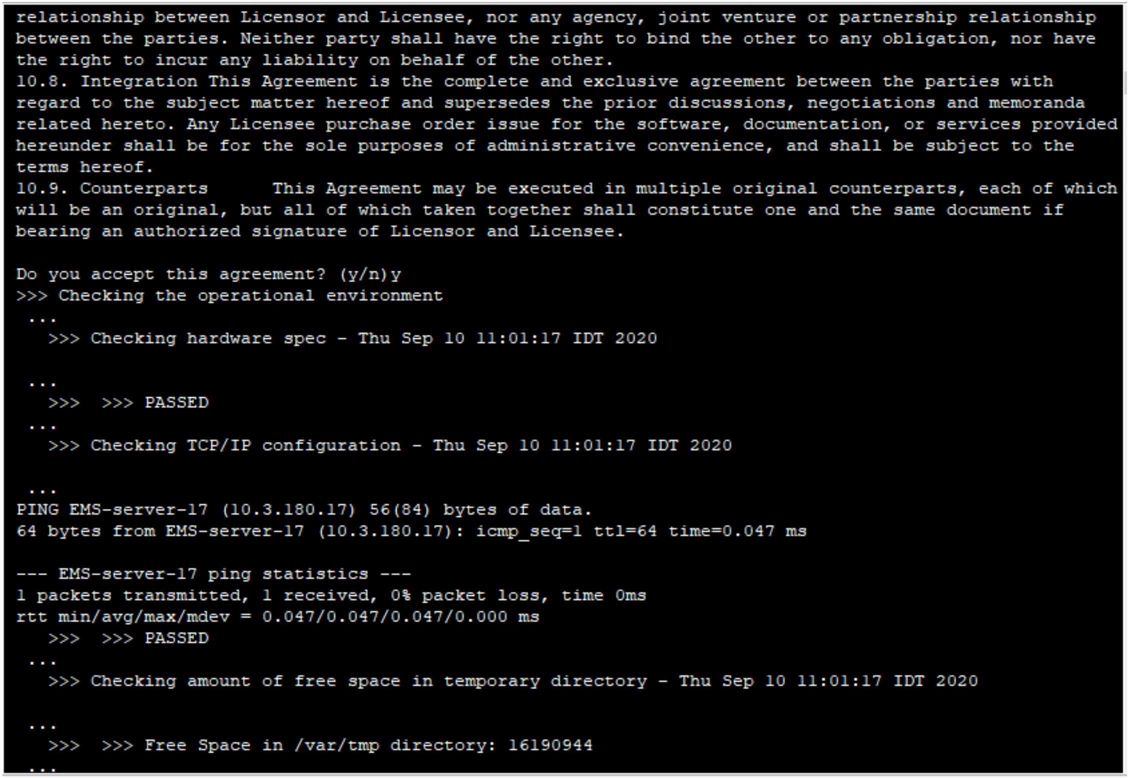
Figure 12-21: OVOC server Installation Script



```
[root@EMS-server-17 ACEMS]# cd /mnt/EmsServerInstall/
[root@EMS-server-17 EmsServerInstall]# ./install
DIR Name /mnt/EmsServerInstall
   >>> Check CD Sequence - Thu Sep 10 11:01:16 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Start executing User Login Check script at Thu Sep 10 11:01:16 IDT 2020 ...
Login Check Successfully Passed.

>>> Verifying OS version - Thu Sep 10 11:01:16 IDT 2020

 ...

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS END USER LICENSE AGREEMENT FOR THE LICENSED SOFTWARE AND
THE ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (NOT
SOLD). BY OPENING THE PACKAGE CONTAINING THE LICENSED SOFTWARE, AND/OR BY USING THE SOFTWARE YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY
THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE LICENSED SOFTWARE TOGETHER WITH
PROOF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE
AGREEMENT BETWEEN YOU ("LICENSEE") AND AUDIOCODES LTD ("LICENSOR"), AND IT SUPERSEDES ANY PRIOR
PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF
THIS LICENSE AGREEMENT.
```

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

Figure 12-22: OVOC server Upgrade – License Agreement



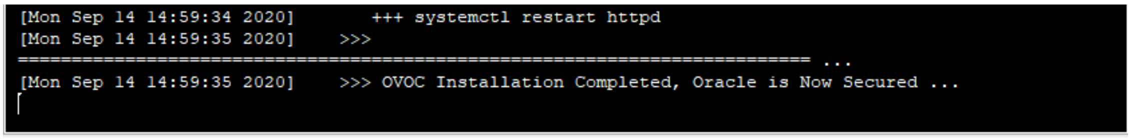
```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```

8. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

- If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).

- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 12-23: OVOC server Installation Complete



```
[Mon Sep 14 14:59:34 2020]        +++ systemctl restart httpd
[Mon Sep 14 14:59:35 2020]     >>>
========================================================================= ...
[Mon Sep 14 14:59:35 2020]     >>> OVOC Installation Completed, Oracle is Now Secured ...
```

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

Upgrade VQM Server

Once you have setup the virtual machines and installed the Management Server (see), you can run the **VQM** server upgrade script.

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

➢ To upgrade VQM server:

1. Using the WinSCP utility (see Transferring Files on page 295), copy the **DVD3** .ISO file containing the VQM server installation that you saved to your PC inStep 1: Setup the Virtual Machine on page 122 to the OVOC server acems user home directory: /home/acems

2. Open an SSH connection or the VM console.

3. Login into the OVOC server as ‘acems’ user with password *acems* (or customer defined password).

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

```
su - root
```

5. Mount the CDROM to make it available:

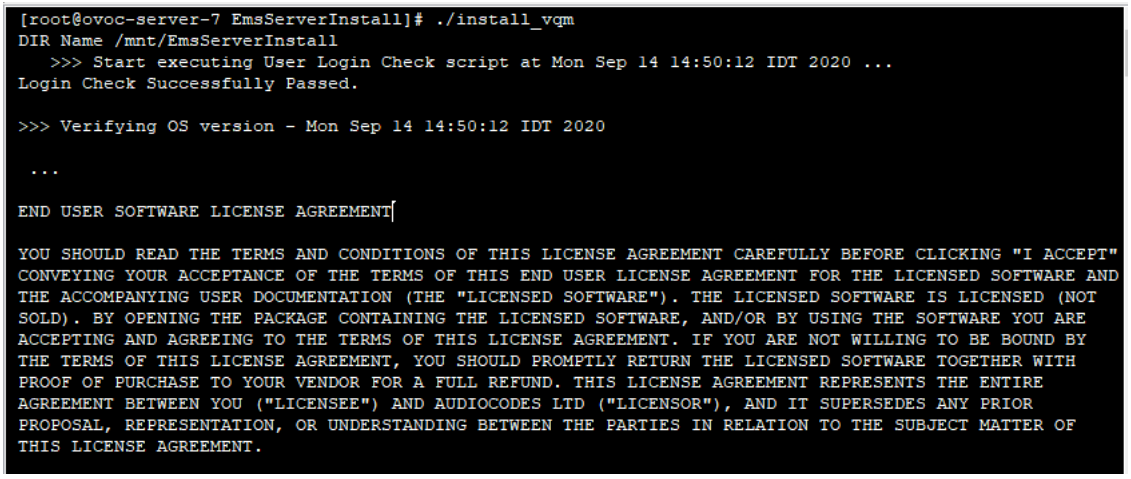
```
mount /home/acems/DVD3_OVOC_ 8.0.110.iso /mnt
```

```
cd /mnt/EmsServerInstall/
```

6. Run the installation script from its location:

```
./install_vqm
```

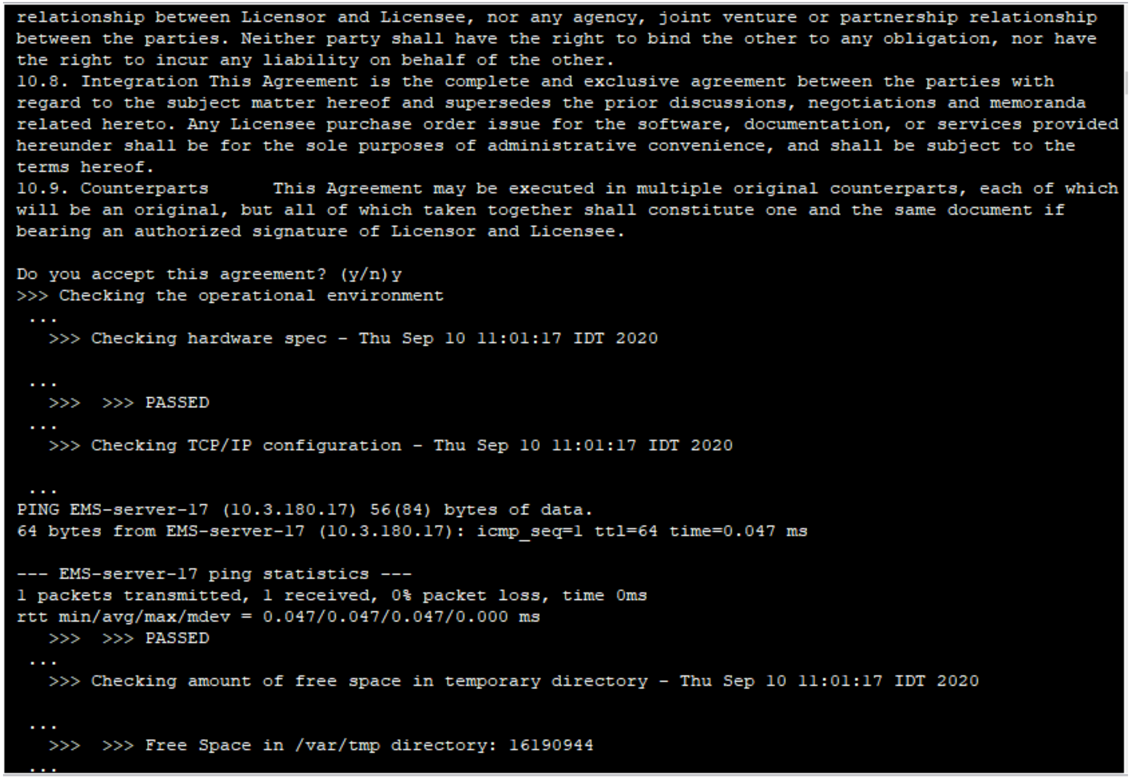
Figure 12-24: OVOC server Installation Script



```
[root@ovoc-server-7 EmsServerInstall]# ./install_vqm
DIR Name /mnt/EmsServerInstall
   >>> Start executing User Login Check script at Mon Sep 14 14:50:12 IDT 2020 ...
Login Check Successfully Passed.

>>> Verifying OS version - Mon Sep 14 14:50:12 IDT 2020

 ...

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS END USER LICENSE AGREEMENT FOR THE LICENSED SOFTWARE AND
THE ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (NOT
SOLD). BY OPENING THE PACKAGE CONTAINING THE LICENSED SOFTWARE, AND/OR BY USING THE SOFTWARE YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY
THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE LICENSED SOFTWARE TOGETHER WITH
PROOF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE
AGREEMENT BETWEEN YOU ("LICENSEE") AND AUDIOCODES LTD ("LICENSOR"), AND IT SUPERSEDES ANY PRIOR
PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF
THIS LICENSE AGREEMENT.
```

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

Figure 12-25: OVOC server Upgrade – License Agreement

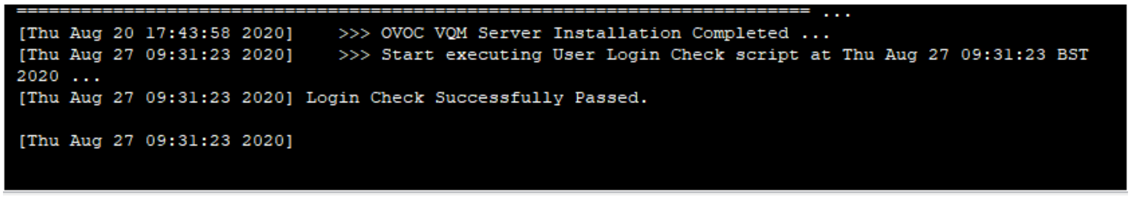


```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```

8. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

   - If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).
   - If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. on the next page

Figure 12-26: OVOC server Installation Complete



```
=========================================================================== ...
[Thu Aug 20 17:43:58 2020]    >>> OVOC VQM Server Installation Completed ...
[Thu Aug 27 09:31:23 2020]    >>> Start executing User Login Check script at Thu Aug 27 09:31:23 BST
2020 ...
[Thu Aug 27 09:31:23 2020] Login Check Successfully Passed.

[Thu Aug 27 09:31:23 2020]
```

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

Upgrade PM Server

Once you have setup the virtual machines and installed the Management Server (see Step 2: Run the OVOC Server Upgrade Script), you can run the **PM** server upgrade script.

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

➢ To run the PM server upgrade:

1. Using the WinSCP utility(see Transferring Files on page 295), copy the **DVD3** .ISO file containing the VQM server installation that you saved to your PC in Step 1: Setup the Virtual Machine on page 122 to the OVOC server acems user home directory: /home/acems.

2. Open an SSH connection or the VM console.

3. Login into the OVOC server as ‘acems’ user with password *acems* (or customer defined password).

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

```
su - root
```

5. Mount the CDROM to make it available:

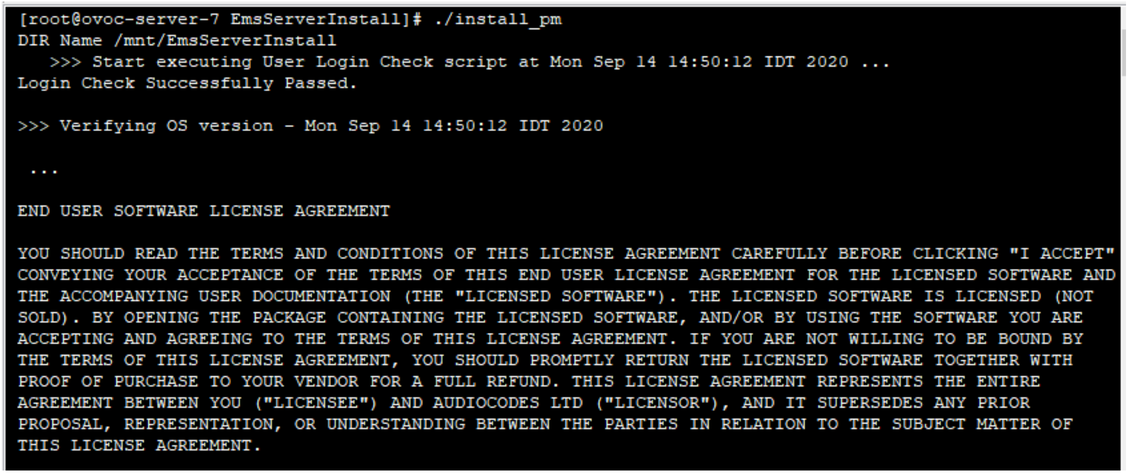
```
mount /home/acems/DVD3_OVOC_ 8.0.110.iso /mnt
```

```
cd /mnt/EmsServerInstall/
```

6. Run the installation script from its location:

```
./install_pm
```

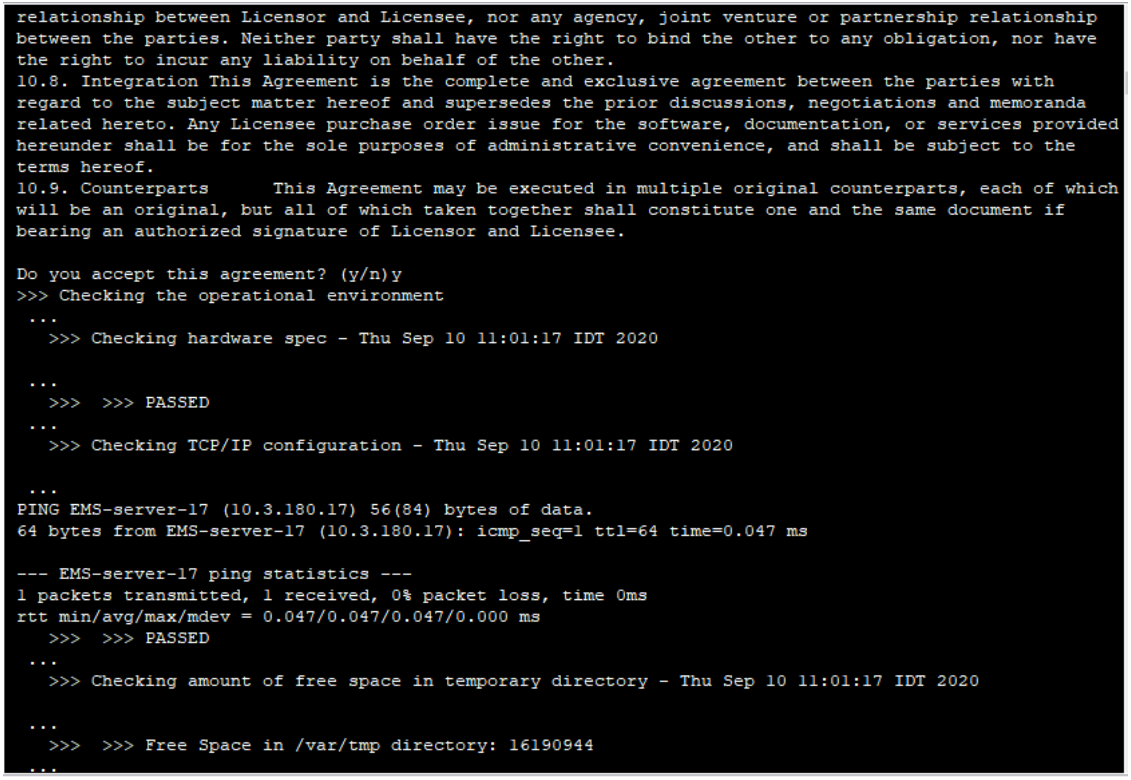
Figure 12-27: OVOC server Installation Script



```
[root@ovoc-server-7 EmsServerInstall]# ./install_pm
DIR Name /mnt/EmsServerInstall
   >>> Start executing User Login Check script at Mon Sep 14 14:50:12 IDT 2020 ...
Login Check Successfully Passed.

>>> Verifying OS version - Mon Sep 14 14:50:12 IDT 2020

 ...

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CLICKING "I ACCEPT"
CONVEYING YOUR ACCEPTANCE OF THE TERMS OF THIS END USER LICENSE AGREEMENT FOR THE LICENSED SOFTWARE AND
THE ACCOMPANYING USER DOCUMENTATION (THE "LICENSED SOFTWARE"). THE LICENSED SOFTWARE IS LICENSED (NOT
SOLD). BY OPENING THE PACKAGE CONTAINING THE LICENSED SOFTWARE, AND/OR BY USING THE SOFTWARE YOU ARE
ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY
THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE LICENSED SOFTWARE TOGETHER WITH
PROOF OF PURCHASE TO YOUR VENDOR FOR A FULL REFUND. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE
AGREEMENT BETWEEN YOU ("LICENSEE") AND AUDIOCODES LTD ("LICENSOR"), AND IT SUPERSEDES ANY PRIOR
PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES IN RELATION TO THE SUBJECT MATTER OF
THIS LICENSE AGREEMENT.
```

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

Figure 12-28: OVOC server Upgrade – License Agreement

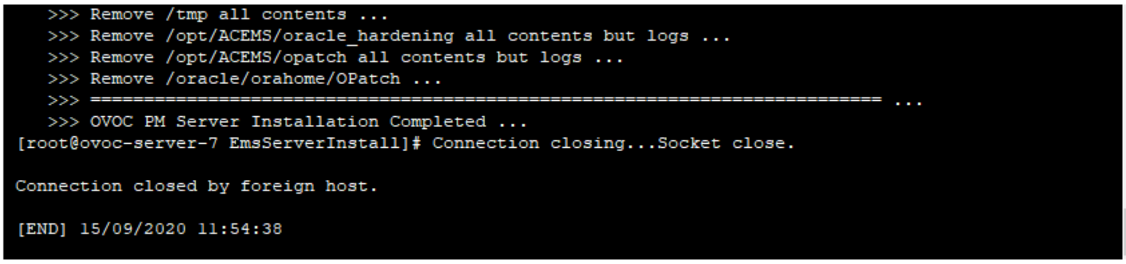


```
relationship between Licensor and Licensee, nor any agency, joint venture or partnership relationship
between the parties. Neither party shall have the right to bind the other to any obligation, nor have
the right to incur any liability on behalf of the other.
10.8. Integration This Agreement is the complete and exclusive agreement between the parties with
regard to the subject matter hereof and supersedes the prior discussions, negotiations and memoranda
related hereto. Any Licensee purchase order issue for the software, documentation, or services provided
hereunder shall be for the sole purposes of administrative convenience, and shall be subject to the
terms hereof.
10.9. Counterparts      This Agreement may be executed in multiple original counterparts, each of which
will be an original, but all of which taken together shall constitute one and the same document if
bearing an authorized signature of Licensor and Licensee.

Do you accept this agreement? (y/n)y
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> PASSED
 ...
   >>> Checking TCP/IP configuration - Thu Sep 10 11:01:17 IDT 2020

 ...
PING EMS-server-17 (10.3.180.17) 56(84) bytes of data.
64 bytes from EMS-server-17 (10.3.180.17): icmp_seq=1 ttl=64 time=0.047 ms

--- EMS-server-17 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.047/0.047/0.047/0.000 ms
   >>>  >>> PASSED
 ...
   >>> Checking amount of free space in temporary directory - Thu Sep 10 11:01:17 IDT 2020

 ...
   >>>  >>> Free Space in /var/tmp directory: 16190944
 ...
```

8. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

   - If you are prompted to reboot, press Enter to reboot the OVOC server and then repeat steps 2-7 (inclusive).
   - If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. on the next page

Figure 12-29: OVOC server Installation Complete



```
   >>> Remove /tmp all contents ...
   >>> Remove /opt/ACEMS/oracle_hardening all contents but logs ...
   >>> Remove /opt/ACEMS/opatch all contents but logs ...
   >>> Remove /oracle/orahome/OPatch ...
   >>> ========================================================================== ...
   >>> OVOC PM Server Installation Completed ...
[root@ovoc-server-7 EmsServerInstall]# Connection closing...Socket close.

Connection closed by foreign host.

[END] 15/09/2020 11:54:38
```

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

Step 3: Connect the OVOC Server to Network

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

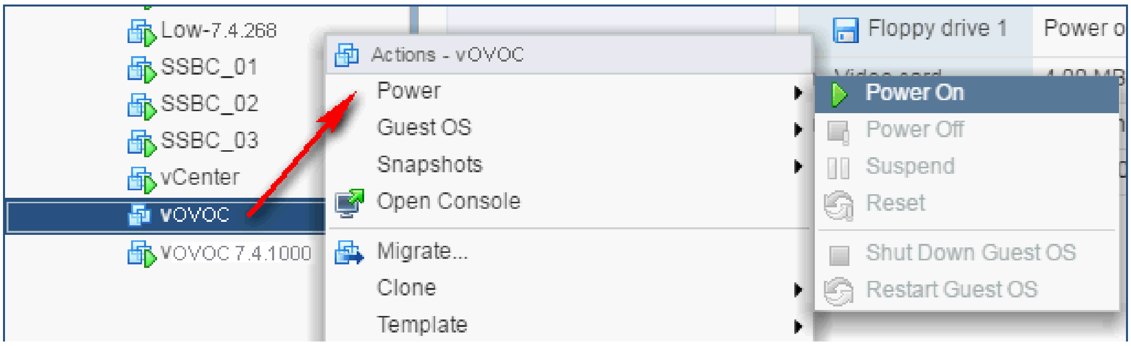
Connecting to OVOC Server on VMware

This section describes how to connect to the OVOC server using the VMware vCenter.

➢ **To connect the OVOC server:**

1. Power on the machine; in the vCenter tree, right-click the AudioCodes One Voice Operations Center node (vOC) and in the drop-down menu, choose **Power** > **Power On**. Upon the initial boot up after reconfiguring the disk space, the internal mechanism configures the server installation accordingly to version specifications (Hardware and Software Specifications on page 8).

Figure 12-30: Power On



2. Wait until the boot process has completed, and then connect the running server through the vSphere client console.

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

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

```
su - root
```

5. Type the following command:

```
# EmsServerManager
```

6. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify login to OVOC Web client is successful.

7. If you are installing the Service Provider Cluster mode, see Service Provider Cluster on page 188

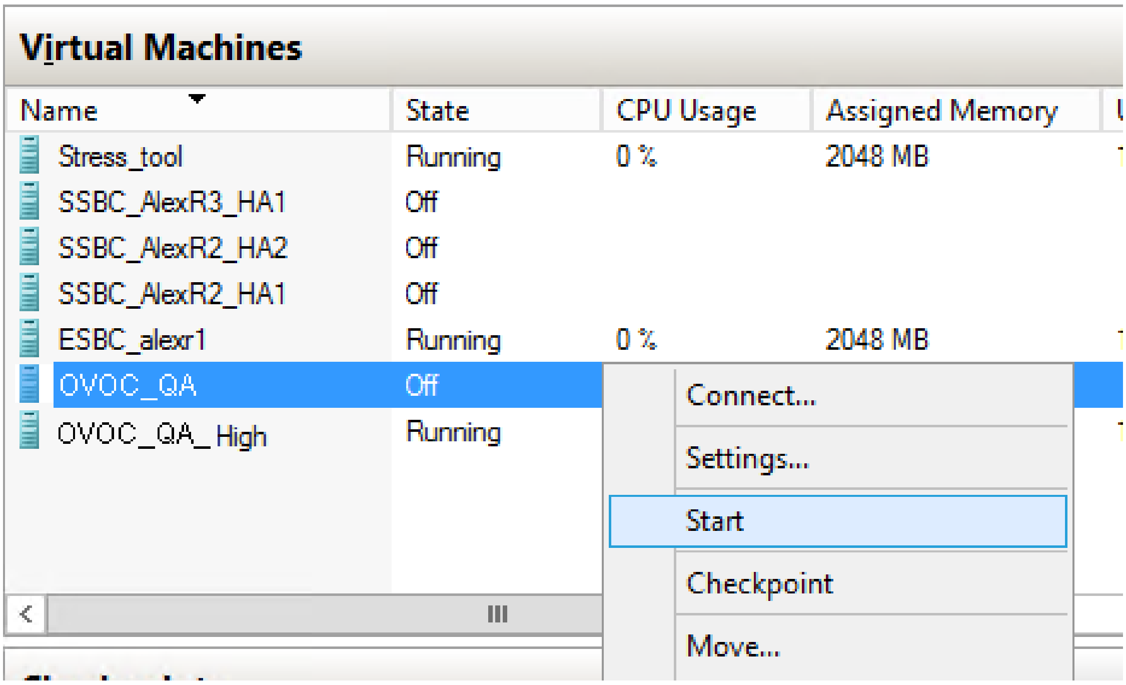
Connecting to OVOC Server on Hyper-V

This section describes how to connect to the OVOC server on the Hyper-V platform.

➢ To connect to the OVOC server:

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

Figure 12-31: Power On Virtual Machine

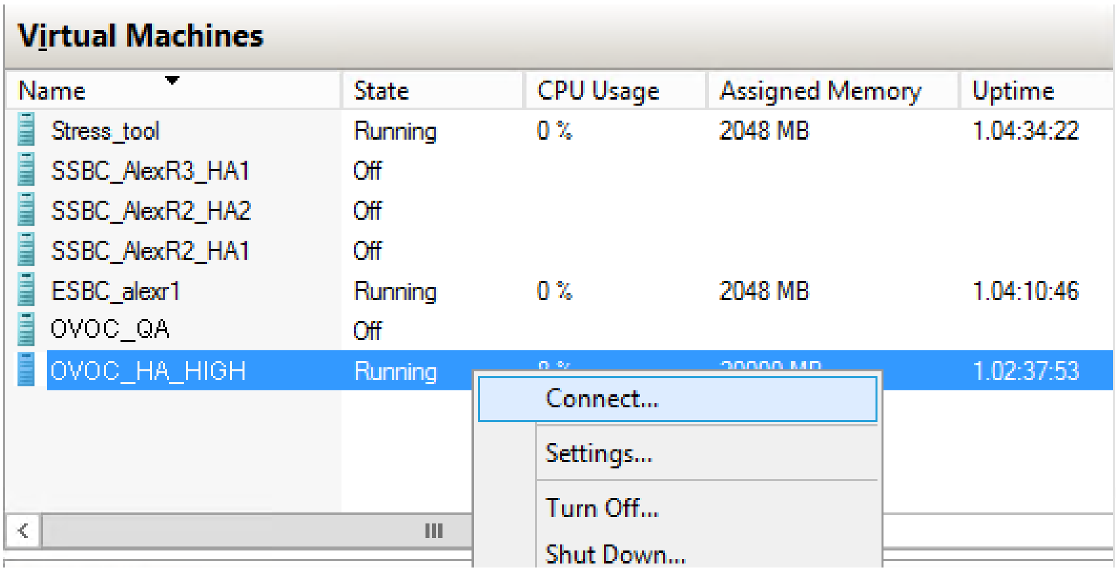


Virtual Machines

Name	State	CPU Usage	Assigned Memory
Stress_tool	Running	0 %	2048 MB
SSBC_AlexR3_HA1	Off		
SSBC_AlexR2_HA2	Off		
SSBC_AlexR2_HA1	Off		
ESBC_alexr1	Running	0 %	2048 MB
OVOC_QA	Off		
OVOC_QA_High	Running		

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

Figure 12-32: 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 %	20000 MB	1.02:37:53

3. Login into the OVOC server by SSH, as ‘acems’ user and enter password *acems*.

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

```
su - root
```

5. Type the following command:

```
# EmsServerManager
```

6. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify login to OVOC Web client is successful.

13 Upgrading OVOC Server on Dedicated Hardware

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

- Before proceeding, it is highly recommended to backup the OVOC server files to an external location (OVOC server Backup).
- If you are upgrading from Version 7.2.3000, you can optionally migrate topology to Version 7.4 and later (see document *Migration from EMS and SEM Version 7.2.3000 to One Voice Operations Center*).
- Before proceeding, ensure that the minimum platform requirements are met (see Hardware and Software Specifications on page 8). Failure to meet these requirements will lead to the aborting of the upgrade.
- Upgrade of OVOC Version 7.8 and later must be performed on HP DL Gen10 machines. Upgrade on HP DL G8 machines is not supported.
- For obtaining the upgrade file, see OVOC Software Deliverables on page 15
  - ✔ Note that you must verify this file, see Files Verification on page 18

Upgrading the OVOC Server-DVD

This section describes how to upgrade the OVOC server from the AudioCodes supplied installation DVD. To upgrade the OVOC server, only **DVD3** is required (see OVOC Software Deliverables on page 15). Verify in the OVOC Manager 'General Info' screen that you have installed the latest Linux revision (seeHardware and Software Specifications on page 8). If you have an older OS revision, a clean installation must be performed using all three DVDs (see Installing the OVOC server on Dedicated Hardware).

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

➢ To upgrade the OVOC server:

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

```
su - root
```

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

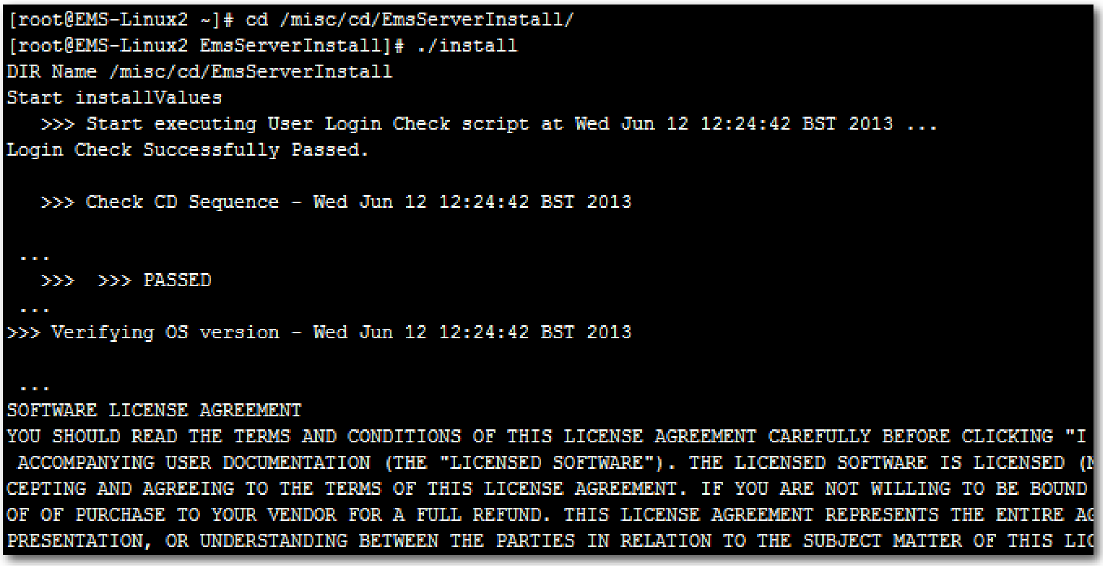
```
mount /home/acems/DVD3_OVOC_/mnt
```

5. Run the installation script from its location:

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

```
./install
```

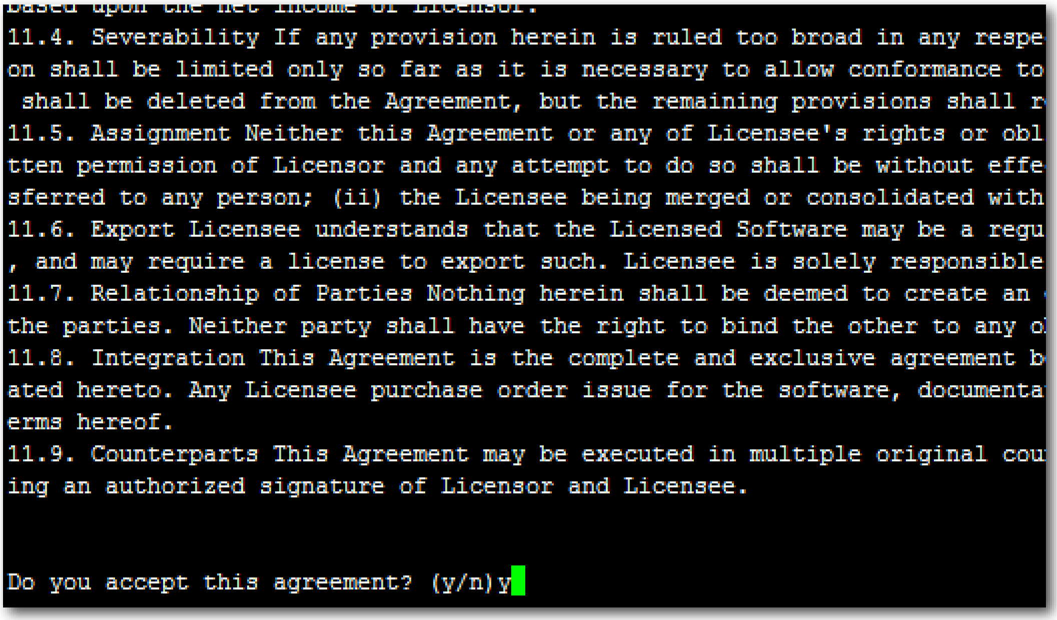
Figure 13-1: OVOC server Upgrade



```
[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 (
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 13-2: OVOC server Upgrade – License Agreement

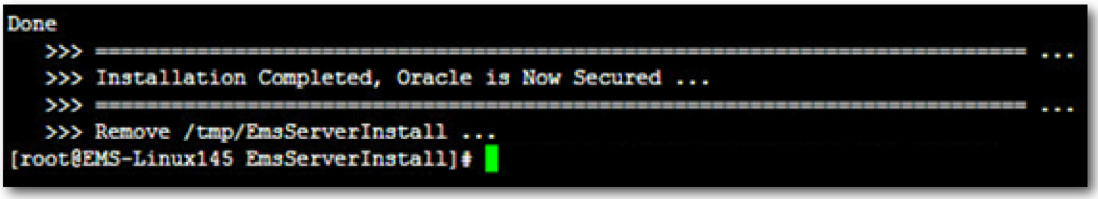


```
based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
 shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement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


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

7. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:
   - If you are prompted to reboot, press Enter to reboot the OVOC server, and then repeat steps 2-7 (inclusive).

- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below

Figure 13-3: OVOC server Installation Complete



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

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

```
su - root
```

11. Type the following command:

```
# EmsServerManager
```

12. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify that login to OVOC Web client is successful.

Upgrading the OVOC Server using an ISO File

This section describes how to upgrade the OVOC server using an ISO file.

➢ 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. Using WinSCP utility (see Transferring Files on page 295), copy the .ISO file that you received from AudioCodes from your PC to the OVOC server acems user home directory: /home/acems
3. Switch to 'root' user and provide *root* password (default password is *root*):

```
su - root
```

4. Specify the following commands:

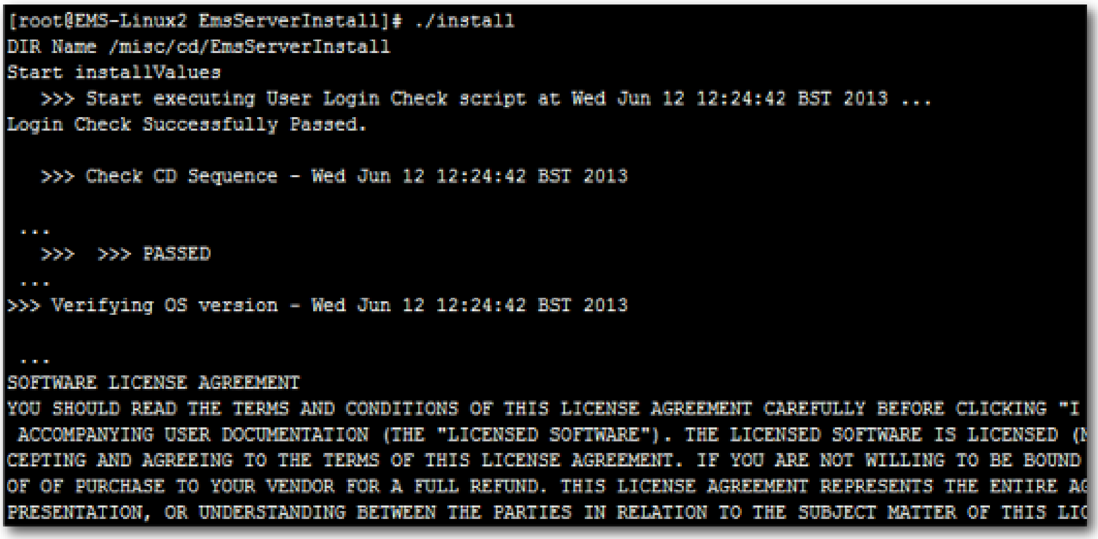
```
mount /home/acems/DVD3_OVOC_ 8.0.110.iso /mnt
```

```
cd /mnt/EmsServerInstall
```

5. Run the installation script from its location:

```
./install
```

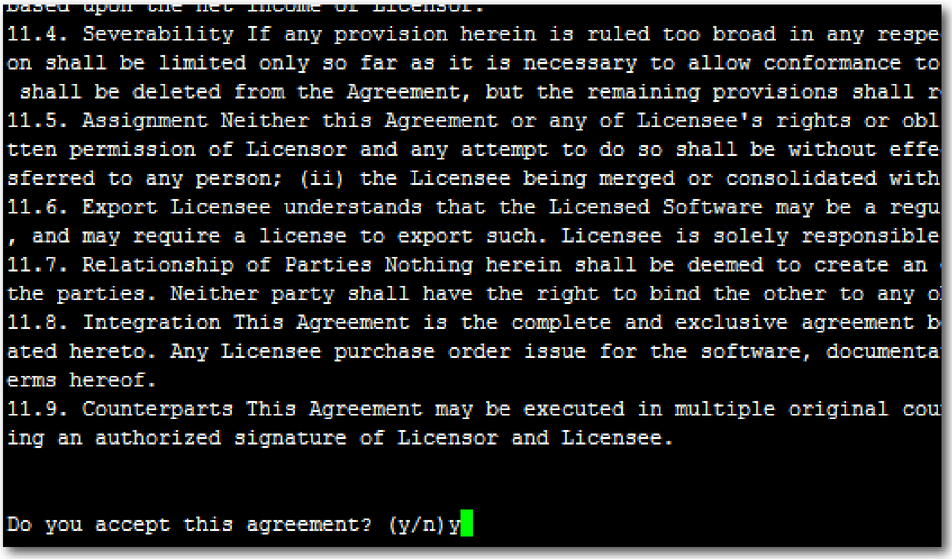
Figure 13-4: OVOC server Upgrade



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

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

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

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

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

Figure 13-5: OVOC server Upgrade– License Agreement

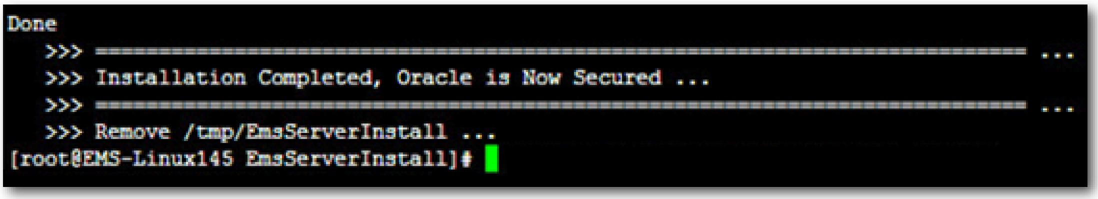


```
based upon the net income of Licensor.
11.4. Severability If any provision herein is ruled too broad in any respe
on shall be limited only so far as it is necessary to allow conformance to
 shall be deleted from the Agreement, but the remaining provisions shall r
11.5. Assignment Neither this Agreement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


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

7. The upgrade process installs OS packages updates and patches. After the patch installation, reboot might be required:

- If you are prompted to reboot, press Enter to reboot the OVOC server, login as 'acems' user, enter password *acems (*or customer defined password) and then repeat steps 4-8 (inclusive).
- If you are not prompted to reboot, proceed to step Wait for the installation to complete and reboot the OVOC server by typing reboot. below.

Figure 13-6: OVOC server Installation Complete



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

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

```
su - root
```

11. Type the following command:

```
# EmsServerManager
```

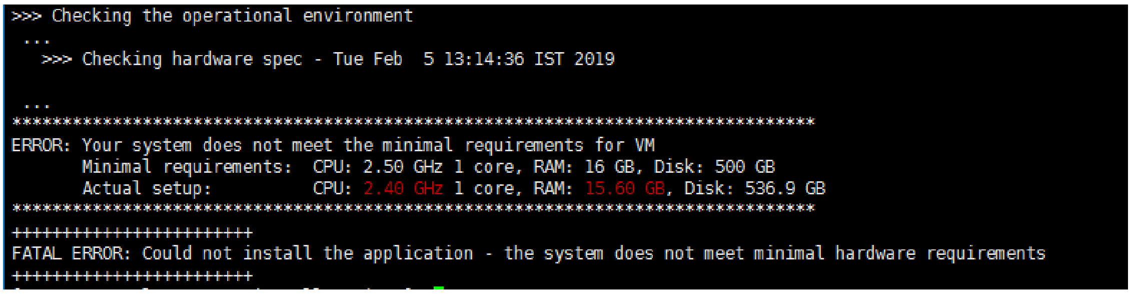
12. Verify that all processes are up and running (Viewing Process Statuses on page 169) and verify that login to OVOC Web client is successful.

14 Installation and Upgrade Troubleshooting of the Operational Environment

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

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

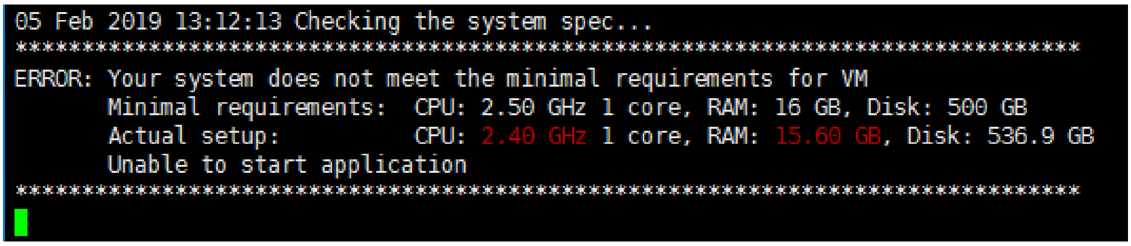
Figure 14-1: Minimum Hardware Requirements Upgrade



```
>>> Checking the operational environment
 ...
   >>> Checking hardware spec - Tue Feb  5 13:14:36 IST 2019

 ...
********************************************************************************
ERROR: Your system does not meet the minimal requirements for VM
       Minimal requirements:  CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
       Actual setup:          CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB
********************************************************************************
++++++++++++++++++++++++
FATAL ERROR: Could not install the application - the system does not meet minimal hardware requirements
++++++++++++++++++++++++
```

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

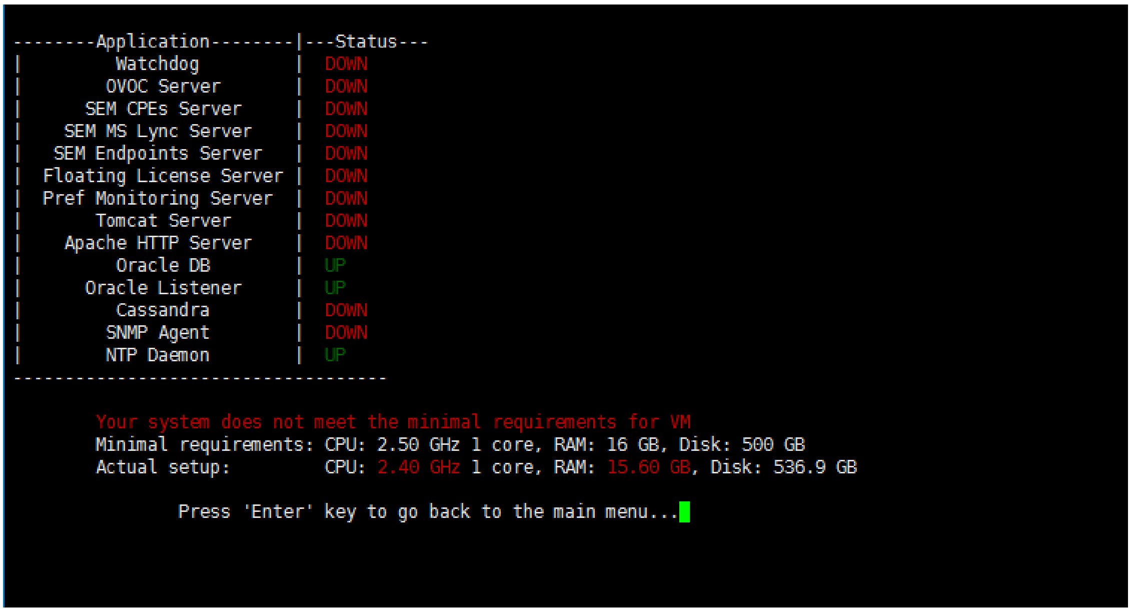
Figure 14-2: Minimum Hardware Requirements System Error



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

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

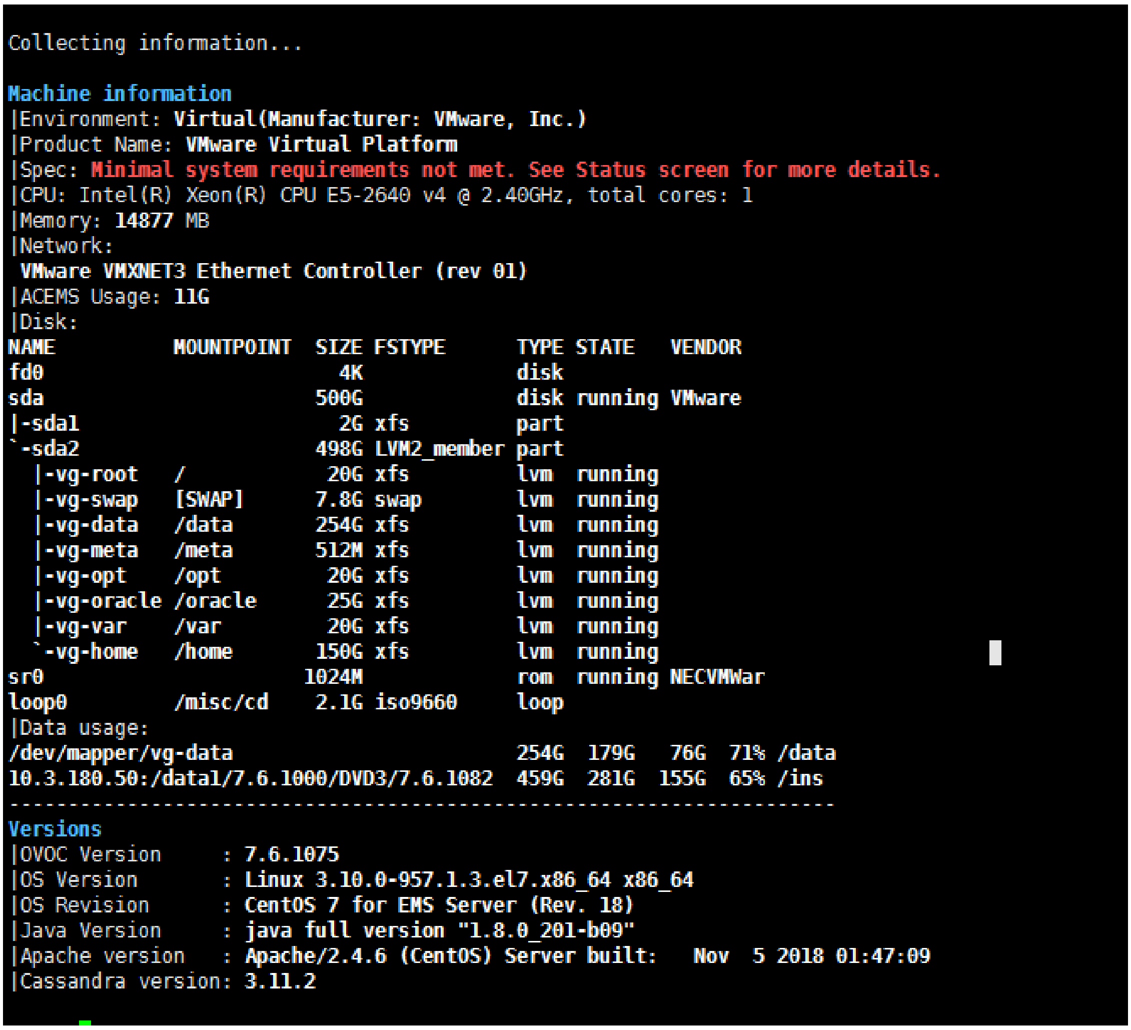
Figure 14-3: Status Screen Error



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

        Your system does not meet the minimal requirements for VM
        Minimal requirements: CPU: 2.50 GHz 1 core, RAM: 16 GB, Disk: 500 GB
        Actual setup:         CPU: 2.40 GHz 1 core, RAM: 15.60 GB, Disk: 536.9 GB

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

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

Figure 14-4: General Info Minimum Requirements



```
Collecting information...

Machine information
|Environment: Virtual(Manufacturer: VMware, Inc.)
|Product Name: VMware Virtual Platform
|Spec: Minimal system requirements not met. See Status screen for more details.
|CPU: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz, total cores: 1
|Memory: 14877 MB
|Network:
 VMware VMXNET3 Ethernet Controller (rev 01)
|ACEMS Usage: 11G
|Disk:
NAME          MOUNTPOINT  SIZE FSTYPE      TYPE STATE   VENDOR
fd0                         4K             disk
sda                       500G             disk running VMware
|-sda1                      2G xfs         part
`-sda2                    498G LVM2_member part
  |-vg-root   /            20G xfs         lvm  running
  |-vg-swap   [SWAP]      7.8G swap        lvm  running
  |-vg-data   /data       254G xfs         lvm  running
  |-vg-meta   /meta       512M xfs         lvm  running
  |-vg-opt    /opt         20G xfs         lvm  running
  |-vg-oracle /oracle      25G xfs         lvm  running
  |-vg-var    /var         20G xfs         lvm  running
  `-vg-home   /home       150G xfs         lvm  running
sr0                      1024M             rom  running NECVMWar
loop0         /misc/cd    2.1G iso9660     loop
|Data usage:
/dev/mapper/vg-data                        254G  179G   76G  71% /data
10.3.180.50:/datal/7.6.1000/DVD3/7.6.1082  459G  281G  155G  65% /ins
----------------------------------------------------------------------
Versions
|OVOC Version     : 7.6.1075
|OS Version       : Linux 3.10.0-957.1.3.el7.x86_64 x86_64
|OS Revision      : CentOS 7 for EMS Server (Rev. 18)
|Java Version     : java full version "1.8.0_201-b09"
|Apache version   : Apache/2.4.6 (CentOS) Server built:   Nov  5 2018 01:47:09
|Cassandra version: 3.11.2
```

Part IV

OVOC Server Machine Backup and Restore

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

15 OVOC Server Backup Processes

There are four 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. For example, dailydbems_ <time&date>_<randomstring>_<index>. In addition, several other configuration and software files are backed up to the archive file emsServerBackup_<version>_ <time&date>.tar in the /data/NBIF/emsBackup/RmanBackup directory. In general, this TAR file contains the entire /data/NBIF directory's content, with the exception of the 'emsBackup' directory, OVOC Software Manager content and server_xxx directory content.

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

- **Daily backup:** runs daily except on the day scheduled for the weekly backup (see above). The daily backup process backs up the last 24 hours. There are no changes in the TAR file in this process.
- **Cassandra backup:** runs daily (runs prior to the above) and backs up the last 24 hours to the archive file cassandraBackup_<version>_<date>_<snapshotId>_<Role>_ numberOfNodes.tar. When working in **Service Provider Cluster**, backup of the cluster node servers (VQM and PM) is performed on the Management server.
- **Configuration backup:** runs daily and backs up to the archive file ovocConfigBackup_ <version>_<time&date>.tar.gz

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

- The Backup process does not backup configurations performed using OVOC Server Manager, such as networking and security.
- RmanBackup files are deleted during the OVOC server upgrade.
- It is highly recommended to maintain all backup files on an external machine. These files can be transferred outside the server directly from their default location by SCP or SFTP client using 'acems' user.

➢ **Do the following:**

1. Copy the following backup files to an external machine:
   - /data/NBIF/emsBackup/emsServerBackup_<version>_<time&date>.tar
   - /data/NBIF/emsBackup/ovocConfigBackup_<version>_<time&date>.tar.gz
   - /data/NBIF/emsBackup/cassandraBackup_<version>_<date>_<snapshotId>_ <MGMT>_numberOfNodes.tar

- /data/NBIF/emsBackup/RmanBackup/daily_dbems_<time&date>_<randomstring>_<index>
- /data/NBIF/emsBackup/RmanBackup/weekly_dbems_<time&date>_<randomstring>_<index>
- /data/NBIF/emsBackup/RmanBackup/control.ctl
- /data/NBIF/emsBackup/RmanBackup/init.ora

Change Schedule Backup Time

This step describes how to reschedule the time to run the automatic backup of the following files:

- emsServerBackup_<version>_<time&date>.tar
- RmanBackup
- ovocConfigBackup_<version>_<time&date>.tar.gz
- cassandraBackup_<version>_<date>_<snapshotId>_<Role>_numberOfNodes.tar.

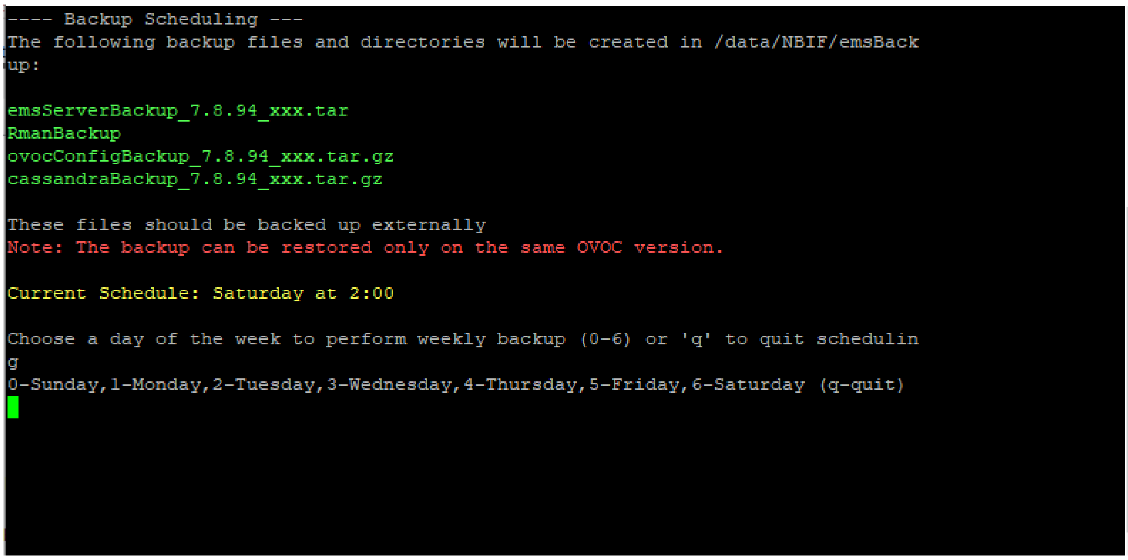
  where:

  - <time&date> is an example; replace this path with your filename.
  - <version> is the version number of the OVOC server release

➢ 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.

Figure 15-1: Backup Scheduling



```
---- Backup Scheduling ---
The following backup files and directories will be created in /data/NBIF/emsBack
up:

emsServerBackup_7.8.94_xxx.tar
RmanBackup
ovocConfigBackup_7.8.94_xxx.tar.gz
cassandraBackup_7.8.94_xxx.tar.gz

These files should be backed up externally
Note: The backup can be restored only on the same OVOC version.

Current Schedule: Saturday at 2:00

Choose a day of the week to perform weekly backup (0-6) or 'q' to quit schedulin
g
0-Sunday,1-Monday,2-Tuesday,3-Wednesday,4-Thursday,5-Friday,6-Saturday (q-quit)
```

16 OVOC Server Restore

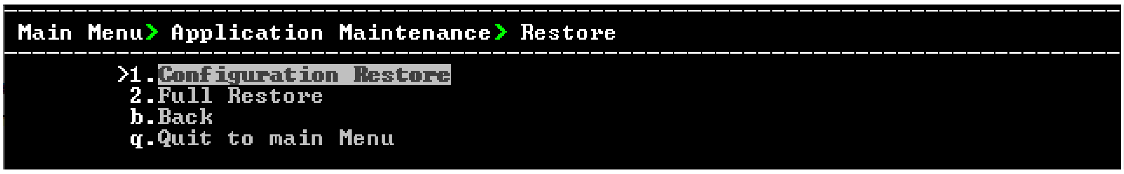
This section describes how to restore the OVOC server. This can be done on the original machine that the backup files were created from or on any other machine.

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

➢ To restore the OVOC server:

1. Install (or upgrade) OVOC to the same version from which the backup files were created. The Linux version must also be identical between the source and target machines.
2. Use the OVOC server Management utility to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.
3. For more details, see Getting Started on page 163.
4. Make sure all server processes are up in OVOC Server Manager / Status menu and the server functions properly.
5. Copy all the files you backed up in Chapter OVOC server Backup to /data/NBIF directory by SCP or SFTP client using the 'acems' user. Overwrite existing files if required.
6. From the Application Maintenance menu, choose the **Restore** option.

Figure 16-1: Restore Menu



```
Main Menu> Application Maintenance> Restore
        >1.Configuration Restore
         2.Full Restore
         b.Back
         q.Quit to main Menu
```

7. Choose one of the following options:
   - Configuration Restore below
   - Full Restore on page 160

Configuration Restore

This option restores OVOC topology and OVOC Web configuration. The following data is restored:

- Network Topology
- License configuration

- Alarm Forwarding Rules
- Report Definitions
- PM Profiles
- QOE Thresholds
- QOE Status and Alarm definitions
- The entire configuration performed under System Configuration and System Administration menus

Data is restored from the following backup files:

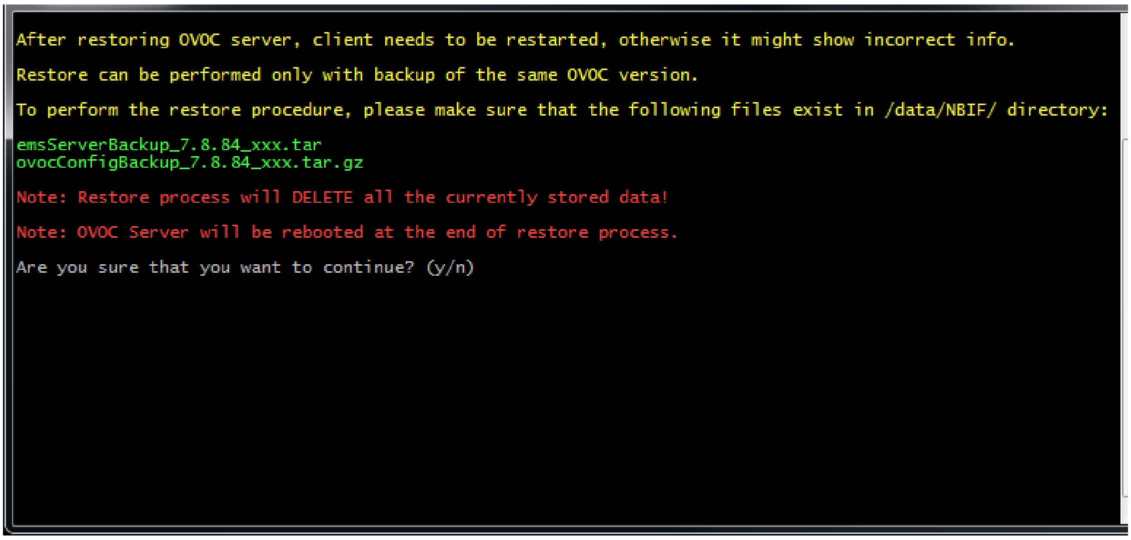
- emsServerBackup_<version>_<time&date>.tar
- ovocConfigBackup_<version>_<time&date>.tar.gz

> The restore process deletes all currently stored data as described above.
> Data that is retrieved from managed devices is not backed up, including: Alarms; Calls& SIP ladder; QoE & PM statistics; Users; Journals and Floating license reports.

➢ To run the configuration restore operation:

1. Select **Option 1: Configuration Restore**. A screen similar to the following is displayed:

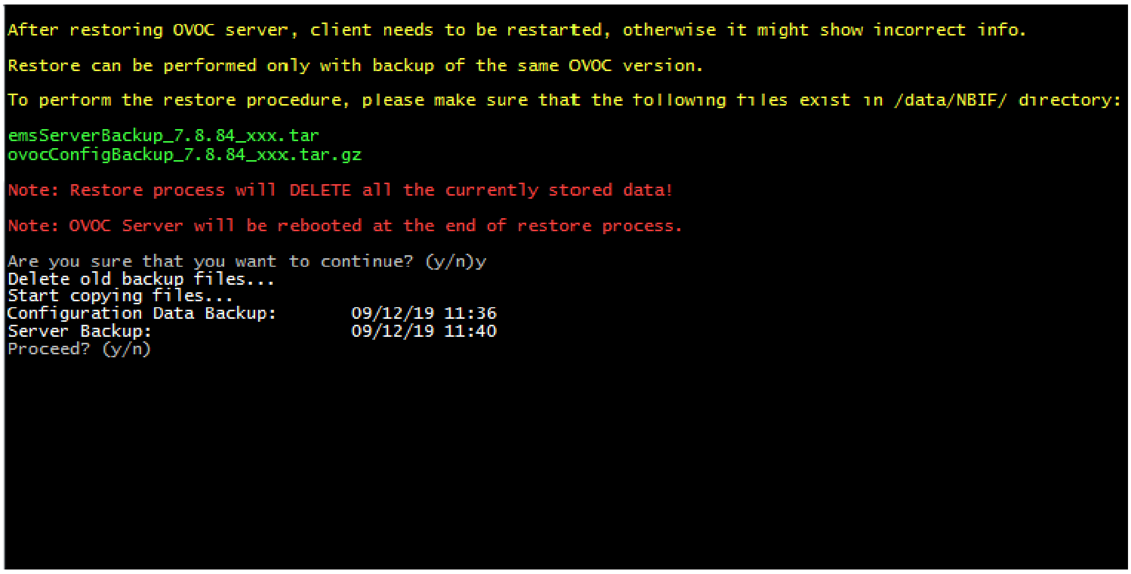
Figure 16-2: Configuration Restore Prompt



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.
Restore can be performed only with backup of the same OVOC version.
To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:
emsServerBackup_7.8.84_xxx.tar
ovocConfigBackup_7.8.84_xxx.tar.gz
Note: Restore process will DELETE all the currently stored data!
Note: OVOC Server will be rebooted at the end of restore process.
Are you sure that you want to continue? (y/n)
```

2. Type **y** to proceed. A screen similar to the following is displayed:

Figure 16-3: Configuration Restore-Confirm



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.

Restore can be performed only with backup of the same OVOC version.

To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:

emsServerBackup_7.8.84_xxx.tar
ovocConfigBackup_7.8.84_xxx.tar.gz

Note: Restore process will DELETE all the currently stored data!

Note: OVOC Server will be rebooted at the end of restore process.

Are you sure that you want to continue? (y/n)y
Delete old backup files...
Start copying files...
Configuration Data Backup:       09/12/19 11:36
Server Backup:                   09/12/19 11:40
Proceed? (y/n)
```

3. Type **y** to proceed.

4. After the restore operation has completed, you are prompted to reboot the OVOC server.

5. If you installed custom certificates prior to the restore operation, you must reinstall these certificates (see Appendix Supplementary Security Procedures on page 283).

Full Restore

This option restores OVOC topology, OVOC Web configuration (as detailed in Configuration Restore on page 158) and data that is retrieved from managed devices including PMs, calls, alarms and journals. Data from the following backup files is restored:

- emsServerBackup_<version>_<time&date>.tar
- cassandraBackup_<version>_<date>_<snapshotId>_<MGMT>_numberOfNodes.tar
- daily_dbems__<time&date>_<randomstring>_<index>
- weekly_dbems__<time&date>_<randomstring>_<index>
- control.ctl
- init.ora

The restore process deletes all currently stored data including PMs, calls, alarms and journals.

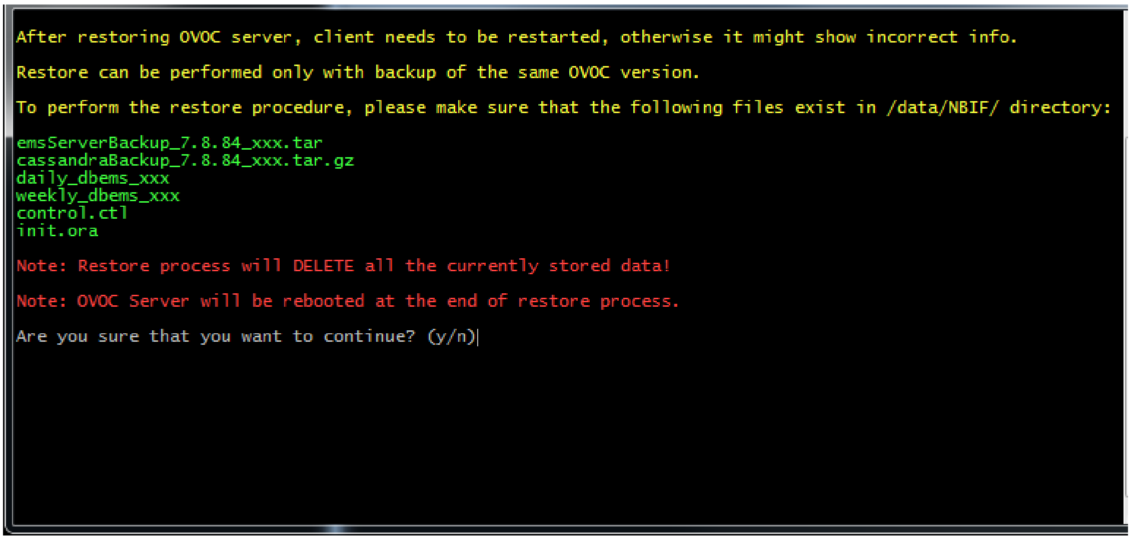
When operating in Service Provider Cluster:

- The restore cluster should be defined with identical system specifications as the backed up server i.e. the same number of VQM/PM servers.
- Following restore, restart slaves and then wait up to 24 hours for Cassandra DB data(call details and PM details) to synchronize on all servers.

➢ To run the full restore operation:

1. Select **Option 2: Full Restore**. A screen similar to the following is displayed:

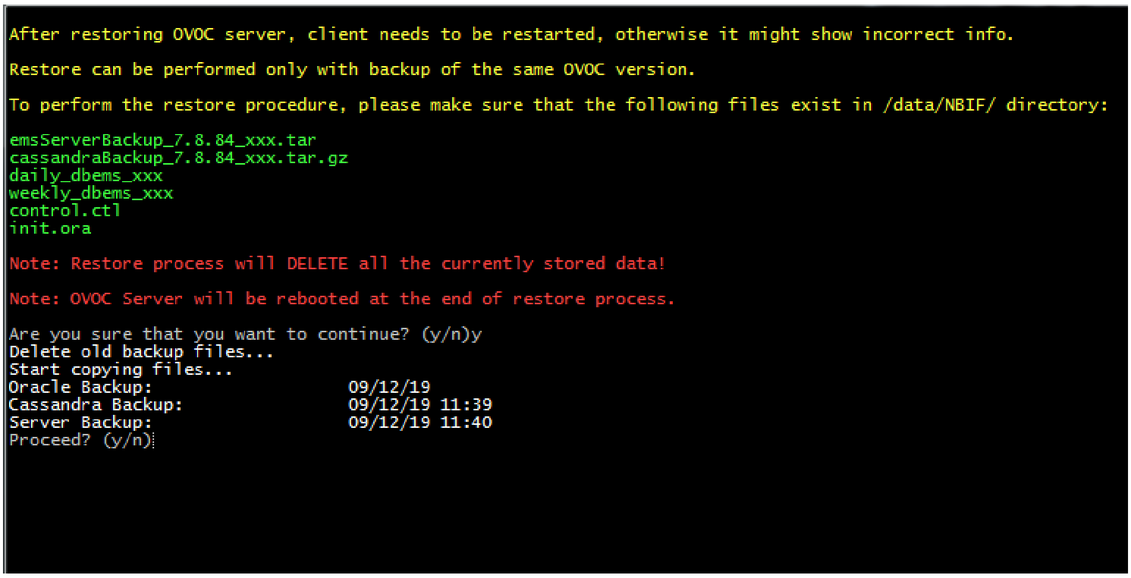
Figure 16-4: Full Restore Prompt



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.

Restore can be performed only with backup of the same OVOC version.

To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:

emsServerBackup_7.8.84_xxx.tar
cassandraBackup_7.8.84_xxx.tar.gz
daily_dbems_xxx
weekly_dbems_xxx
control.ctl
init.ora

Note: Restore process will DELETE all the currently stored data!

Note: OVOC Server will be rebooted at the end of restore process.

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

2. Type **y** to proceed. A screen similar to the following is displayed:

Figure 16-5: Confirm Full Restore



```
After restoring OVOC server, client needs to be restarted, otherwise it might show incorrect info.

Restore can be performed only with backup of the same OVOC version.

To perform the restore procedure, please make sure that the following files exist in /data/NBIF/ directory:

emsServerBackup_7.8.84_xxx.tar
cassandraBackup_7.8.84_xxx.tar.gz
daily_dbems_xxx
weekly_dbems_xxx
control.ctl
init.ora

Note: Restore process will DELETE all the currently stored data!

Note: OVOC Server will be rebooted at the end of restore process.

Are you sure that you want to continue? (y/n)y
Delete old backup files...
Start copying files...
Oracle Backup:                   09/12/19
Cassandra Backup:                09/12/19 11:39
Server Backup:                   09/12/19 11:40
Proceed? (y/n)
```

3. Type **y** to proceed.

4. After the restore operation has completed, you are prompted to reboot the OVOC server.

5. If you installed custom certificates prior to the restore, you must reinstall these certificates (see Appendix Supplementary Security Procedures on page 283).

Part V

OVOC Server Manager

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

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

Note: To exit the OVOC Server Managerto Linux OS shell level, press q.

17 Getting Started

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

Connecting to the OVOC Server Manager

You can either run the OVOC Server Managerutility locally or remotely:

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

➢ **Do the following:**

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

   ```
   su - root
   ```

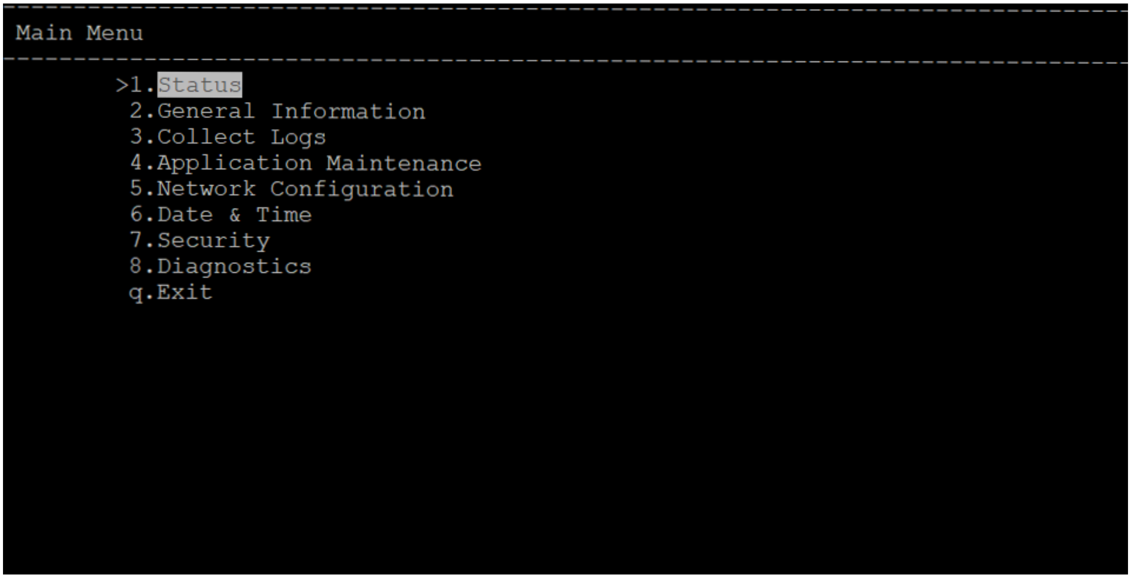
3. Type the following command:

   ```
   # EmsServerManager
   ```

   The OVOC Server Managermenu is displayed:

Figure 17-1: OVOC Server ManagerMenu

Figure 17-2:



```
-------------------------------------------------------------------------------
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
```

- 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.

Using the OVOC Server Manager

The following describes basic user hints for using the OVOC 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".

OVOC Server Manager Menu Options Summary

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

- **Status** – Shows the status of current OVOC processes (Viewing Process Statuses on page 169)
- **General Information** – Provides the general OVOC server current information from the Linux operating system, including OVOC Version, OVOC server Process Status, Oracle Server Status, Apache Server Status, Java Version, Memory size and Time Zone (Viewing General Information on page 174).
- **Collect Logs** – Collates all important logs into a single compressed file (Collecting Logs on page 178):
- **Application Maintenance** – Manages system maintenance actions (Application Maintenance on page 180):
    - Start / Restart the Application
    - Stop Application
    - Web Servers
    - Change Schedule Backup Time
    - Restore
    - License
    - Analytics API
    - Service Provider Cluster
    - Shutdown the machine
    - Reboot the machine
- **Network Configuration** – Provides all basic, advanced network management and interface updates (Network Configuration on page 194):
    - Server IP Address (The server is rebooted)
    - Ethernet Interfaces (The server is rebooted)
    - Ethernet Redundancy (The server is rebooted)
    - DNS Client
    - NAT
    - Static Routes
    - SNMP Agent
        - Configure SNMP Agent

          -SNMP Agent Listening Port

          -Linux System Traps Forwarding Configuration

          -SNMPv3 Engine ID
        - Start SNMP Agent
        - SNMPv3 Engine ID

  - Cloud Architecture
- **Date & Time** – Configures time and date settings (Date and Time Settings on page 216):
  - NTP
  - Timezone Settings
  - Date and Time Settings
- **Security** – Manages all the relevant security configurations (Security on page 217):
  - Add OVOC user
  - SSH
  - Oracle DB Password (OVOC server will be stopped)
  - Cassandra DB Password (OVOC server will be stopped)
  - OS Users Passwords
  - HTTP Security Settings:
    - TLS Version 1.0
    - TLS Version 1.1
    - Show Allowed SSL Cipher Suites
    - Edit SSL Cipher Suites Configuration String
    - Restore SSL Cipher Suites Configuration Default
    - Manage HTTP Service (Port 80)
    - Manage IPP Files Service (Port 8080)
    - Manage IPPs HTTP (Port 8081)
    - Manage IPPs HTTPS (Port 8082)
    - OVOC REST (Port 911)
    - Floating License REST (Port 912)
    - OVOC WebSocket (Port 915)
    - SBC HTTPS Authentication
    - Enable Device Manager client secured communication (Apache will be restarted)
    - Change HTTP/S Authentication Password for NBIF Directory
  - File Integrity Checker
  - Software Integrity Checker (AIDE) and Prelinking
  - USB Storage
  - Network Options
  - Audit Agent Options (the server will be rebooted)

  - Server Certificates Update
  - OVOC Voice Quality Package - SBC Communication
- **Diagnostics** – Manages system debugging and troubleshooting (Diagnostics on page 248):
  - Server Syslog
  - Devices Syslog
  - Devices Debug
  - Server Logger Levels
  - Network Traffic Capture

OVOC Server Manager Options for Service Provider Cluster

The following options are available in the OVOC Server Manager menu on the PM and VQM servers when the Service Provider Cluster feature is enabled:

- Status
- General Information
- Collect Logs
- Application Maintenance
  - Restart Application
  - Restore
  - Service Provider Cluster Configuration
  - Shutdown
  - Reboot
- Network Configuration
  - Server IP address
- Date & Time
  - NTP
  - Timezone Settings
  - Date & Time Settings
- Security
  - SSH
  - OS Users Passwords
  - File Integrity Checker
  - Software Integrity Checker (AIDE) and Prelinking
  - USB Storage

    - Network options

- Diagnostics

    - Logger Levels

    - Network Traffic Capture

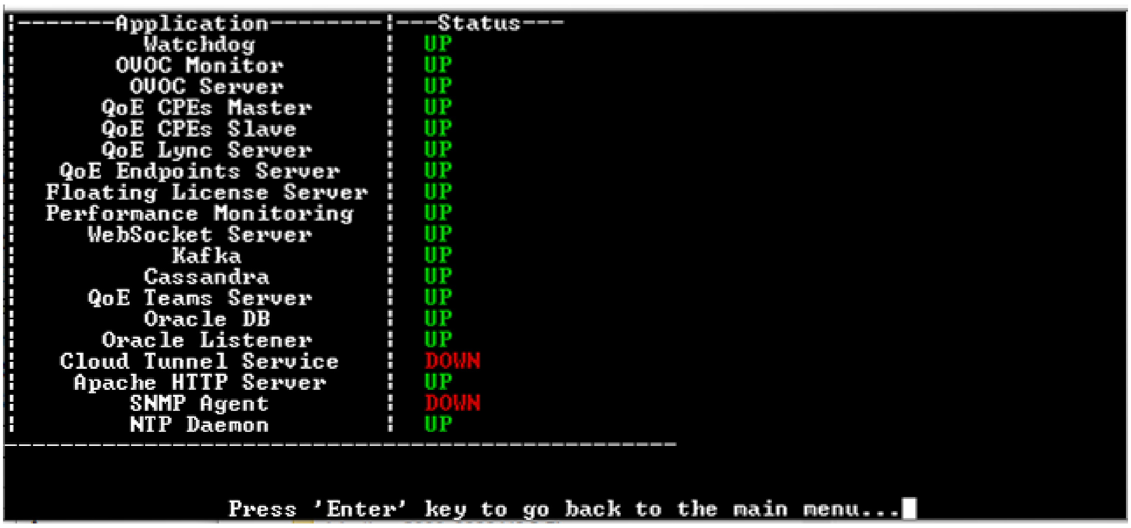
18 Viewing Process Statuses

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 18-1: Application Status in Stand-alone Mode



```
|-------Application--------|---Status---
|         Watchdog         |  UP
|       OVOC Monitor       |  UP
|       OVOC Server        |  UP
|     QoE CPEs Master      |  UP
|     QoE CPEs Slave       |  UP
|     QoE Lync Server      |  UP
|   QoE Endpoints Server   |  UP
|  Floating License Server |  UP
|  Performance Monitoring  |  UP
|     WebSocket Server     |  UP
|          Kafka           |  UP
|        Cassandra         |  UP
|     QoE Teams Server     |  UP
|        Oracle DB         |  UP
|     Oracle Listener      |  UP
|   Cloud Tunnel Service   |  DOWN
|    Apache HTTP Server    |  UP
|        SNMP Agent        |  DOWN
|        NTP Daemon        |  UP
------------------------------------------------

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

The following table describes the application statuses when OVOC runs in Stand-alone mode.

Table 18-1: Application Statuses in Stand-alone Mode

Application	Status
Watchdog	Indicates the status of the OVOC Watchdog process.
OVOC Monitor	Validates the local OVOC server connection, clock configuration and installed software version.
OVOC Server	Indicates the status of the OVOC server process.
QoE CPEs Master	Indicates the voice quality master process status on the local server
QoE CPEs Slave	Indicates the voice quality slave process status on the local server (identical to QoE CPEs Master process in Stand-alone mode)
QoE Lync Server	Indicates the status of the process that is responsible for retrieving Skype for Business calls and for monitoring connectivity status with Microsoft Lync server.
QoE Endpoints Server	Indicates the status of the Endpoint Server, which manages the UDP connection with the Endpoints (IP Phones) for Voice Quality Package

Application	Status
	SIP Publish RFC 6035 messages.
Floating License Server	Indicates the status of the connection between the OVOC server and the Floating License service.
Performance Monitoring Server	Indicates the status of the internal SNMP connection used by the OVOC server for polling managed devices.
WebSocket Server	Indicates the status of the internal connection between the WebSocket client (OVOC Web interface) and the OVOC server. This connection is used for managing the alarm and task notification mechanism.
Kafka	Indicates the status of the Kafka process for managing alarms retrieved from the VQM and PM servers.
Cassandra	Indicates the status of the Cassandra database that manages Call Details and SIP Ladder messages.
QoE Teams Server	Indicates the status of the OVOC process (QoE Teams Server – Up/Down) that is responsible for retrieving Teams Call Records from defined MS Teams Tenants and for monitoring connectivity status with MS Teams Tenants.
Oracle DB	Indicates the status of the Oracle Database process.
Oracle Listener	Indicates the status of the Oracle Listener process.
Cloud Tunnel Service	Indicates the status of the Cloud Tunnel Service (see Configure OVOC Cloud Architecture Mode on page 115
Apache HTTP 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.
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.

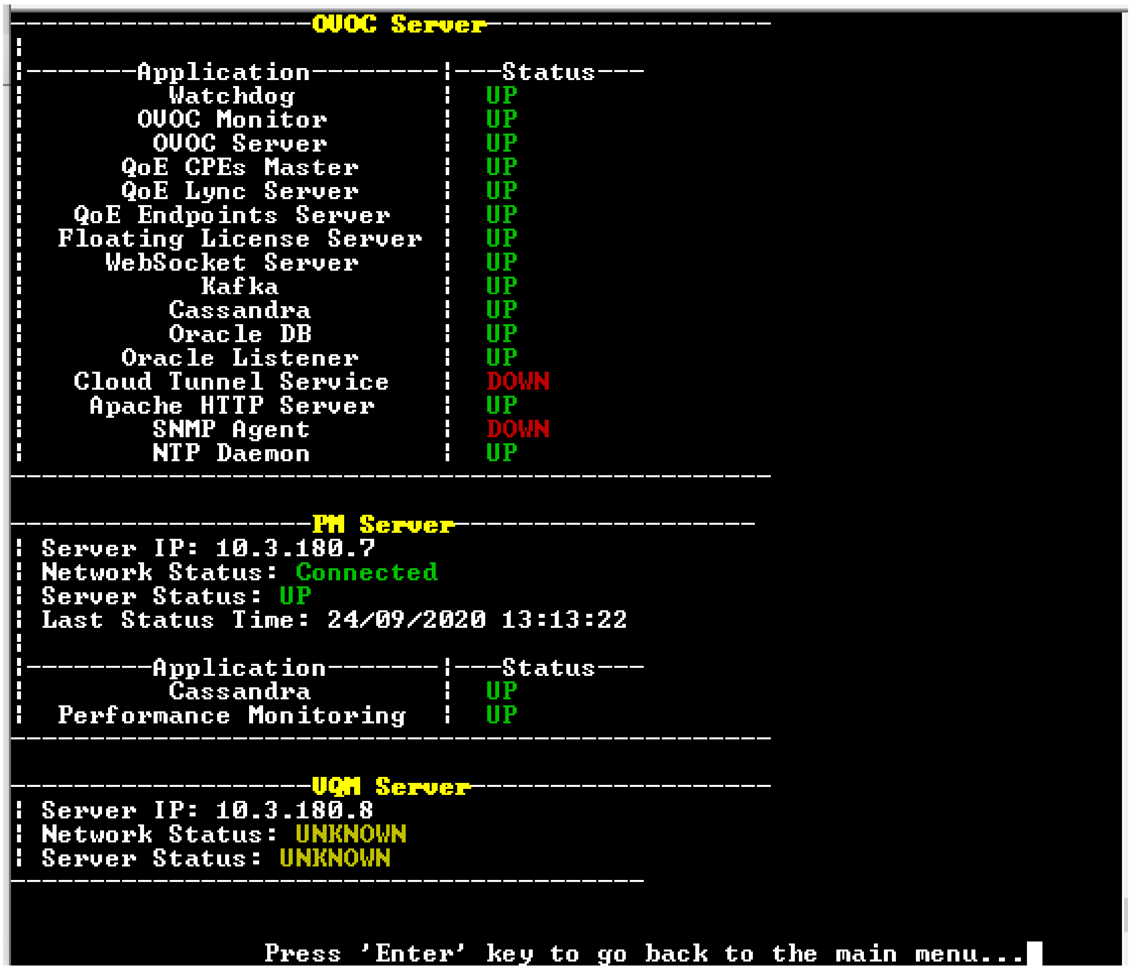
Viewing Process Statuses in Service Provider Cluster Mode

The figure below illustrates the process statuses in Service Provider Cluster mode.

➢ **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 18-2: Application Statuses in Service Provider Cluster on Management Server



```
-------------------OVOC Server------------------
|
|-------Application--------|---Status---
|       Watchdog           |  UP
|      OVOC Monitor        |  UP
|       OVOC Server        |  UP
|     QoE CPEs Master      |  UP
|     QoE Lync Server      |  UP
|  QoE Endpoints Server    |  UP
| Floating License Server  |  UP
|    WebSocket Server      |  UP
|          Kafka           |  UP
|        Cassandra         |  UP
|        Oracle DB         |  UP
|     Oracle Listener      |  UP
|  Cloud Tunnel Service    |  DOWN
|   Apache HTTP Server     |  UP
|       SNMP Agent         |  DOWN
|       NTP Daemon         |  UP
------------------------------------------------

-------------------PM Server-------------------
| Server IP: 10.3.180.7
| Network Status: Connected
| Server Status: UP
| Last Status Time: 24/09/2020 13:13:22
|
|--------Application-------|---Status---
|        Cassandra         |  UP
|  Performance Monitoring  |  UP
------------------------------------------------

-------------------VQM Server-------------------
| Server IP: 10.3.180.8
| Network Status: UNKNOWN
| Server Status: UNKNOWN
----------------------------------------


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

Table 18-2: Application Statuses in Service Provider Cluster

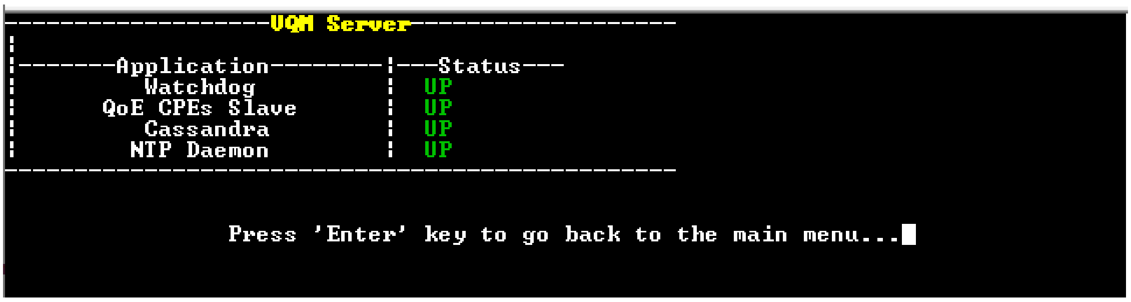
Application	Status
Watchdog	Indicates the status of the OVOC Watchdog process.
OVOC Monitor	Validates that all the cluster nodes are connected to the network, their clocks are synchronized with the Management server and are all nodes are installed with the same OVOC software version.
OVOC Server	Indicates the status of the OVOC server process.
QoE CPEs Master	Indicates the voice quality process status on the Management

Application	Status
	server.
QoE CPEs Slave	Indicates the voice quality process status on the VQM server node in the clustesr.
QoE Lync Server	Indicates the status of the Skype for Business Server MS-SQL Server HTTP/S connection.
QoE Endpoints Server	Indicates the status of the Endpoint Server, which manages the UDP connection with the Endpoints (IP Phones) for Voice Quality Package SIP Publish RFC 6035 messages.
Floating License Server	Indicates the status of the connection between the OVOC server and the Floating License service.
Performance Monitoring Server	Indicate the PM process status on the PM server node in the cluster.
WebSocket Server	Indicates the status of the internal connection between the WebSocket client (OVOC Web interface) and the OVOC server. This connection is used for managing the alarm and task notification mechanism.
Kafka	Indicates the status of the Kafka process for managing alarms retrieved from the VQM and PM servers.
Cassandra	Indicates the status of the Cassandra database that manages Call Details and SIP Ladder messages.
QoE Teams Server	Indicates the status of the OVOC process (QoE Teams Server – Up/Down) that is responsible for retrieving Teams Call Records from defined MS Teams Tenants and for monitoring connectivity status with MS Teams Tenants.
Oracle DB	Indicates the status of the Oracle Database process.
Oracle Listener	Indicates the status of the Oracle Listener process.
Cloud Tunnel Service	Indicates the status of the Cloud Tunnel Service (see Configure OVOC Cloud Architecture Mode on page 115
Apache HTTP 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.

Application	Status
	■ The HTTP connection that is used by Endpoints for downloading firmware and configuration files from the OVOC server.
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.

The following figure displays the server status on the VQM node.

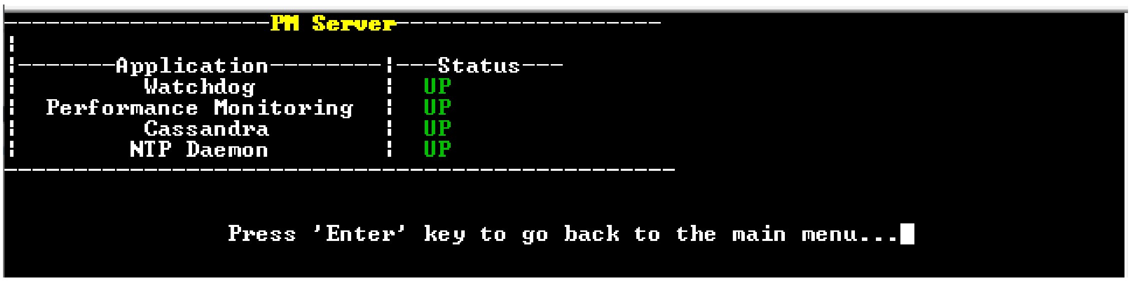
Figure 18-3: VQM Server Status



```
-------------------VQM Server-------------------
¦
¦-------Application--------¦---Status---
¦         Watchdog         ¦  UP
¦      QoE CPEs Slave      ¦  UP
¦         Cassandra        ¦  UP
¦        NTP Daemon        ¦  UP
------------------------------------------------


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

The following figure displays the status on the PM server.

Figure 18-4: PM Server Status



```
-------------------PM Server-------------------
¦
¦-------Application--------¦---Status---
¦         Watchdog         ¦  UP
¦  Performance Monitoring  ¦  UP
¦         Cassandra        ¦  UP
¦        NTP Daemon        ¦  UP
------------------------------------------------

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

19 Viewing General Information

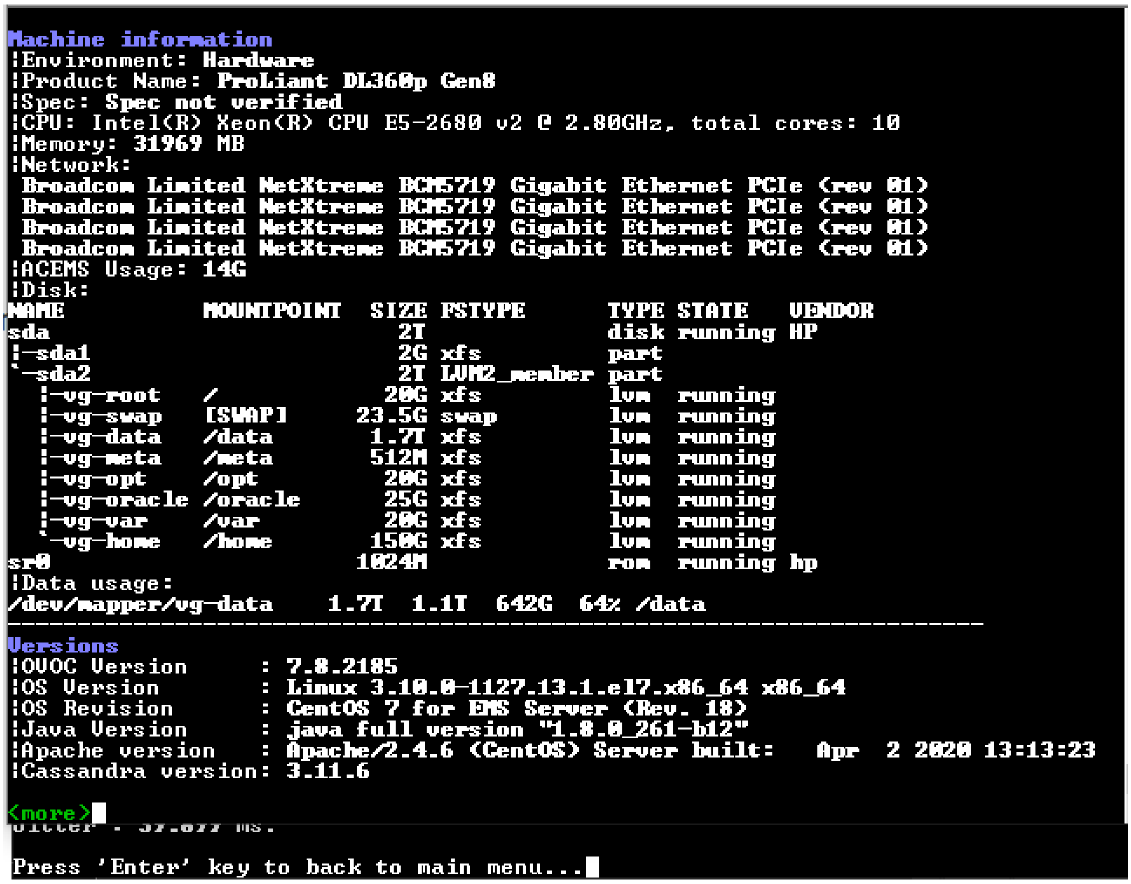
This section describes the General Information and Logs collection options. The General Information option provides detailed information about the OVOC server configuration and current status variables. The following information is provided:

- Components versions
- Components Statuses
- Memory size and disk usage
- Network configuration
- Time Zone and NTP configuration
- User logged in and session type

➢ To view General Information:

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

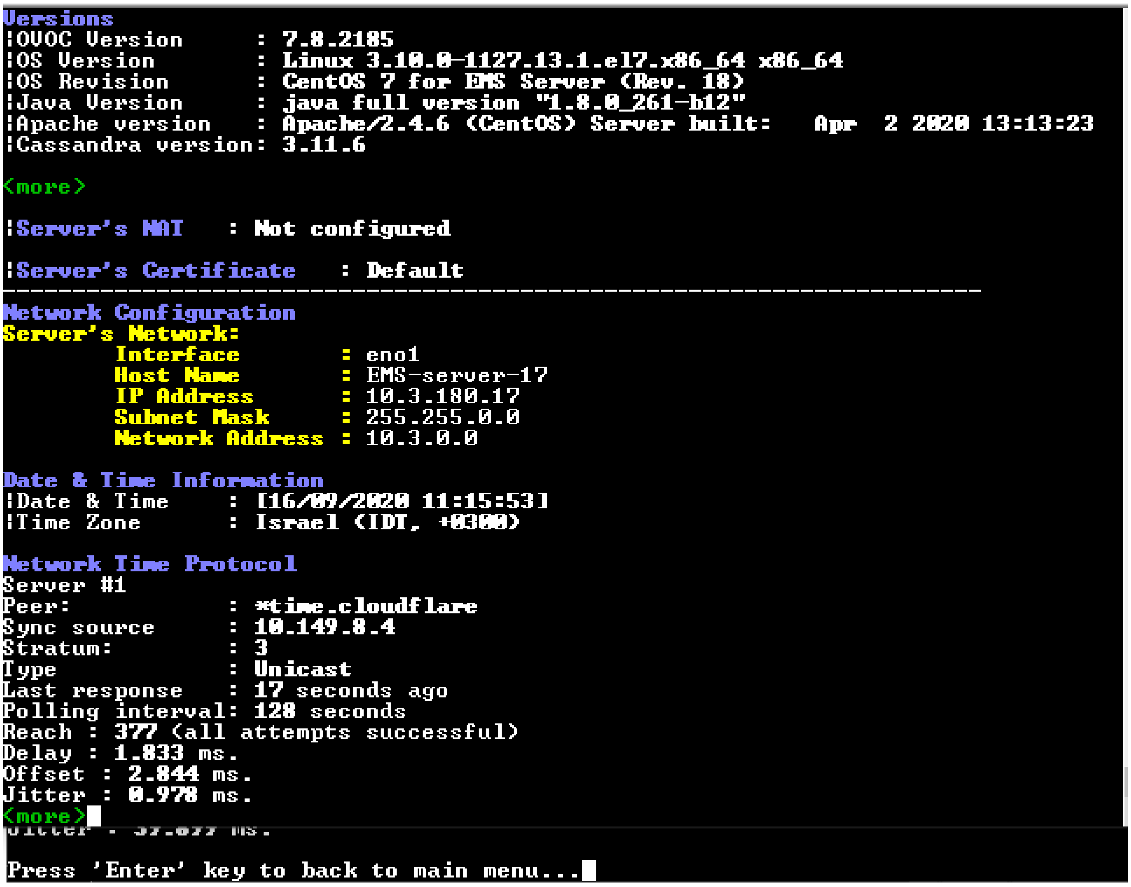
Figure 19-1: General Information



```
Machine information
¦Environment: Hardware
¦Product Name: ProLiant DL360p Gen8
¦Spec: Spec not verified
¦CPU: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz, total cores: 10
¦Memory: 31969 MB
¦Network:
 Broadcom Limited NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
 Broadcom Limited NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
 Broadcom Limited NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
 Broadcom Limited NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
¦ACEMS Usage: 14G
¦Disk:
NAME           MOUNTPOINT  SIZE FSTYPE      TYPE STATE   VENDOR
sda                          2T             disk running HP
¦-sda1                       2G xfs         part
`-sda2                       2T LVM2_member part
  ¦-vg-root    /           20G 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         20G xfs         lvm  running
  ¦-vg-oracle  /oracle      25G xfs         lvm  running
  ¦-vg-var     /var         20G xfs         lvm  running
  `-vg-home    /home       150G xfs         lvm  running
sr0                       1024M             rom  running hp
¦Data usage:
/dev/mapper/vg-data    1.7T  1.1T  642G  64% /data
-----------------------------------------------------------------------
Versions
¦OVOC Version      : 7.8.2185
¦OS Version        : Linux 3.10.0-1127.13.1.el7.x86_64 x86_64
¦OS Revision       : CentOS 7 for EMS Server (Rev. 18)
¦Java Version      : java full version "1.8.0_261-b12"
¦Apache version    : Apache/2.4.6 (CentOS) Server built:   Apr  2 2020 13:13:23
¦Cassandra version: 3.11.6

<more>
Jitter : 37.877 ms.

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

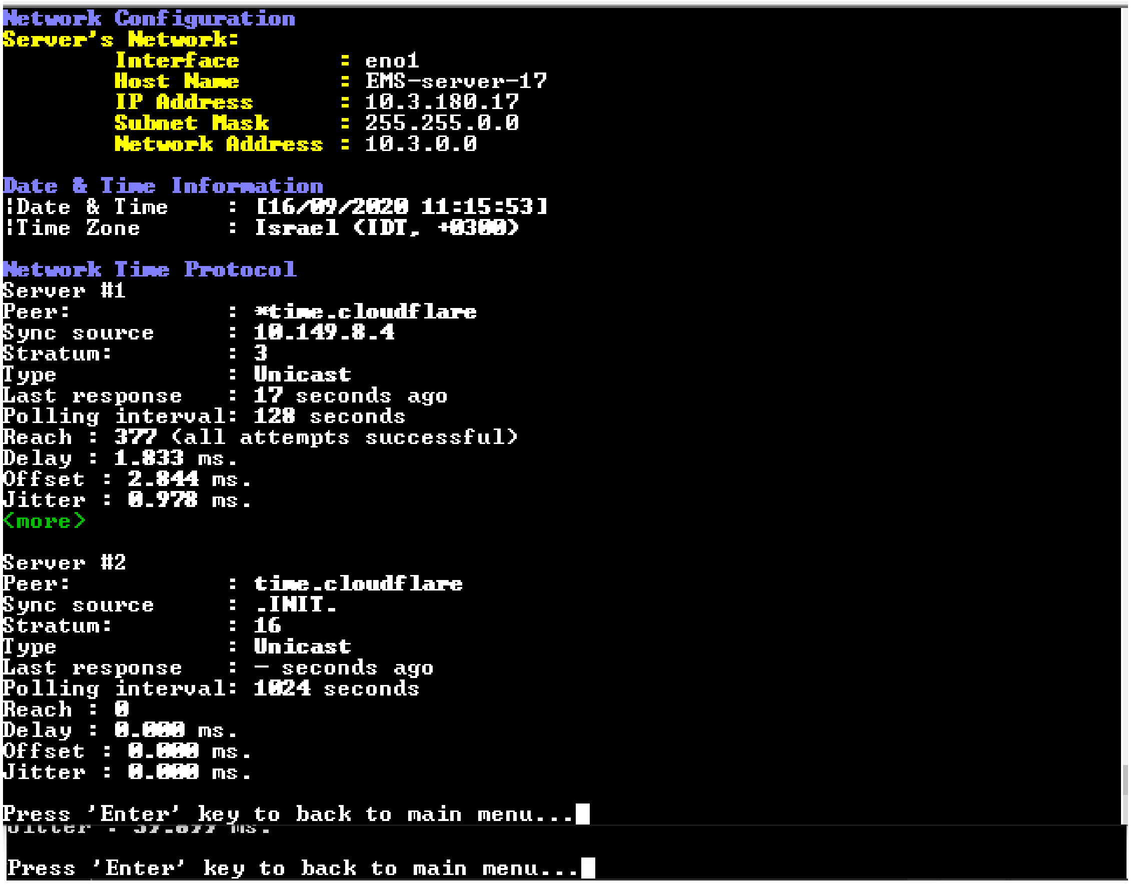
2. Press **<more>** to view more information; the following is displayed:

Figure 19-2: General Information 1



```
Versions
|OVOC Version       : 7.8.2185
|OS Version         : Linux 3.10.0-1127.13.1.el7.x86_64 x86_64
|OS Revision        : CentOS 7 for EMS Server (Rev. 18)
|Java Version       : java full version "1.8.0_261-b12"
|Apache version     : Apache/2.4.6 (CentOS) Server built:   Apr  2 2020 13:13:23
|Cassandra version: 3.11.6

<more>

|Server's NAT    : Not configured

|Server's Certificate    : Default
----------------------------------------------------------------------
Network Configuration
Server's Network:
        Interface         : eno1
        Host Name         : EMS-server-17
        IP Address        : 10.3.180.17
        Subnet Mask       : 255.255.0.0
        Network Address : 10.3.0.0

Date & Time Information
|Date & Time      : [16/09/2020 11:15:53]
|Time Zone        : Israel (IDT, +0300)

Network Time Protocol
Server #1
Peer:             : *time.cloudflare
Sync source       : 10.149.8.4
Stratum:          : 3
Type              : Unicast
Last response     : 17 seconds ago
Polling interval: 128 seconds
Reach : 377 (all attempts successful)
Delay : 1.833 ms.
Offset : 2.844 ms.
Jitter : 0.978 ms.
<more>
Jitter : 37.077 ms.

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

Figure 19-3: General Information 2



```
Network Configuration
Server's Network:
        Interface       : eno1
        Host Name       : EMS-server-17
        IP Address      : 10.3.180.17
        Subnet Mask     : 255.255.0.0
        Network Address : 10.3.0.0

Date & Time Information
|Date & Time     : [16/09/2020 11:15:53]
|Time Zone       : Israel (IDT, +0300)

Network Time Protocol
Server #1
Peer:            : *time.cloudflare
Sync source      : 10.149.8.4
Stratum:         : 3
Type             : Unicast
Last response    : 17 seconds ago
Polling interval: 128 seconds
Reach : 377 (all attempts successful)
Delay : 1.833 ms.
Offset : 2.844 ms.
Jitter : 0.978 ms.
<more>

Server #2
Peer:            : time.cloudflare
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...
Jitter : 37.677 ms.

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

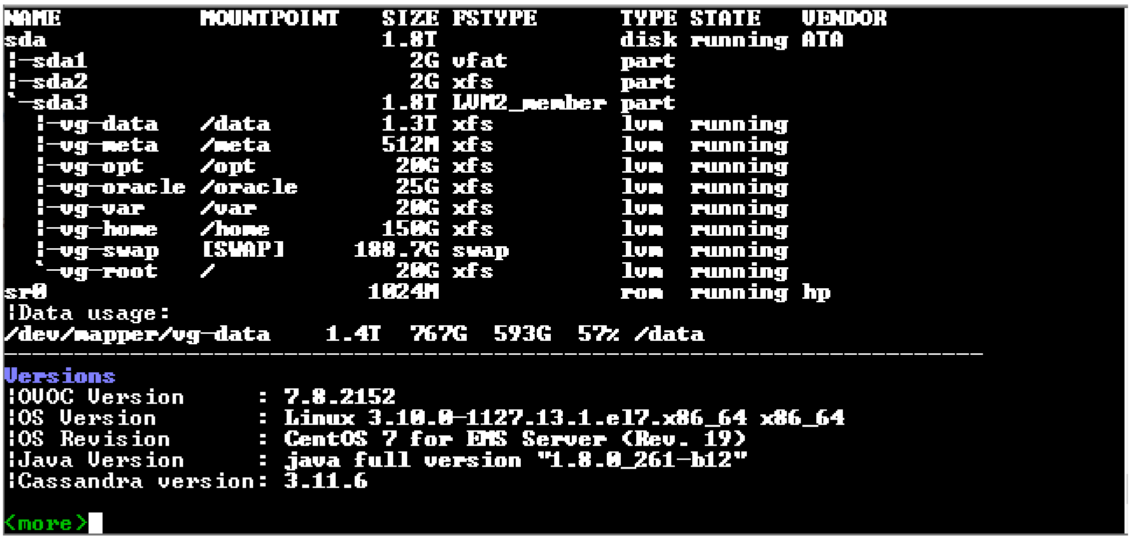
Viewing General Information in Service Provider Cluster Mode

The following shows general information that is displayed when the OVOC server is configured in Service Provider Cluster mode.

➢ To view General Information:

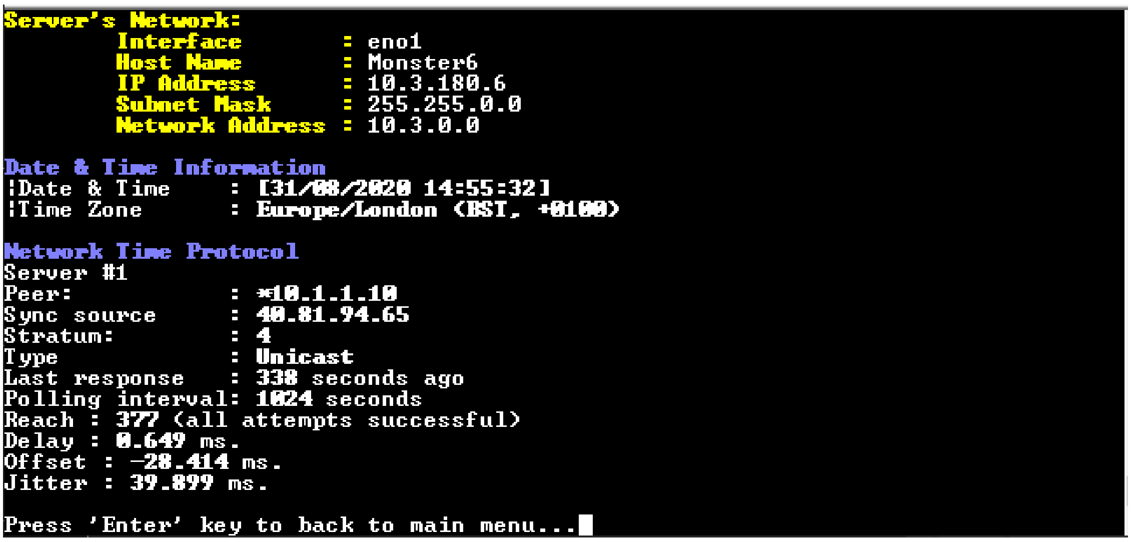
1. From the OVOC Server Manager root menu, choose **General Information**, and then press Enter; the following is displayed:

Figure 19-4: General Information Service Provider Cluster Node (PM/VQM servers)



```
NAME          MOUNTPOINT   SIZE FSTYPE      TYPE STATE   VENDOR
sda                        1.8T             disk running ATA
¦-sda1                       2G vfat        part
¦-sda2                       2G xfs         part
`-sda3                     1.8T LVM2_member part
  ¦-vg-data   /data        1.3T xfs         lvm  running
  ¦-vg-meta   /meta        512M xfs         lvm  running
  ¦-vg-opt    /opt          20G xfs         lvm  running
  ¦-vg-oracle /oracle       25G xfs         lvm  running
  ¦-vg-var    /var          20G xfs         lvm  running
  ¦-vg-home   /home        150G xfs         lvm  running
  ¦-vg-swap   [SWAP]     188.7G swap        lvm  running
  `-vg-root   /             20G xfs         lvm  running
sr0                       1024M             rom  running hp
¦Data usage:
/dev/mapper/vg-data    1.4T  767G  593G  57% /data
 ---------------------------------------------------------------------
Versions
¦OVOC Version     : 7.8.2152
¦OS Version       : Linux 3.10.0-1127.13.1.el7.x86_64 x86_64
¦OS Revision      : CentOS 7 for EMS Server (Rev. 19)
¦Java Version     : java full version "1.8.0_261-b12"
¦Cassandra version: 3.11.6

<more>
```

Figure 19-5: General Information Service Provider Cluster Node (PM/VQM servers)



```
Server's Network:
        Interface       : eno1
        Host Name       : Monster6
        IP Address      : 10.3.180.6
        Subnet Mask     : 255.255.0.0
        Network Address : 10.3.0.0

Date & Time Information
¦Date & Time     : [31/08/2020 14:55:32]
¦Time Zone       : Europe/London (BST, +0100)

Network Time Protocol
Server #1
Peer:            : *10.1.1.10
Sync source      : 40.81.94.65
Stratum:         : 4
Type             : Unicast
Last response    : 338 seconds ago
Polling interval: 1024 seconds
Reach : 377 (all attempts successful)
Delay : 0.649 ms.
Offset : -28.414 ms.
Jitter : 39.899 ms.

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

20 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.

⚠ When operating in the Service Provider Cluster Mode, logs are collected from all server nodes in the cluster (Management, VQM and PM servers)

The following log files are collected:

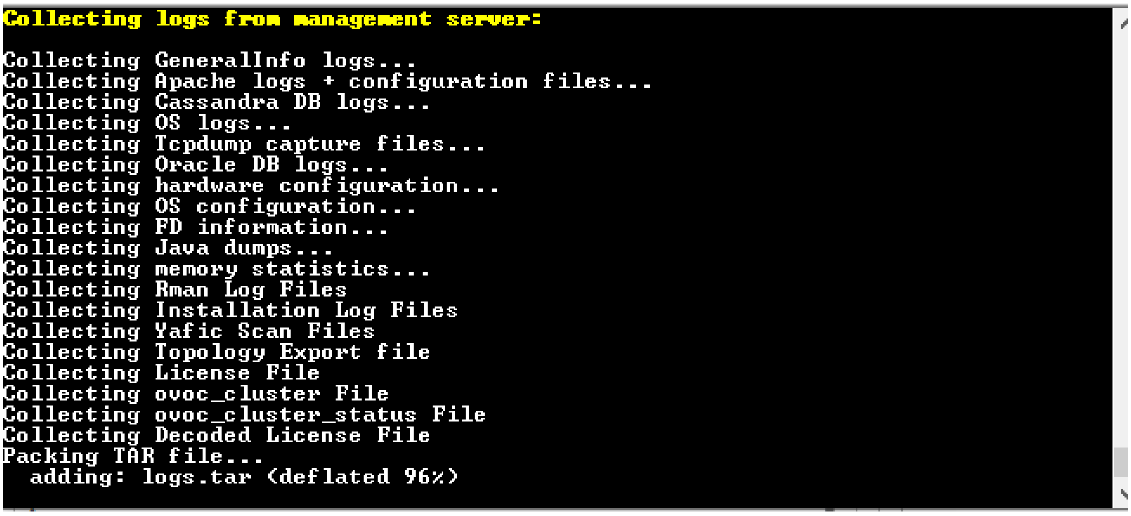
- OVOC server Application logs
- General Info logs
- Apache logs and configuration files
- Cassandra DB logs
- OS logs
- Oracle DB logs
- Hardware information (including disk)
- OS Configuration
- File Descriptors used by processes info
- Rman logs
- Installation logs
- Oracle Database logs
- Server's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

➢ To collect logs:

- From the OVOC server Management root menu, choose **Collect Logs**, and then press Enter; you are prompted if you wish to collect logs, enter **y** to proceed, the OVOC server commences the log collection process:

  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 20-1: Collecting Logs



```
Collecting logs from management server:

Collecting GeneralInfo logs...
Collecting Apache logs + configuration files...
Collecting Cassandra DB logs...
Collecting OS logs...
Collecting Tcpdump capture files...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting FD information...
Collecting Java dumps...
Collecting memory statistics...
Collecting Rman Log Files
Collecting Installation Log Files
Collecting Yafic Scan Files
Collecting Topology Export file
Collecting License File
Collecting ovoc_cluster File
Collecting ovoc_cluster_status File
Collecting Decoded License File
Packing TAR file...
  adding: logs.tar (deflated 96%)
```

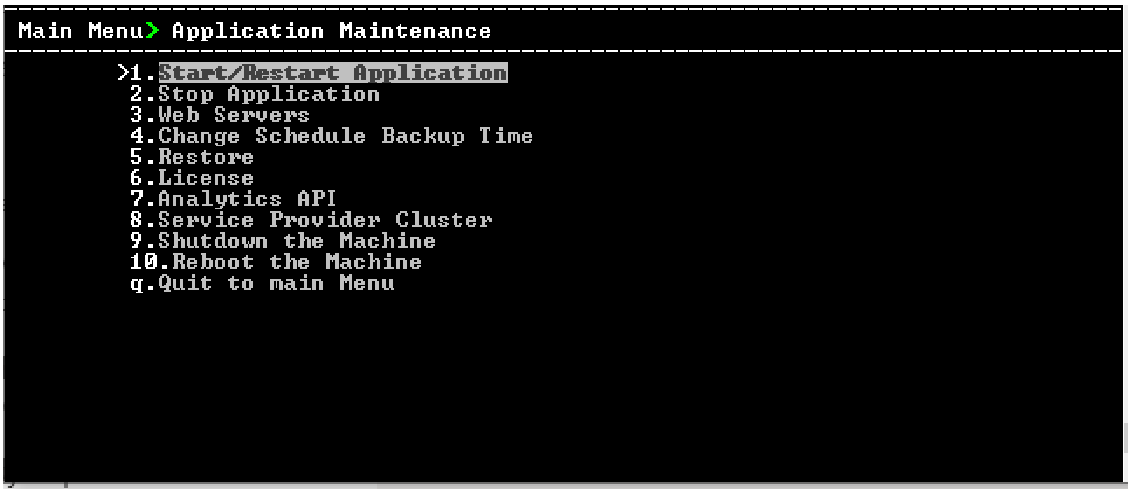
21 Application Maintenance

This section describes the application maintenance.

➢ **To configure application maintenance:**

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

Figure 21-1: Application Maintenance



```
Main Menu> Application Maintenance

        >1.Start/Restart Application
         2.Stop Application
         3.Web Servers
         4.Change Schedule Backup Time
         5.Restore
         6.License
         7.Analytics API
         8.Service Provider Cluster
         9.Shutdown the Machine
         10.Reboot the Machine
         q.Quit to main Menu
```

This menu includes the following options:

- Start/Restart Application .(Start or Restart the Application below
- Stop Application (Stop the Application on page 182)
- Web Servers (Web Servers on page 182)
- Change Schedule Backup Time (Change Schedule Backup Time)
- Restore (OVOC Server Restore on page 158)
- License (License on page 183)
- Analytics API (Analytics API on page 187)
- Service Provider Cluster (Service Provider Cluster on page 188)
- Shutdown the Machine (Shutdown the OVOC Server Machine on page 193)
- Reboot the Machine (Reboot the OVOC Server Machine on page 193)

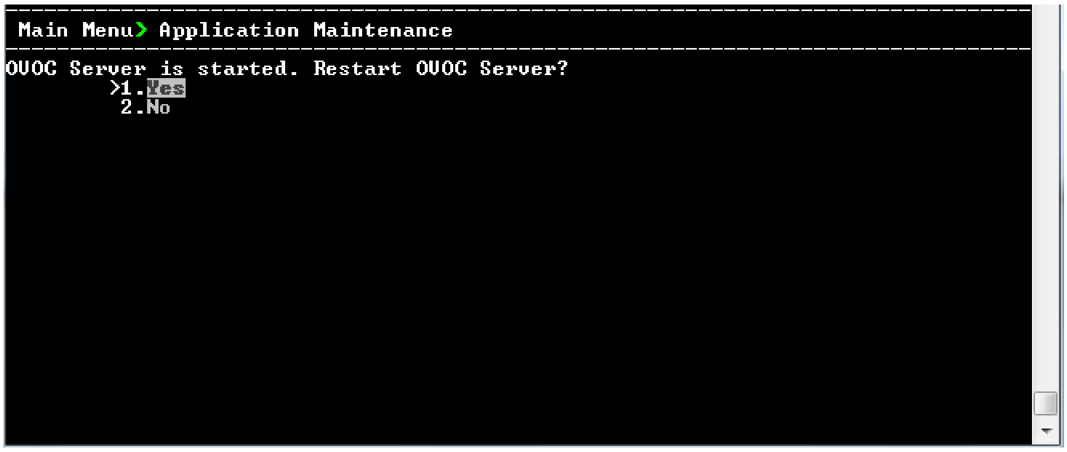
Start or Restart the Application

This section describes how to start or restart the application.

➢ To start/restart the application:

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

Figure 21-2: Start or Restart the OVOC server



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

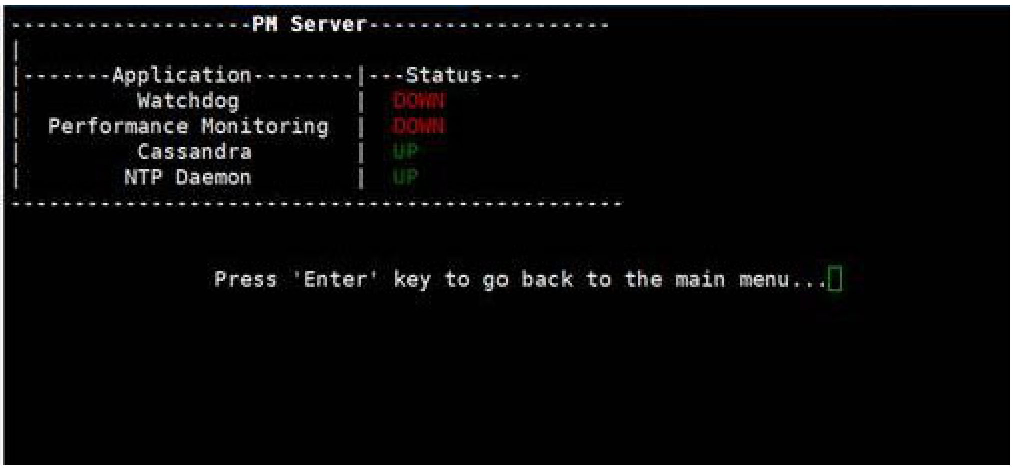
2. Do one of the following:
   - Select **Yes** to start/restart the OVOC server
   - Select **No** to return to menu

Start and Restart in Service Provider Cluster Mode

When running in Service Provider Cluster, the processes statuses following start or restart of the OVOC server are shown in the figures below:

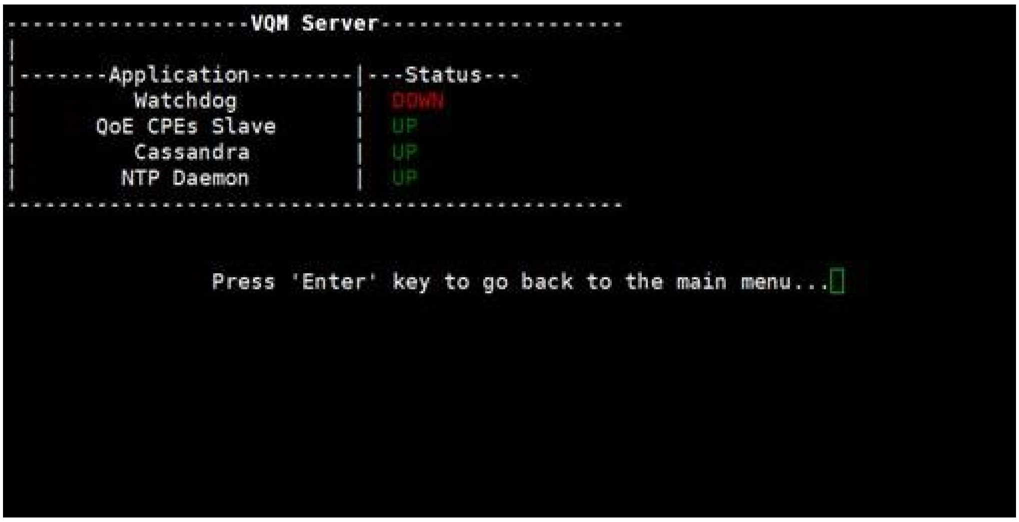
For VQM and PM servers, there is no option in the OVOC Server Manager to stop the server (only the"Restart" action is available).

Figure 21-3: PM Server



```
-------------------PM Server-------------------
|
|-------Application--------|---Status---
|        Watchdog          |  DOWN
|  Performance Monitoring  |  DOWN
|        Cassandra         |  UP
|        NTP Daemon        |  UP
------------------------------------------------


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

Figure 21-4: VQM Server



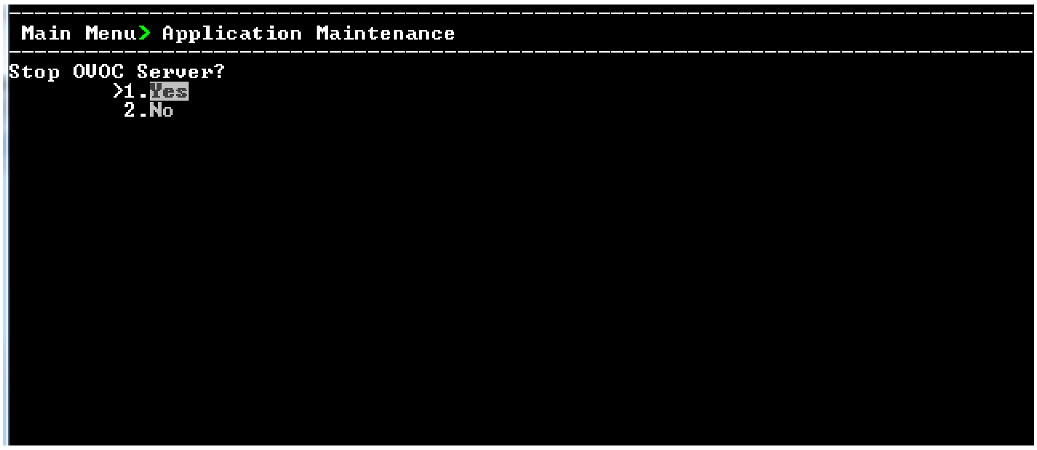
```
------------------VQM Server------------------
|
|-------Application--------|---Status---
|       Watchdog           |  DOWN
|     QoE CPEs Slave       |  UP
|       Cassandra          |  UP
|      NTP Daemon          |  UP
-----------------------------------------------

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

Stop the Application

➢ To stop the application:

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

Figure 21-5: Stop OVOC server



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

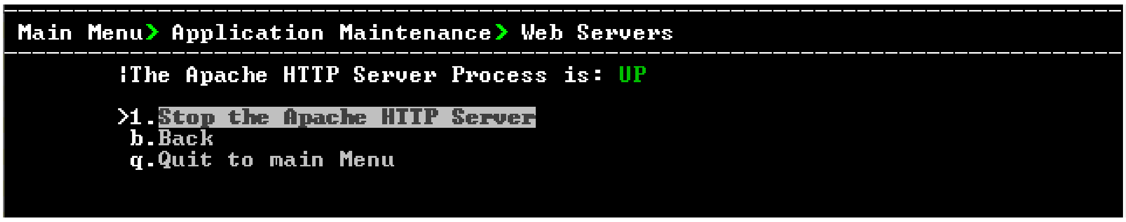
Web Servers

This option enables you to stop and start the Apache HTTP Web server.

➢ To stop/start the Apache HTTP Web server:

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

Figure 21-6: Web Servers



```
Main Menu> Application Maintenance> Web Servers

         !The Apache HTTP Server Process is: UP

         >1.Stop the Apache HTTP Server
          b.Back
          q.Quit to main Menu
```

2. Select option **Stop/Start the Apache HTTP Server**.

Change Schedule Backup Time

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

License

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

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

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

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

- **ProductKey:** the Product Key string is used in the customer order for upgrading the OVOC product. For more information, contact your AudioCodes partner.
- **Machine ID:** indicates the OVOC Machine ID that should be taken from the server as shown in the screen below (enter this ID in the Fingerprint field in the Activation form). This ID is also used in the customer order process when the product key is not known (for more information contact your AudioCodes representative).
- **License Status:** indicates whether the OVOC license is enabled (OVOC License on the next page below).
- **OVOC Advanced:** indicates whether the Voice Quality license is enabled (default-no). When this parameter is set to default, the followingVoice Quality feature licenses are available:
  - Total Devices = 2
  - Total Endpoints = 10
  - Total Sessions = 10
  - Total Users = 10

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

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

  The time zone is determined by the configured date and time in the Date & Time menu (Timezone Settings on page 214).

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

OVOC License

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

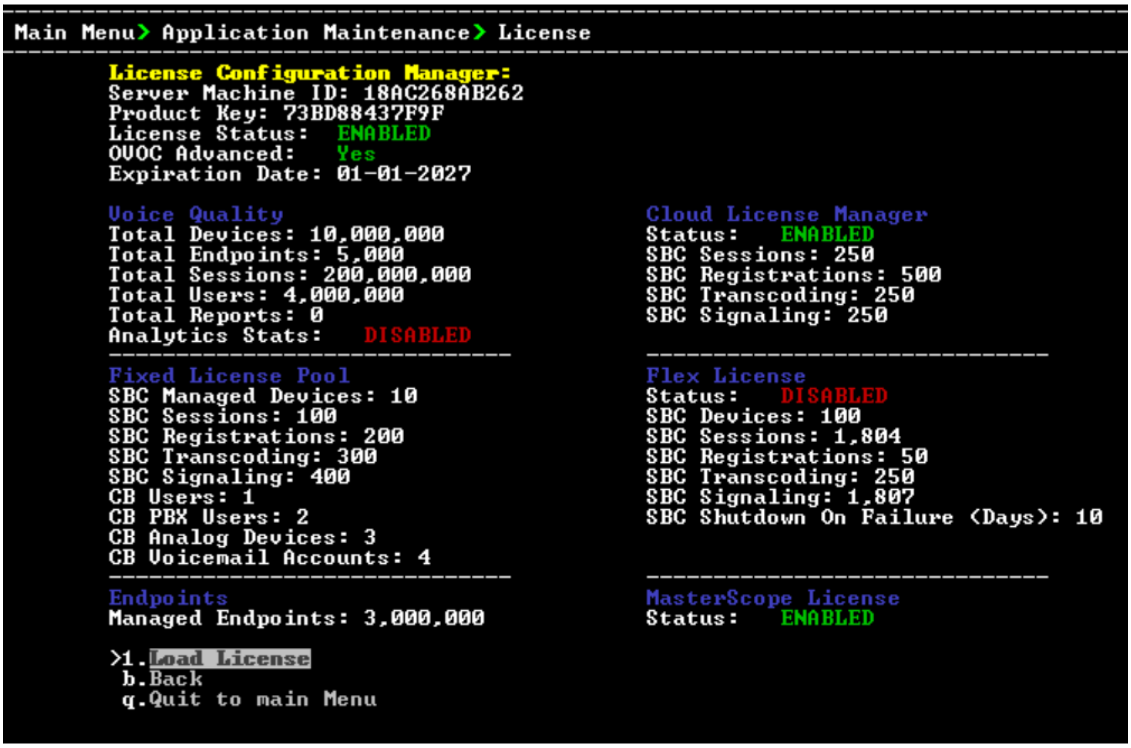
➢ To view the license details or upload a new license:

1. Copy the license file that you have obtained from AudioCodes to the following path on the OVOC server machine:

   /home/acems/<License_File>

2. From the Application Maintenance menu, choose **License** option, and then press Enter; the current License details are displayed:

Figure 21-7: License Manager



```
--------------------------------------------------------------------------------------
Main Menu> Application Maintenance> License
--------------------------------------------------------------------------------------
       License Configuration Manager:
       Server Machine ID: 18AC268AB262
       Product Key: 73BD88437F9F
       License Status:  ENABLED
       OVOC Advanced:   Yes
       Expiration Date: 01-01-2027

       Voice Quality                           Cloud License Manager
       Total Devices: 10,000,000               Status:    ENABLED
       Total Endpoints: 5,000                  SBC Sessions: 250
       Total Sessions: 200,000,000             SBC Registrations: 500
       Total Users: 4,000,000                  SBC Transcoding: 250
       Total Reports: 0                        SBC Signaling: 250
       Analytics Stats:   DISABLED
       ------------------------------          ------------------------------
       Fixed License Pool                      Flex License
       SBC Managed Devices: 10                 Status:    DISABLED
       SBC Sessions: 100                       SBC Devices: 100
       SBC Registrations: 200                  SBC Sessions: 1,804
       SBC Transcoding: 300                    SBC Registrations: 50
       SBC Signaling: 400                      SBC Transcoding: 250
       CB Users: 1                             SBC Signaling: 1,807
       CB PBX Users: 2                         SBC Shutdown On Failure (Days): 10
       CB Analog Devices: 3
       CB Voicemail Accounts: 4
       ------------------------------          ------------------------------
       Endpoints                               MasterScope License
       Managed Endpoints: 3,000,000            Status:    ENABLED

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

Table 21-1: License Pool Parameters

License Type	License Parameter
Floating License	
SBC Sessions	The maximum number of concurrent SBC call sessions.
SBC Registrations	The maximum number of SIP endpoints that can register with the SBC devices.
SBC Transcoding	The maximum number of SBC transcoding sessions.
SBC Signaling	The maximum number of SBC signaling sessions.
FlexPool License	
SBC Devices	The maximum number of SBC devices that can be managed by the FlexPool.
SBC Sessions	The maximum number of concurrent license SBC call sessions.
SBC Registrations	The maximum number of SIP endpoints that can register with the SBC devices
SBC	The maximum number of SBC transcoding sessions.

License Type	License Parameter
Transcoding	
SBC Signaling	The maximum number of SBC signaling sessions
SBC Shutdown on Failure (Days) Default:-90 days	When an SBC device does not receive acknowledgment from the OVOC server that Usage reports have been received within the specified grace period, then service is shutdown for this SBC device. The SBC must then re-establish connection with the OVOC server.
Fixed License Pool	
SBC Managed Devices	The total number of devices that can be managed by the Fixed License Pool.
SBC Registrations	The number of SIP endpoints that can register with the SBC devices.
SBC Sessions	The maximum number of concurrent license SBC call sessions
SBC Signaling	The maximum number of SBC signaling sessions
SBC Transcoding	The maximum number of SBC transcoding sessions
CB Users	The maximum number of CloudBond 365 users
CB PBX Users	The maximum number of PBX users. Currently not supported.
CB Analog Devices	The maximum number of CB Analog devices. Currently not supported.
CB Voicemail Accounts	The maximum number of CB Voicemail accounts. Currently not supported.
Endpoints	
Devices	The maximum number of endpoints that can be managed by the Device Manager Pro.
Voice Quality	
Total Devices	The maximum number of Voice Quality monitored devices.
Total Endpoints	The maximum number of Voice Quality monitored endpoints.
Total Sessions	The maximum number of concurrent Voice Quality monitored SBC call sessions.

License Type	License Parameter
Total Users	The maximum number of Voice Quality monitored users supported by the SBC. ⚠ ● A license value higher than 10 must be purchased to enable adding Skype for Business devices in the OVOC Web interface. ● For customers with existing Skype for Business devices defined in OVOC with 10 or fewer licenses , there are no changes; however, new Skype for Business devices cannot be added.
Total Reports	The maximum number of customized Voice Quality reports that can be generated in OVOC. ⚠ ● Template reports can be generated without purchasing licenses; however, to generate customized reports, licenses must be purchased. These licenses can be allocated to tenant or system operators in the OVOC Web interface. ● **For OVOC upgrades prior to version 7.8 releases:** OVOC migrates old Scheduled reports as Custom reports even if there are insufficient licenses; however, the operator will not be able to add additional Custom reports even if they delete existing reports until the Custom Reports count is below the Total Reports license value.
Analytics Stats	Enables the Analytics API feature for retrieving Voice Quality data from Northbound Database access clients. By default disabled when OVOC Advanced package is enabled.
Masterscope	
MasterScope License	Enables Single Sign-on to the MasterScope network equipment analysis application from the OVOC Web interface.

3. To load a new license, choose option **1**.

4. Enter the license file path and name.

5. Restart the OVOC server.

Analytics API

The Analytic API enables access to selected data from the OVOC database for the purpose of integration into Northbound third-party interfaces. Customers can connect to the OVOC Database using third-party DB access clients and retrieve topology and statistics. This data can then be used in management interfaces such as Power BI, Splunk and other Analytic tools to generate customized dashboards, reports and other representative management data. This may be particularly useful during management reporting periods. The following data can be retrieved:

- Network Topology including Tenants, Regions, Devices, Non-ACL Devices, Links
- QoE Statistics including Calls, Nodes and Links Summaries
- Active and History Alarms

A dedicated DB operator ("Analytics") is used for securing connection to the OVOC server over port 1521. This port must be open on the customer firewall once this feature is enabled by the feature key (seeOVOC License on page 184) and in the procedure described below.

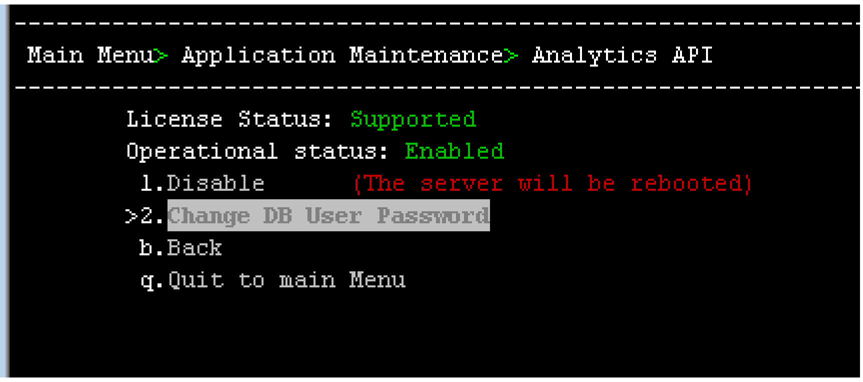
For more information, refer to the *OVOC Northbound Integration Guid*e.

➢ To manage the Analytics API:

1. From the Application Maintenance menu, choose **Analytics API**.

   The License status indicates whether the license feature is enabled and the Operational status indicates whether this option is enabled.

Figure 21-8: Analytics API



```
-------------------------------------------------------------
 Main Menu> Application Maintenance> Analytics API
-------------------------------------------------------------
        License Status: Supported
        Operational status: Enabled
         1.Disable      (The server will be rebooted)
        >2.Change DB User Password
         b.Back
         q.Quit to main Menu
```

Once enabled, an option "Change DB User Password" to change the default authentication password for the Analytics user connection appears in the menu. Enter the desired password and confirm.

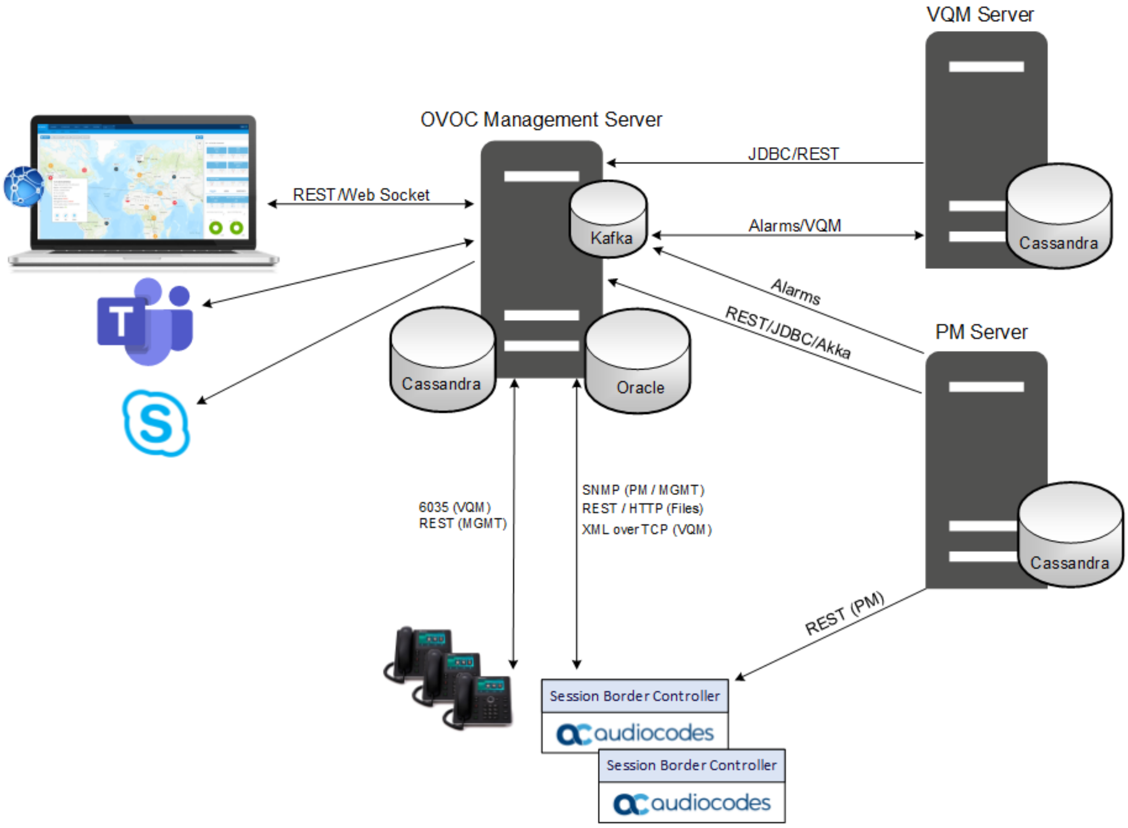
Service Provider Cluster

The Service Provider Cluster mode enables load sharing between Voice Quality and Performance Monitoring and General Management processes with a separate Virtual Machines for each process.

> Service Provider Cluster setup is released in this version as a Controlled Introduction feature. When customers are ready to deploy this feature, contact the AudioCodes OVOC Product Manager to coordinate an initial interview session.

The figure below illustrates the topology.

Figure 21-9: Service Provider Cluster



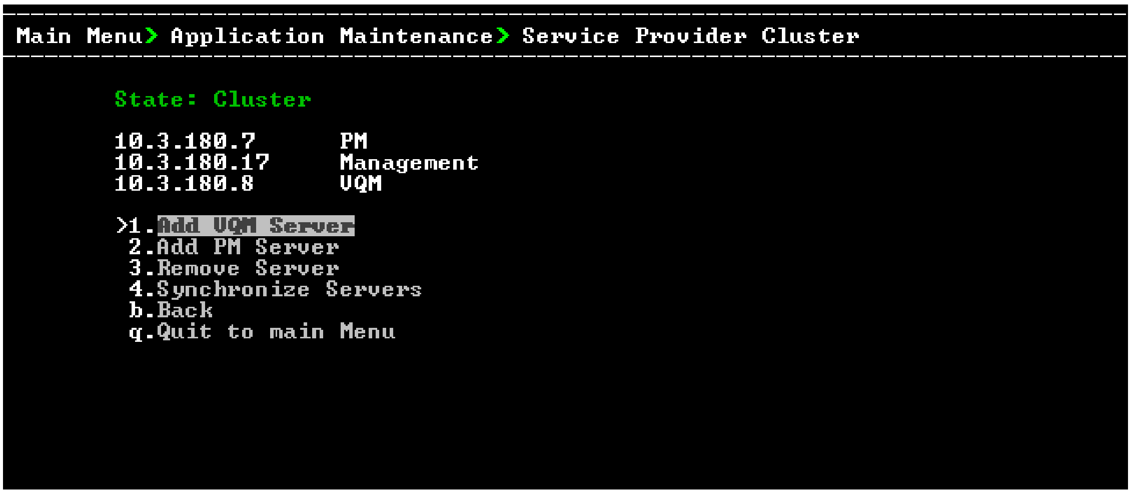
- The Cassandra database for managing Call Details, SIP Ladder messages and PM Details runs in a Cluster mode on each of the following nodes: Management; VQM and PM servers.
- The QoE CPEs server process for managing the XML-based Voice Quality Package communication with managed devices runs as a sub-process on the VQM server.
- The Performance Monitoring process for polling managed devices runs as a sub-process on the Performance Monitoring Slave server.
- Alarms are sent from the node servers to the Management server using Kafka

The procedure below describes how to configure the cluster nodes and to perform synchronization between the configured cluster nodes and the management server.

➢ To configure service provider cluster:

1. From the Application Maintenance menu, choose **Service Provider Cluster**.

Figure 21-10: Service Provider Cluster



```
Main Menu> Application Maintenance> Service Provider Cluster

        State: Cluster

        10.3.180.7       PM
        10.3.180.17      Management
        10.3.180.8       VQM

        >1.Add VQM Server
         2.Add PM Server
         3.Remove Server
         4.Synchronize Servers
         b.Back
         q.Quit to main Menu
```

2. Select option 'Add VQM Server' to add a virtual machine for a VQM Server:
   - Enter the server's IP address and confirm.
3. Select option 'Add PM Server' to add a virtual machine for a PM Server:
   - Enter the server's IP address and confirm.

- The server that you wish to add must be connected to the network
- The OVOC server must be pre-installed on the PM/VQM server (see OVOC Software Deliverables on page 15)
- The Management server clock must be synchronized with the PM/VQM clock.

Remove PM or VQM Server from Cluster

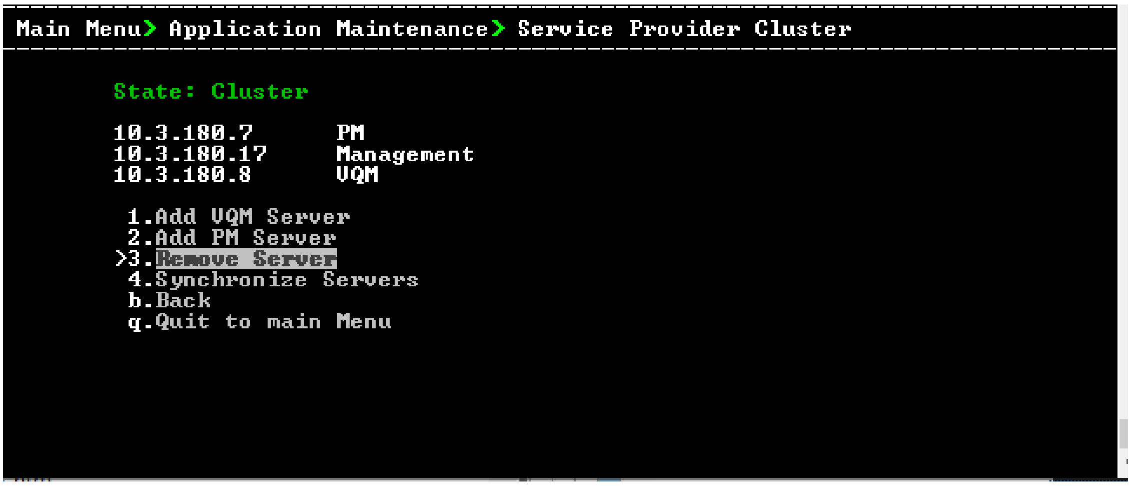
This section describes how to remove a PM or VQM server from the Service Provider Cluster. This scenario occurs when this server is connected to the cluster and needs to be removed (its data is synchronized with other servers in the network).

- Before performing this action, its recommended to backup from cluster (see OVOC Server Backup Processes on page 156).
- The server removal process is time-consuming due mainly to the data redistribution process.
- Make sure that the PM/VQM server is connected and running before removing it.

➢ To remove PM or VQM server from the cluster:

1. From the Service Provider Cluster menu, choose **Remove Server**.

Figure 21-11: Removing PM/VQM Server



```
Main Menu> Application Maintenance> Service Provider Cluster

        State: Cluster

        10.3.180.7       PM
        10.3.180.17      Management
        10.3.180.8       VQM

         1.Add VQM Server
         2.Add PM Server
        >3.Remove Server
         4.Synchronize Servers
         b.Back
         q.Quit to main Menu
```

Force Remove PM or VQM Server from Cluster

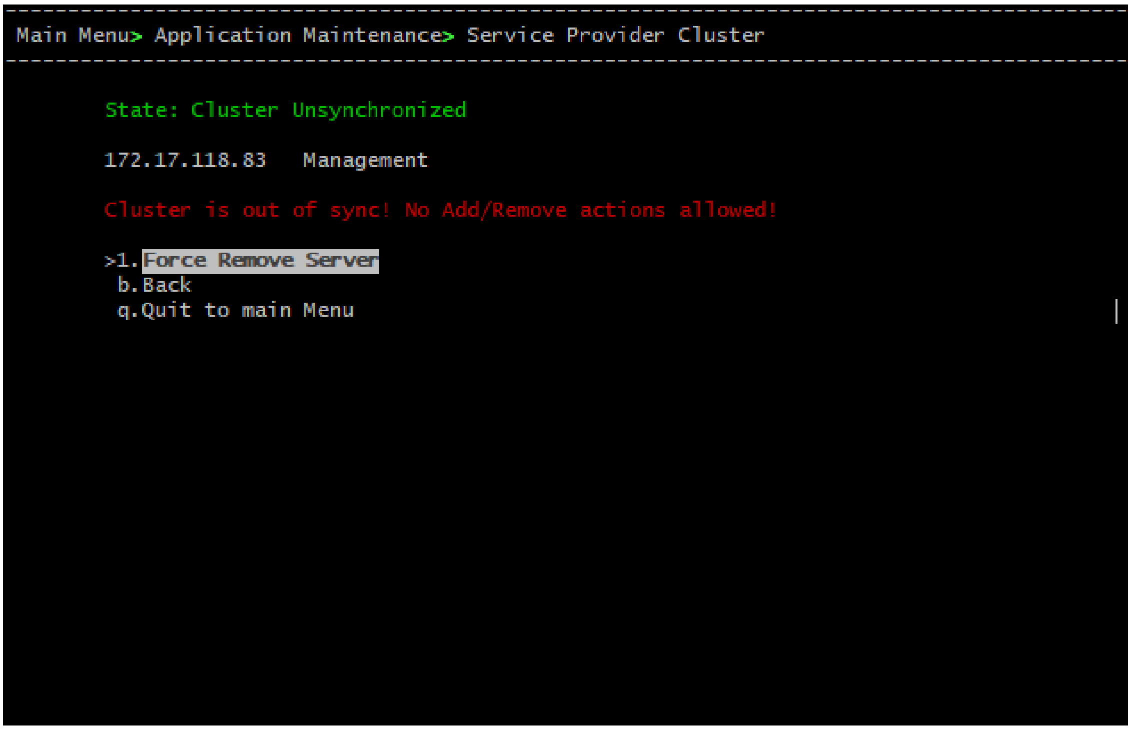
This section describes how to force remove a PM or VQM server from the Service Provider Cluster. This scenario occurs when this server is not connected and its data cannot be synchronized and you wish to remove it from the cluster.

- Before performing this action, its recommended to backup from cluster (see OVOC Server Backup Processes on page 156).
- Data may be lost since removed server data cannot be redistributed.

➢ **To force remove a node from the service provider cluster:**

1. From the Service Provider Cluster menu, choose **Force Remove Server**.

Figure 21-12: Removing Slave Server



```
Main Menu> Application Maintenance> Service Provider Cluster

       State: Cluster Unsynchronized

       172.17.118.83   Management

       Cluster is out of sync! No Add/Remove actions allowed!

       >1.Force Remove Server
        b.Back
        q.Quit to main Menu
```

Synchronize Cluster Node Servers

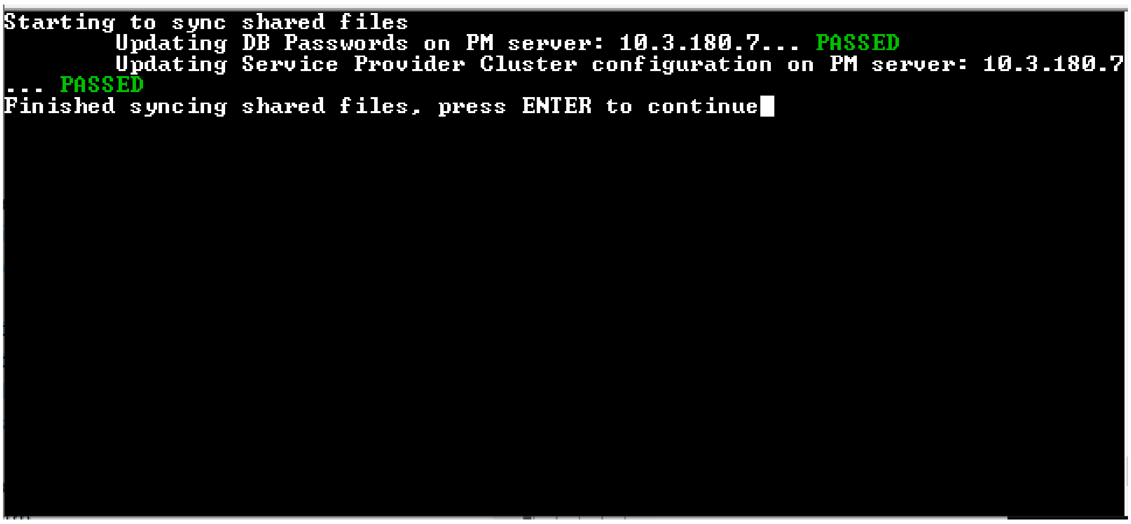
The synchronization option performs sync on the shared files in the cluster configuration including DB passwords and server configurations.

➢ To synchronize cluster node servers:

1. From the Service Provider Cluster menu, choose **Synchronize Servers.**

   Shared files in the cluster are updated.

Figure 21-13: Synchronize Cluster Mode



```
Starting to sync shared files
        Updating DB Passwords on PM server: 10.3.180.7... PASSED
        Updating Service Provider Cluster configuration on PM server: 10.3.180.7
... PASSED
Finished syncing shared files, press ENTER to continue
```

Shutdown the OVOC Server Machine

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

⚠ When operating in the Service Provider Cluster Mode, enabling this option shuts down the entire cluster.

➢ To shut down the OVOC server machine:

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

Reboot the OVOC Server Machine

This section describes how to reboot the OVOC server machine.

➢ To reboot the OVOC server machine:

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

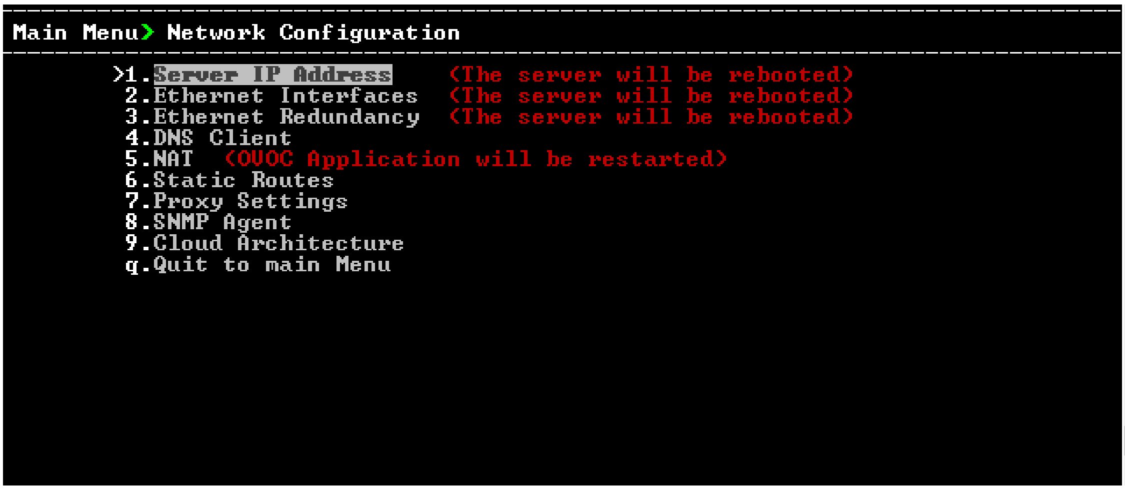
22 Network Configuration

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

➢ To run the network configuration:

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

Figure 22-1: 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  (OVOC Application will be restarted)
         6.Static Routes
         7.Proxy Settings
         8.SNMP Agent
         9.Cloud Architecture
         q.Quit to main Menu
```

This menu includes the following options:

- Server IP Address (the server will be rebooted) (Server IP Address on the next page)
- Ethernet Interfaces (the server will be rebooted) (Ethernet Interfaces on page 196)
- Ethernet Redundancy (the server will be rebooted) (Ethernet Redundancy on page 200)
- DNS Client (DNS Client on page 204)
- NAT (Configure OVOC Server with Public or NAT IP Address on page 114)
- Static Routes (Static Routes on page 205)
- OVOC Proxy Settings (Proxy Settings on page 206)
- SNMP Agent (SNMP Agent on page 207)
- Cloud Architecture (Configure OVOC Cloud Architecture Mode on page 115)

The following options are not applicable in Cloud deployments:

- Server IP Address
- Ethernet interfaces
- Ethernet redundancy

Server IP Address

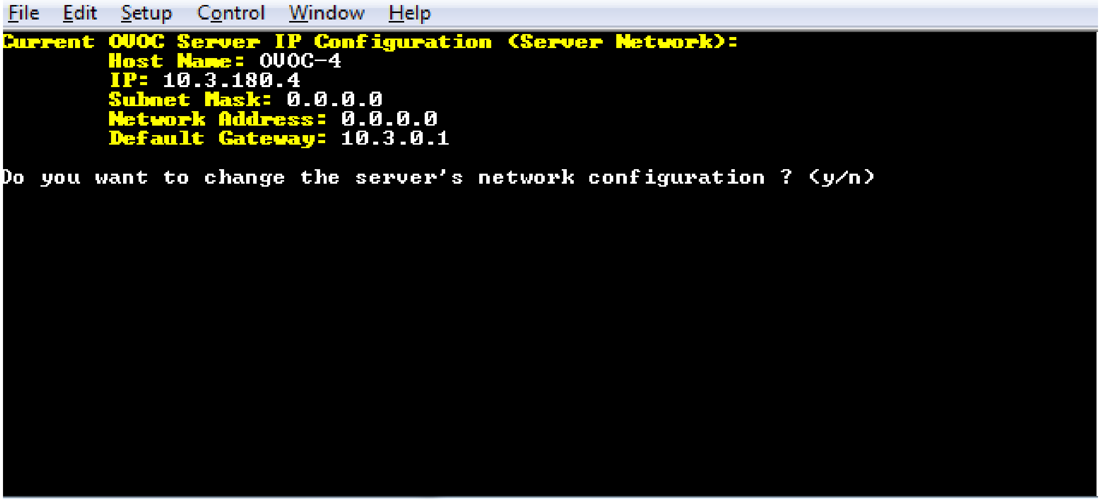
This option enables you to update the OVOC server's IP address. This option also enables you to modify the OVOC server host name.

- When this operation has completed, the OVOC automatically reboots for the changes to take effect.
- **When configuring PM and VQM servers:** this option can only be applied before adding these servers to the cluster.

➢ 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 22-2: OVOC Server Manager – Change Server's IP Address



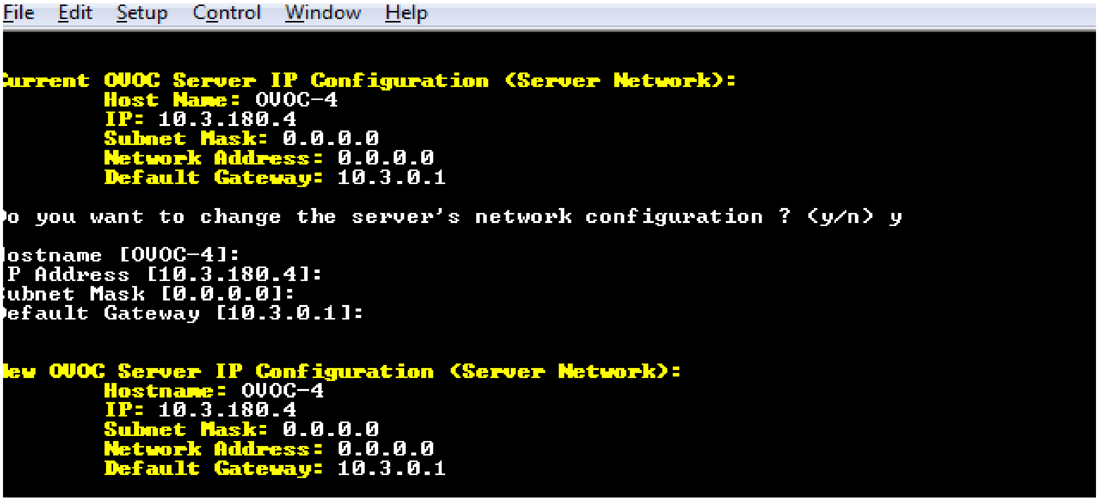
```
Current OVOC Server IP Configuration (Server Network):
        Host Name: OVOC-4
        IP: 10.3.180.4
        Subnet Mask: 0.0.0.0
        Network Address: 0.0.0.0
        Default Gateway: 10.3.0.1

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 22-3: IP Configuration Complete



```
urrent 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

o you want to change the server's network configuration ? (y/n) y

ostname [OVOC-4]:
P Address [10.3.180.4]:
ubnet Mask [0.0.0.0]:
efault Gateway [10.3.0.1]:

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

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

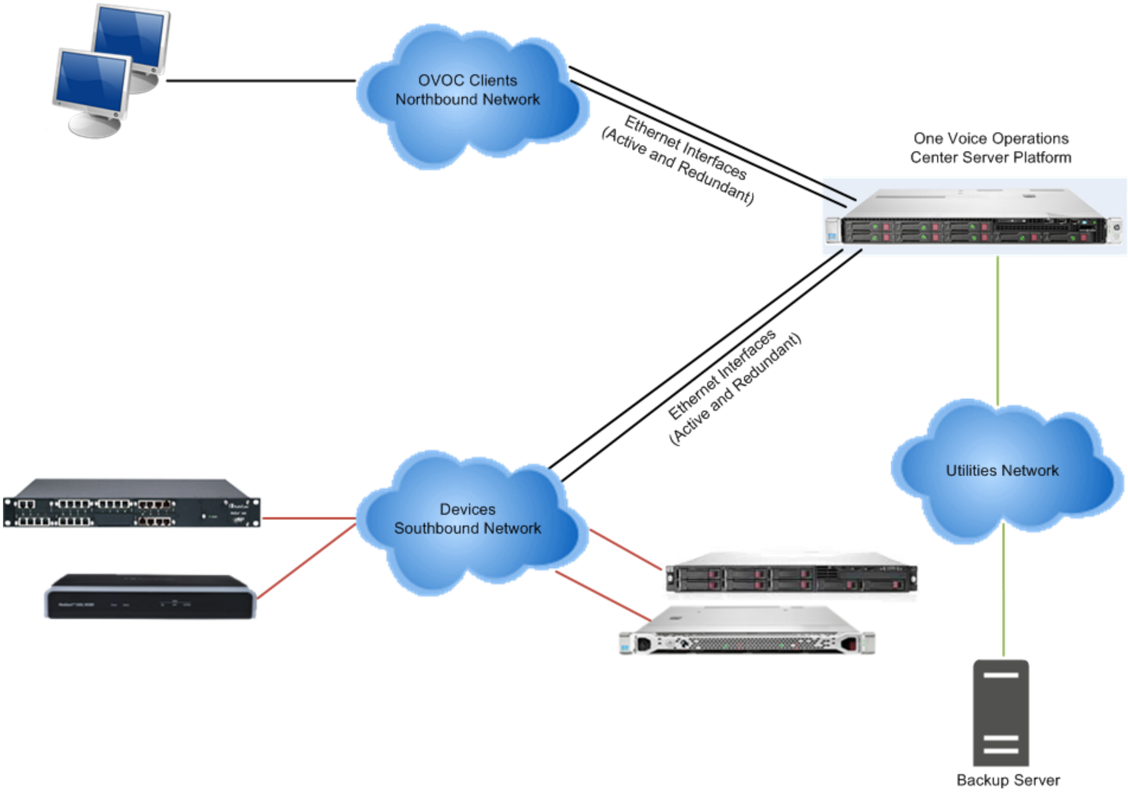
Ethernet Interfaces

This section describes how to configure Ethernet interfaces.

OVOC Client Login on all OVOC Server Network Interfaces

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

Figure 22-4: OVOC server: Triple Ethernet Interfaces



In case gateways are located in different subnets, static routes should be provisioned to allow the connection from 'Southbound Network' to each one of the subnets. For Static Routes configuration, Static Routes on page 205.

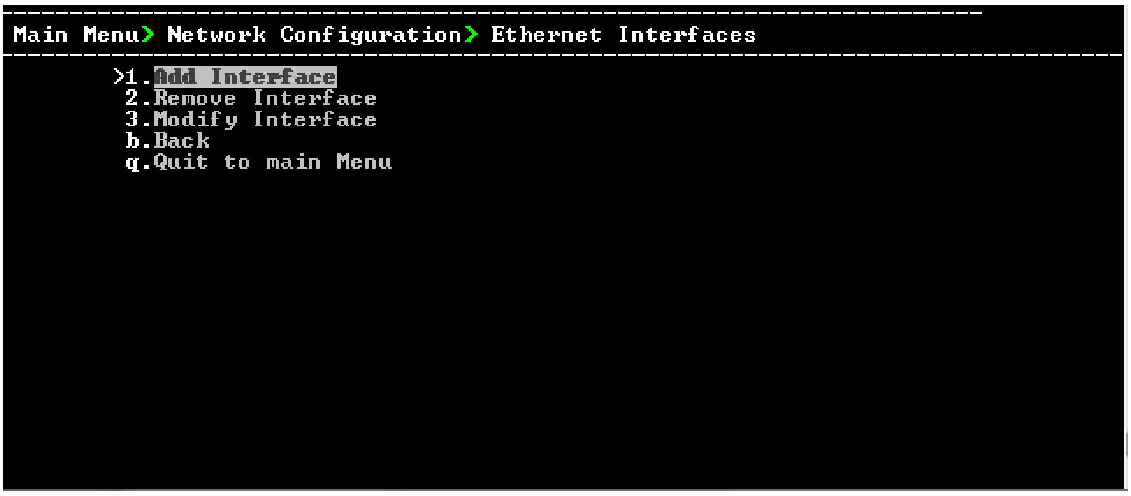
To ensure that the network configuration is performed successfully, test that the OVOC is successfully connected to each one of the gateways by running the following basic tests:

- 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 22-5: OVOC 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 (Add Interface below).
- **Remove Interface** – Removes an existing interface from the OVOC server (Remove Interface on the next page).
- **Modify Interface** – Modifies an existing interface from the OVOC server (Type y to confirm the changes; the OVOC server automatically reboots for the changes to take effect. on the next page).

Add Interface

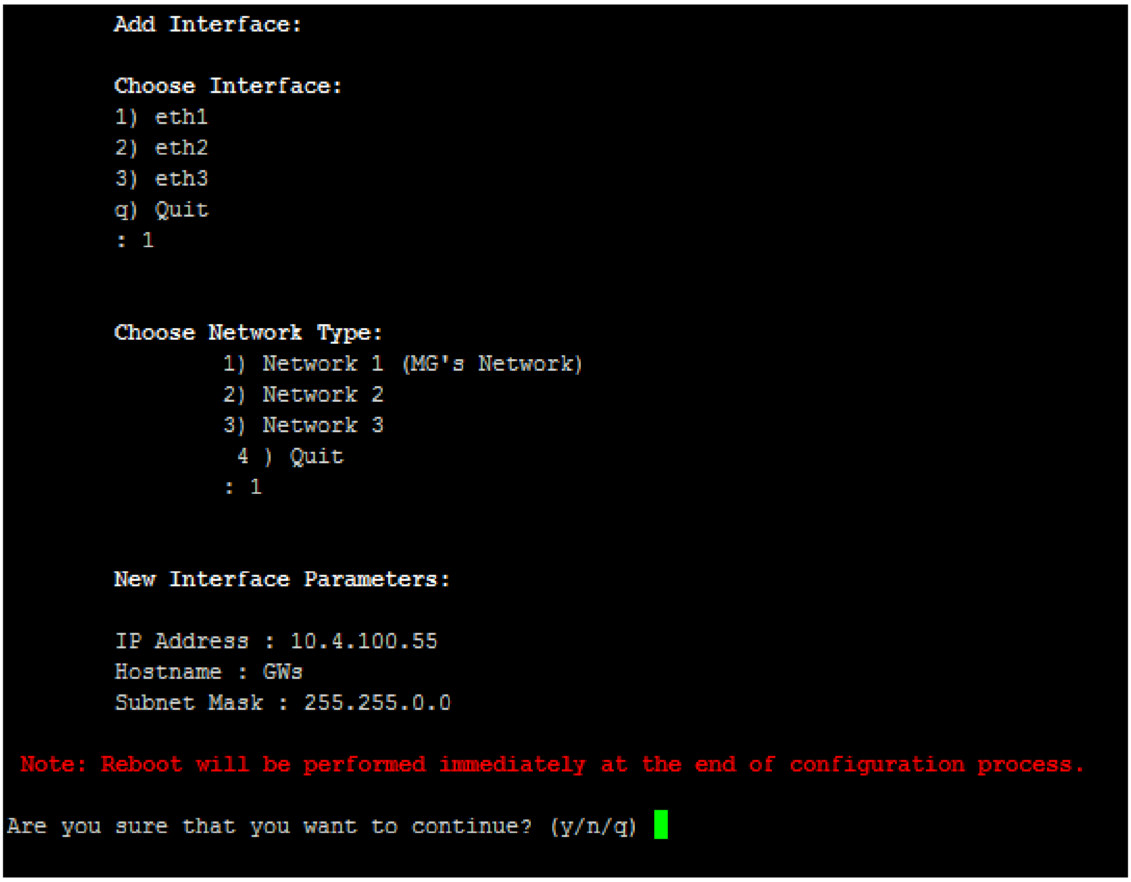
This section describes how to add a new interface.

➢ To add a New Interface:

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

   The new interface parameters are displayed.
5. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Figure 22-6: Add Interface Parameters



```
        Add Interface:

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


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


        New Interface Parameters:

        IP Address : 10.4.100.55
        Hostname : GWs
        Subnet Mask : 255.255.0.0

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

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

Remove Interface

This section describes how to remove an interface.

➢ To remove an existing interface:

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

Modify Interface

This section describes how to modify an existing interface.

➢ To modify an existing interface:

1. From the Ethernet Interfaces menu, choose option **3**.
2. Choose the interface to modify; the following is displayed:
3. Change the interface parameters.

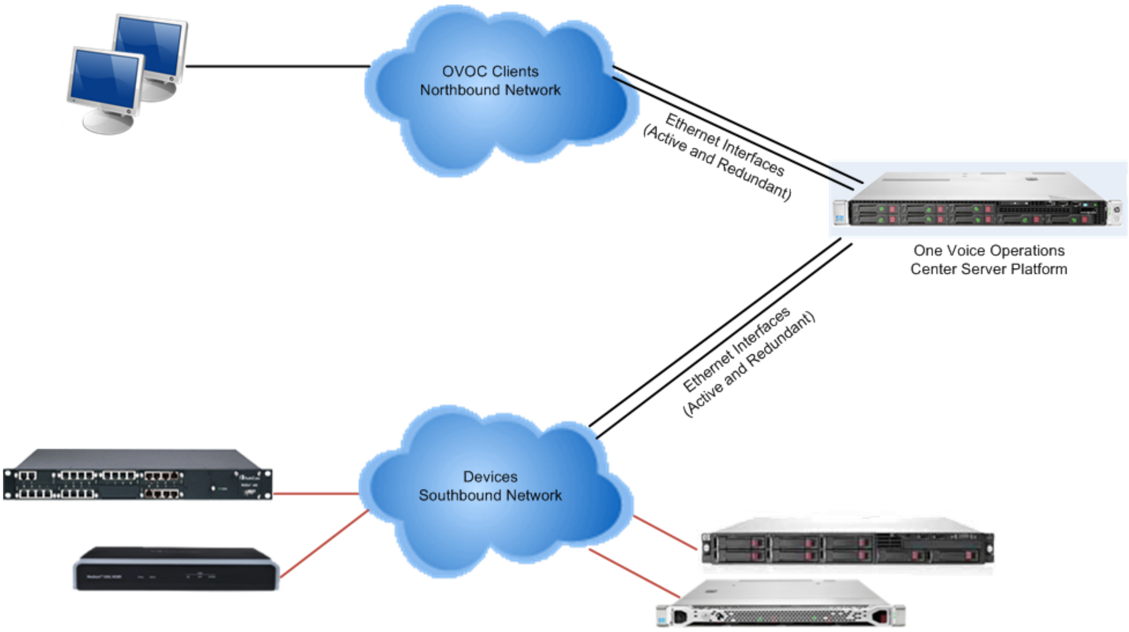
4. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Ethernet Redundancy

This section describes how to configure Ethernet Redundancy. Physical Ethernet Interfaces Redundancy provides failover when you have multiple network interface cards that are connected to the same IP link. The OVOC server supports up to four Ethernet interfaces. For enhanced network security, it is recommended to use two interfaces and to define Ethernet ports redundancy on both of them. For example, OVOC Clients [Northbound] and Gateways [Southbound]). This option enables you to configure Ethernet ports redundancy.

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

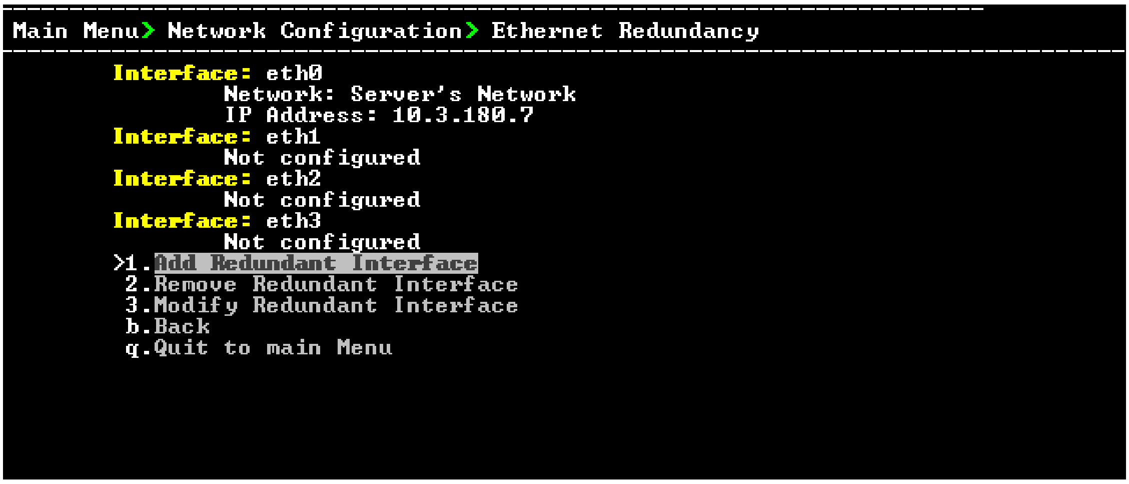
Figure 22-7: Physical Ethernet Interfaces Redundancy



➢ **To configure Ethernet Redundancy:**

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

Figure 22-8: Ethernet Redundancy Configuration



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

2. This menu includes the following options:

- Add Redundant Interface (Add Redundant Interface below).
- Remove Redundant Interface (Remove Ethernet Redundancy on the next page).
- Modify Redundant Interface (Modify Redundant Interface on page 203).

Add Redundant Interface

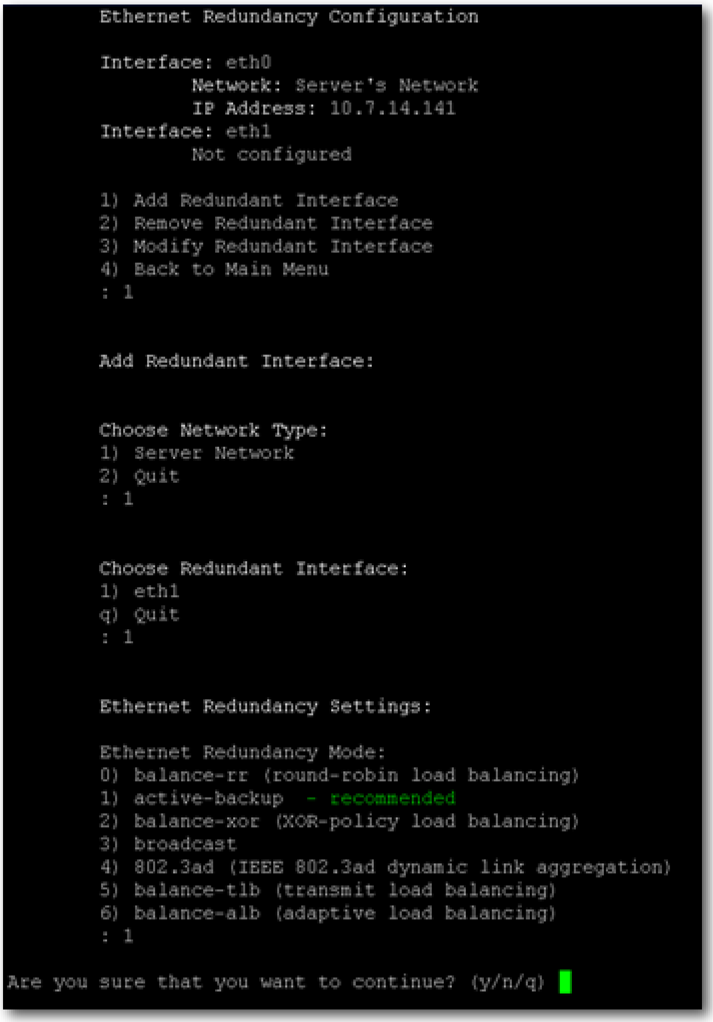
Remove a redundant interface under the following circumstances:

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

➢ To add a redundant interface:

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

Figure 22-9: Add Redundant Interface



```
        Ethernet Redundancy Configuration

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

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


        Add Redundant Interface:


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


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


        Ethernet Redundancy Settings:

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

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

Remove Ethernet Redundancy

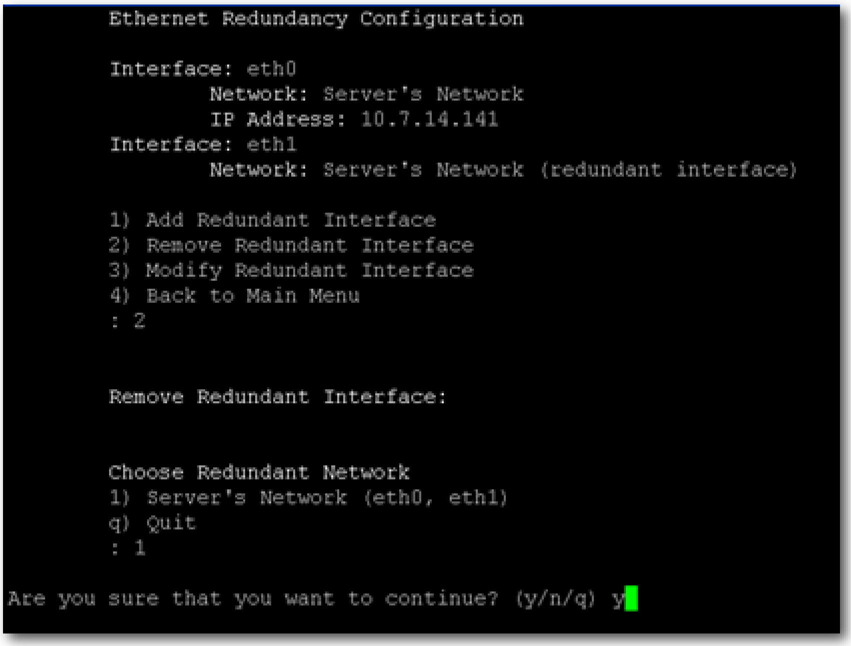
This section describes how to remove an Ethernet redundancy interface.

➢ To remove the Ethernet Redundancy interface:

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

   The current Ethernet redundancy configuration is displayed.
3. Type **y** to confirm the changes; the OVOC server automatically reboots for the changes to take effect.

Figure 22-10: Ethernet Redundancy Interface to Disable



```
        Ethernet Redundancy Configuration

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

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


        Remove Redundant Interface:


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

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

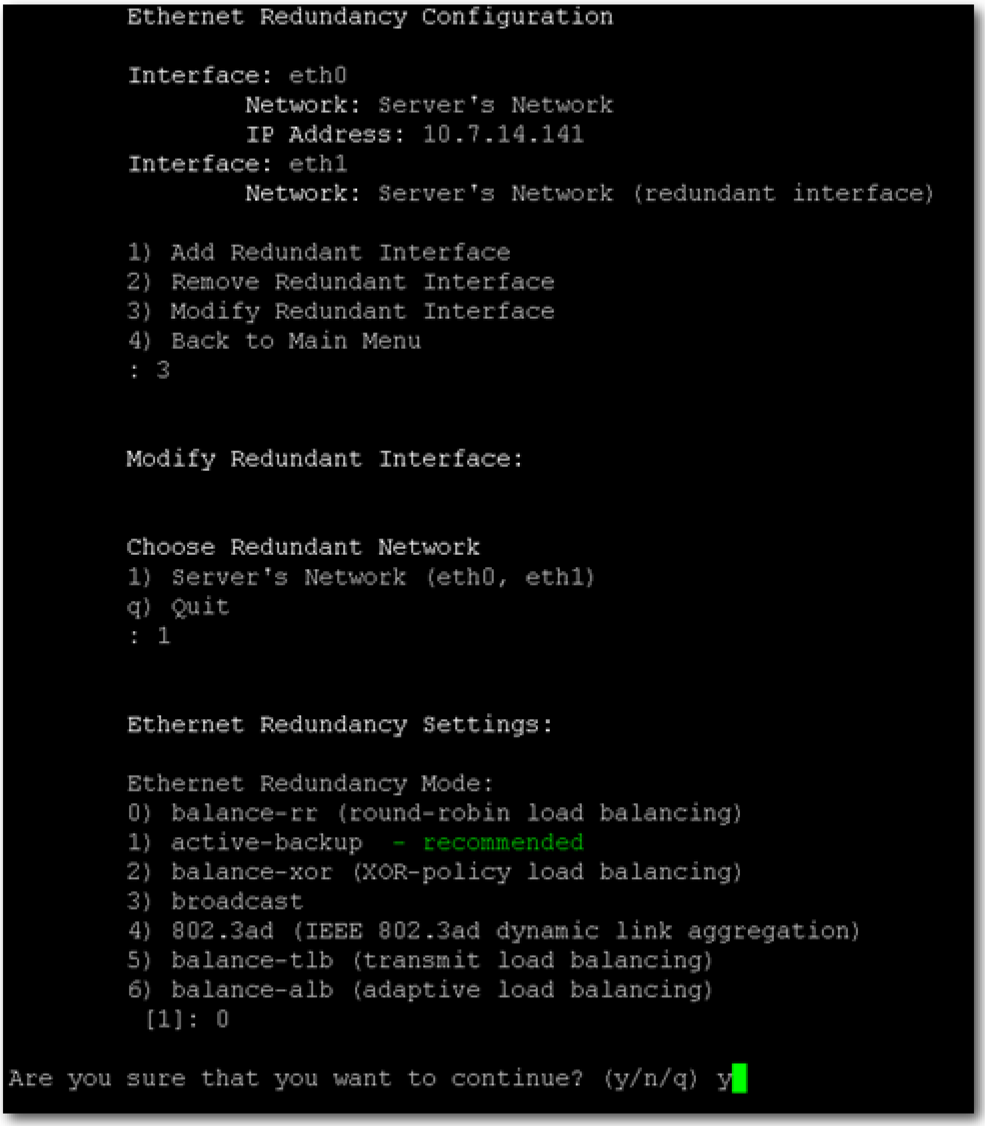
Modify Redundant Interface

This section describes how to modify a redundant interface.

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

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

Figure 22-11: Modify Redundant Interface



```
      Ethernet Redundancy Configuration

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

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


      Modify Redundant Interface:


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


      Ethernet Redundancy Settings:

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

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

DNS Client

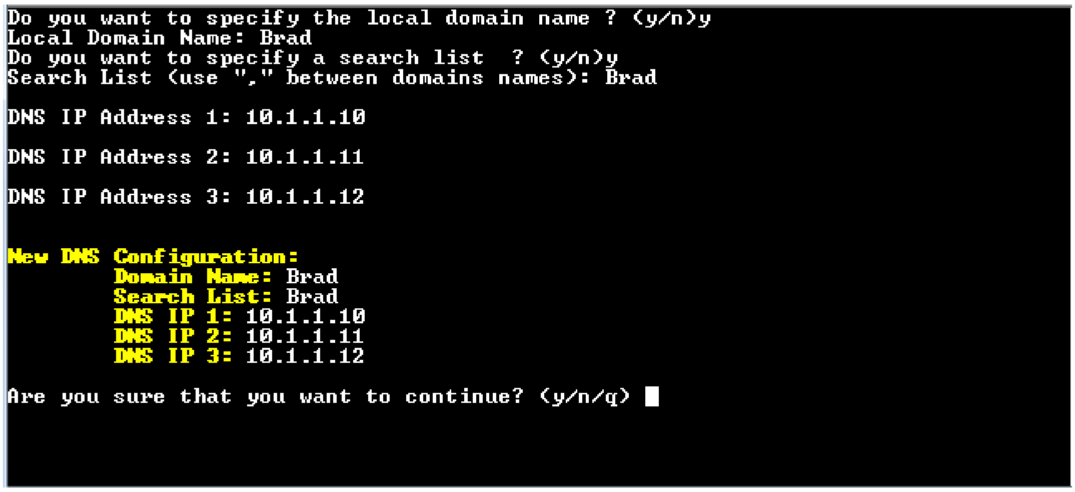
Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address. If a DNS server cannot fulfill your request, it refers the request to another DNS server - and the request is passed along until the domain-name-to-IP-address match is made.

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

➢ To Configure the DNS Client:

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

Figure 22-12: DNS Setup



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

DNS IP Address 1: 10.1.1.10

DNS IP Address 2: 10.1.1.11

DNS IP Address 3: 10.1.1.12


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

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

2. Specify the location domain. Type **y** to specify the local domain name or type **n**, and then press Enter.

3. Specify a search list; type **y** to specify a list of domains (use a comma delimiter to separate search entries in the list) or type **n**, and then press Enter.

4. Specify DNS IP addresses **1, 2** and **3**.

5. Type **y** to confirm your configuration; the new configuration is displayed.

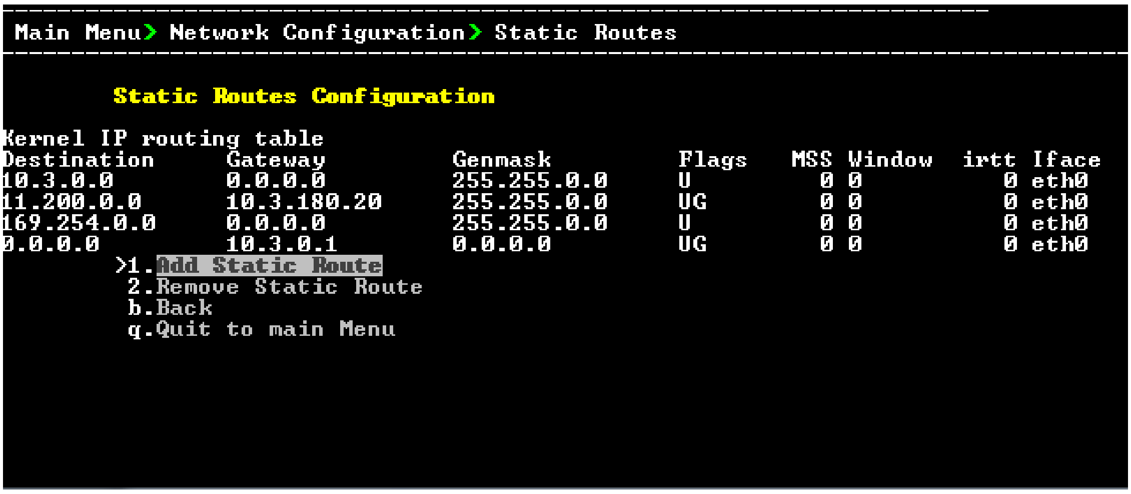
Static Routes

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 22-13: Routing Table and Menu



```
 Main Menu> Network Configuration> Static Routes

        Static Routes Configuration

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

2. From the Static Routes configuration screen, choose one of the following options:
   - Add a Static Route
   - Remove a Static Route

➢ To add a static route:

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

➢ To remove a static route:

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

Proxy Settings

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

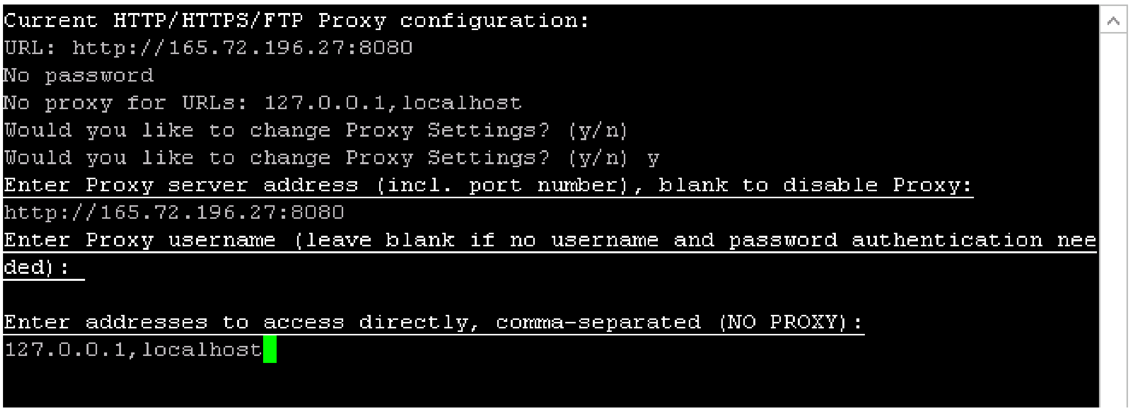
➢ To configure proxy settings:

1. From the Network Configuration menu, choose **Proxy Settings**.
2. Select **Configure Proxy**, and confirm that you wish to configure the HTTP/HTTPS/FTP Proxy server.
3. Enter the FQDN (without underscores), IP address and port of the proxy server.

4. Enter the Proxy username and password.

5. Enter "No Proxy" addresses (a list of IP addresses for connecting directly from OVOC and not through a proxy server).

Figure 22-14: Proxy Settings



```
Current HTTP/HTTPS/FTP Proxy configuration:
URL: http://165.72.196.27:8080
No password
No proxy for URLs: 127.0.0.1,localhost
Would you like to change Proxy Settings? (y/n)
Would you like to change Proxy Settings? (y/n) y
Enter Proxy server address (incl. port number), blank to disable Proxy:
http://165.72.196.27:8080
Enter Proxy username (leave blank if no username and password authentication nee
ded):

Enter addresses to access directly, comma-separated (NO PROXY):
127.0.0.1,localhost
```

HTTPS Proxy server is currently not supported.

SNMP Agent

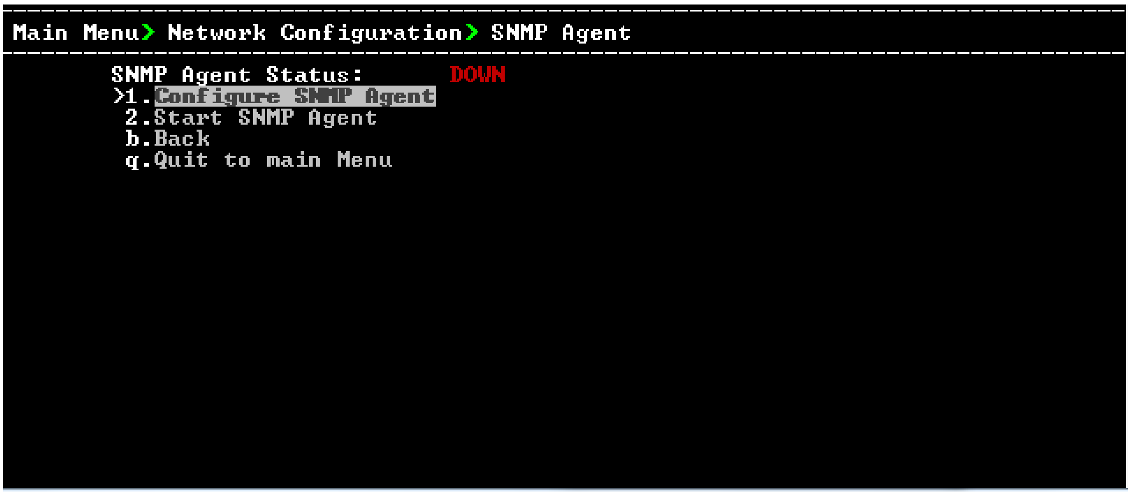
The SNMP Management agent enables access to system inventory and monitoring and provides support for alarms using the industry standard management protocol: Simple Network Management Protocol (SNMP). This agent serves OVOC, NMS, or higher level management system synchronization. This menu includes the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

- Stop and start the SNMP agent
- Configure the SNMP agent including:
  - Configure the SNMP agent listening port (SNMP Agent Listening Port on the next page)
  - Configure the northbound destination for linux system traps forwarding (Linux System Trap Forwarding Configuration on page 209).
  - Configure the SNMPv3 Engine ID (Server SNMPv3 Engine ID on page 209)

➢ **To configure SNMP Agent:**

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

Figure 22-15: SNMP Agent



```
Main Menu> Network Configuration> SNMP Agent

          SNMP Agent Status:        DOWN
         >1.Configure SNMP Agent
          2.Start SNMP Agent
          b.Back
          q.Quit to main Menu
```

The SNMP Agent status is displayed.

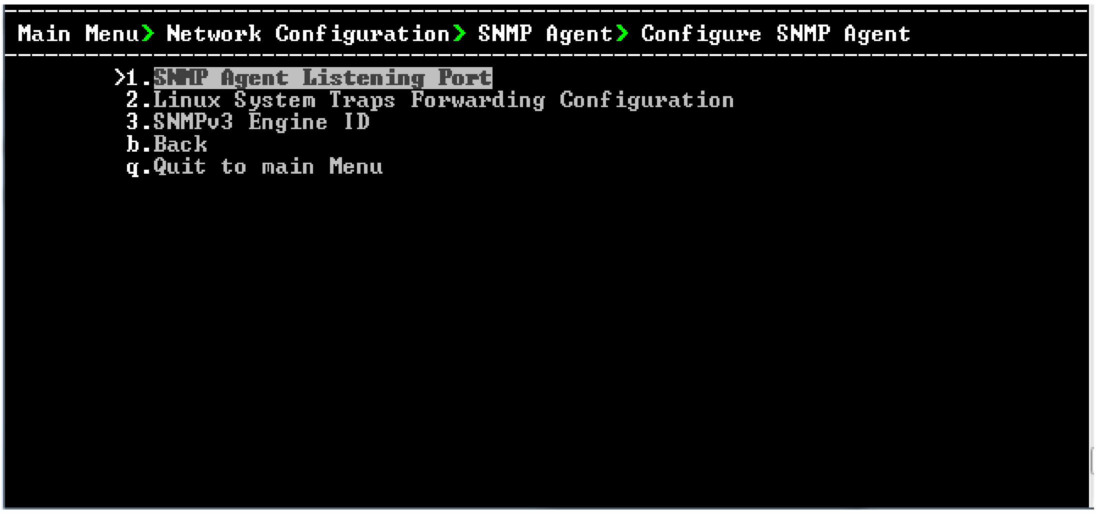
➢ **To start the SNMP Agent:**

- Choose option **2**.

➢ **To configure SNMP Agent:**

1. Choose option **1**.

Figure 22-16: Configure SNMP Agent



```
Main Menu> Network Configuration> SNMP Agent> Configure SNMP Agent

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

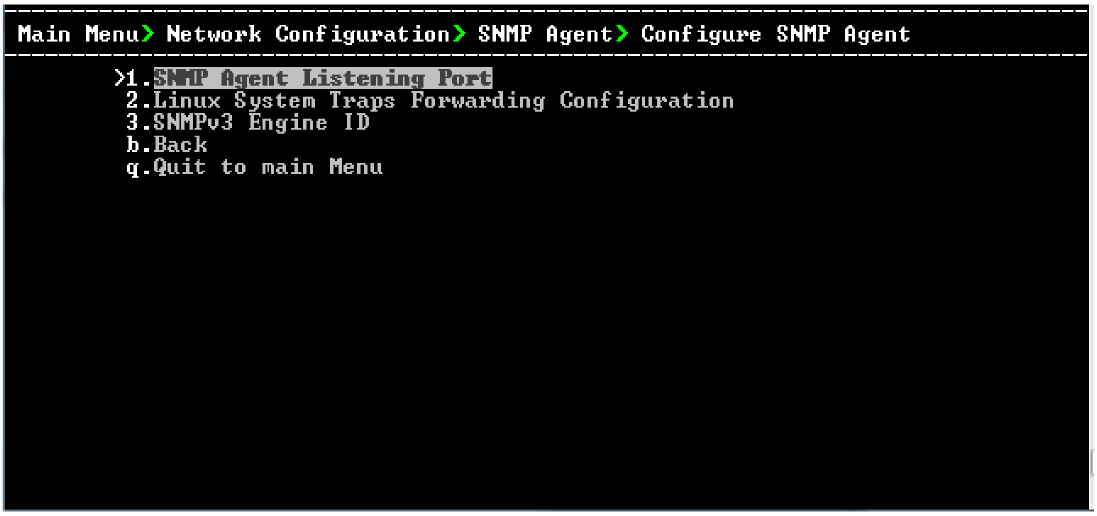
SNMP Agent Listening Port

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

➢ **To configure SNMP Agent Listening port**

1. Choose option **1**.

Figure 22-17: SNMP Agent Listening Port



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

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

Linux System Trap Forwarding Configuration

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

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

1. Choose option **2**.
2. Configure the NMS IP address.
3. Enter the Community string; the new configuration is applied.

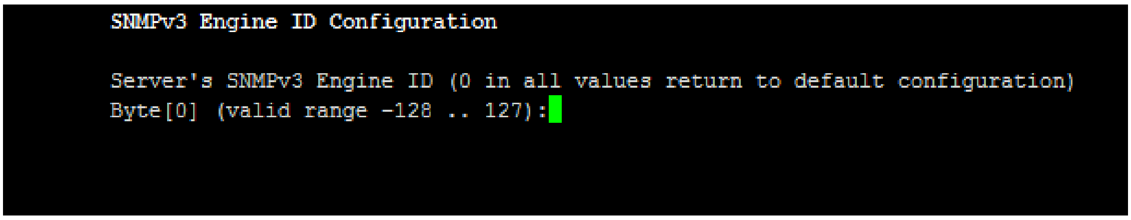
Server SNMPv3 Engine ID

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

➢ **To configure the SNMPv3 Engine ID:**

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

Figure 22-18: OVOC Server Manager – Configure SNMPv3 Engine ID

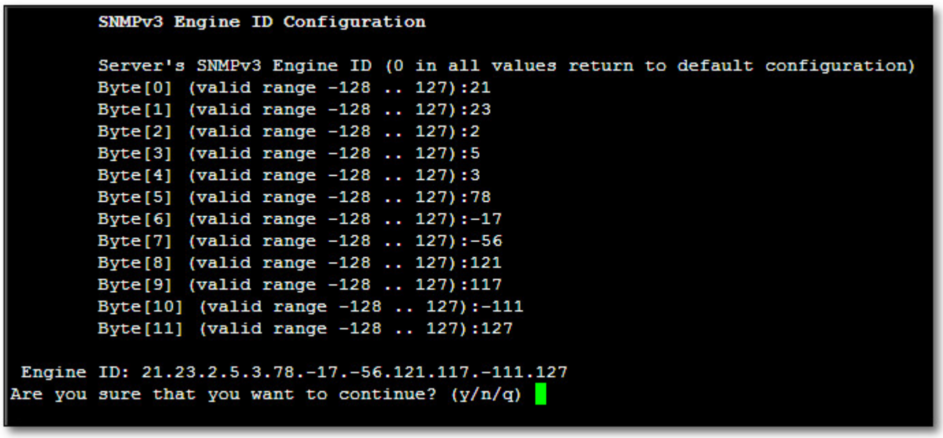


```
SNMPv3 Engine ID Configuration

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 OVOC Server Manager, press **q**.

Figure 22-19: SNMPv3 Engine ID Configuration – Complete Configuration



```
        SNMPv3 Engine ID Configuration

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

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

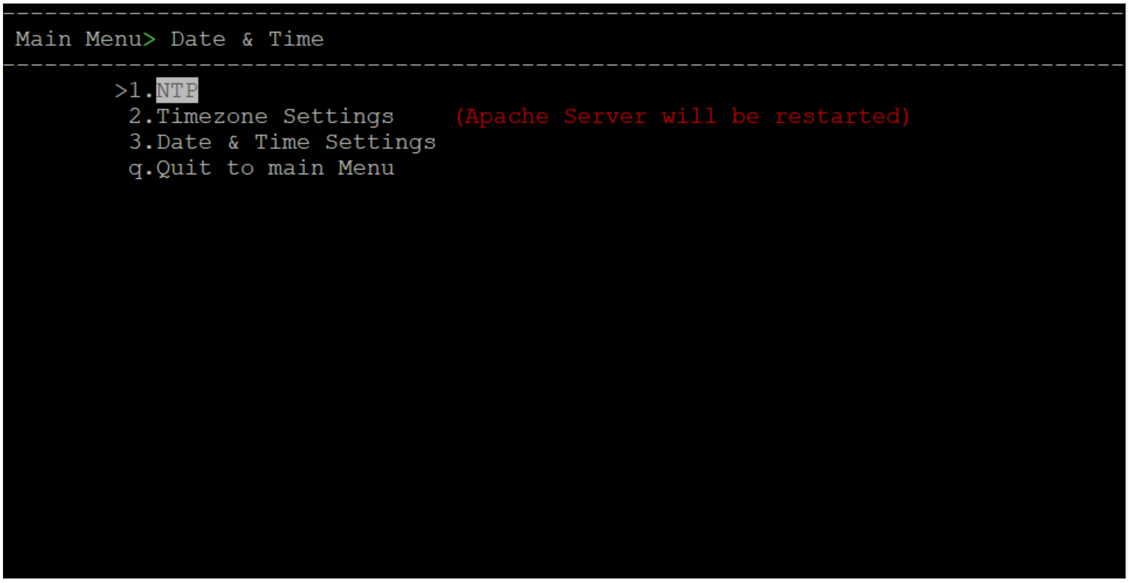
23 NTP & Clock Settings

This chapter describes how to configure the NTP clock source and the OVOC server system clock.

1. From the OVOC server Manager menu, choose **Date & Time**.

Figure 23-1: Date & Time Settings

Figure 23-2:



```
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 (see NTP below)
- Timezone Settings (Timezone Settings on page 214)
- Date & Time Settings (Date and Time Settings on page 216)

NTP

Network Time Protocol (NTP) is used to synchronize the time and date of the OVOC server and all its components with connected devices in the IP network. This option enables you to do the following:

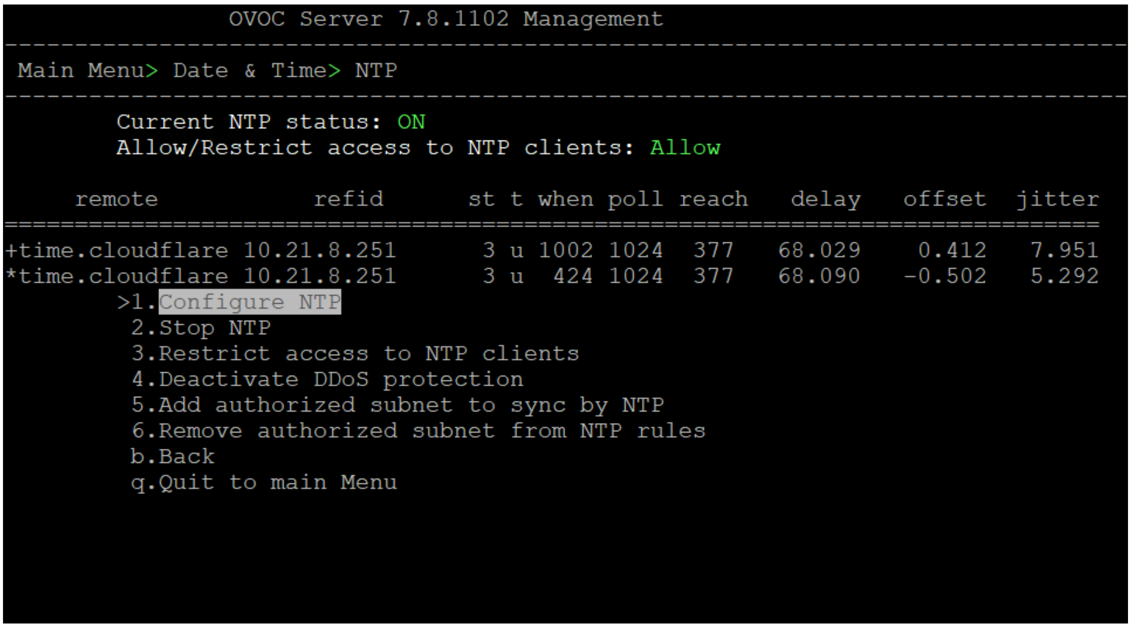
- Configure the OVOC server to obtain its clock from an external NTP clock source. Other devices that are connected to the OVOC server in the IP network can synchronize with this clock source. These devices may be any device containing an NTP server or client.
- Configure the OVOC server as the NTP server source (Stand-alone NTP server) and allow other clients and subnets in the IP network to synchronize to this source.

- 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. For example, for Cloud deployments, it is recommended to configure the Microsoft Azure or Amazon AWS platforms as the external clock source.
- Configure the same NTP server IP address/domain name and other relevant settings on both the OVOC server and on the the AudioCodes device (Setup > Administration > Time & Date).
- When connecting OVOC to Skype For Business, ensure that the same NTP server clock source is configured on both ends.

➢ To configure NTP:

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

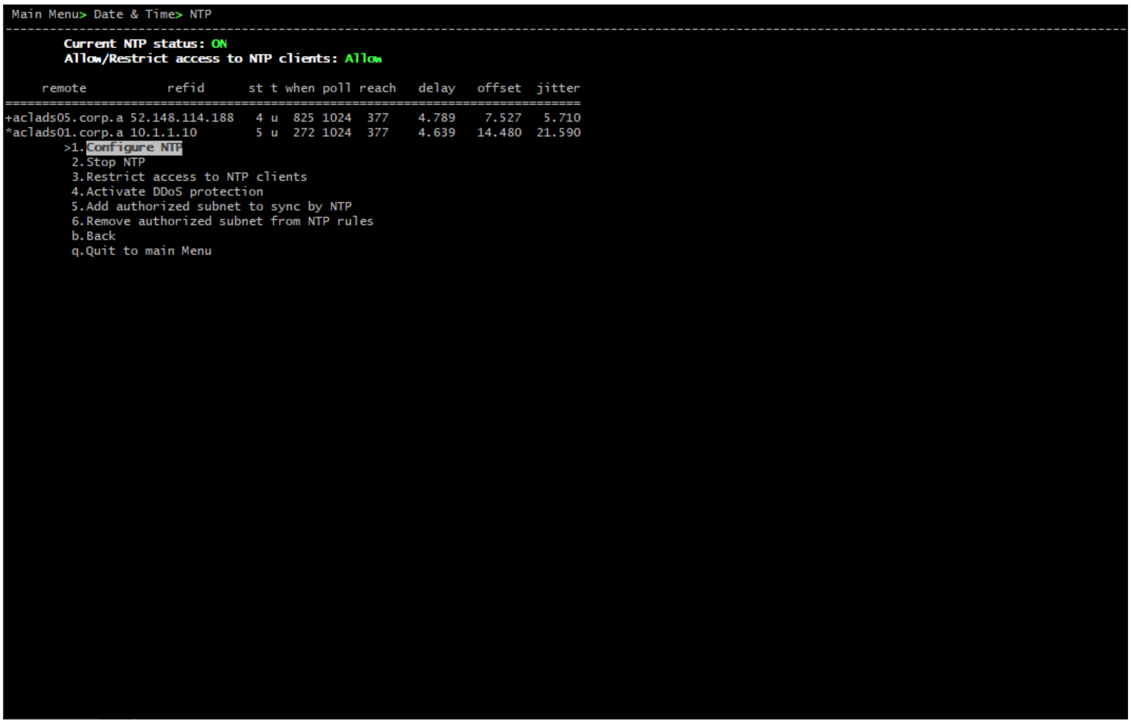
Figure 23-3: OVOC Server Manager - Configure NTP



```
                OVOC Server 7.8.1102 Management
--------------------------------------------------------------------------------
 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
==============================================================================
+time.cloudflare 10.21.8.251      3 u 1002 1024  377   68.029    0.412   7.951
*time.cloudflare 10.21.8.251      3 u  424 1024  377   68.090   -0.502   5.292
        >1.Configure NTP
         2.Stop NTP
         3.Restrict access to NTP clients
         4.Deactivate 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 **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 address or domain name of the NTP servers to serve as the clock reference source for the NTP client (Up to four NTP servers can be configured). The NTP process daemon starts and the NTP status information is displayed on the screen.

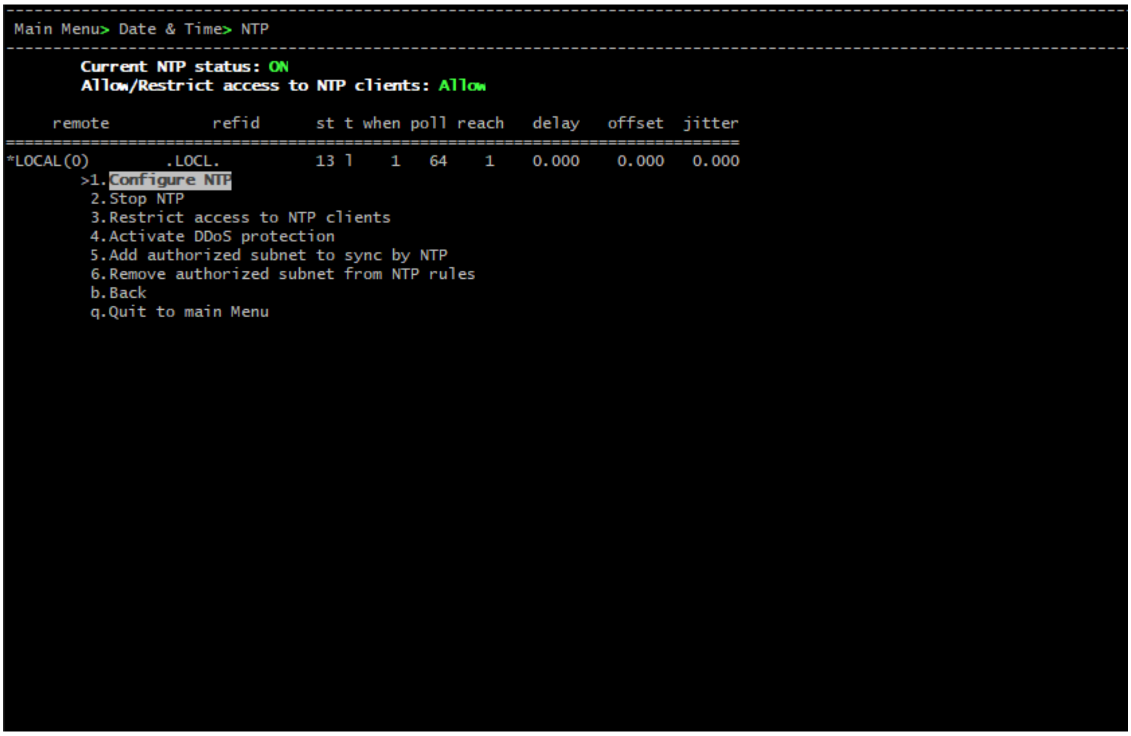
Figure 23-4: External Clock Source



```
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
==============================================================================
+aclads05.corp.a 52.148.114.188   4 u  825 1024  377    4.789    7.527   5.710
*aclads01.corp.a 10.1.1.10        5 u  272 1024  377    4.639   14.480  21.590
       >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
```

- Type **n** for the OVOC server to function as a Stand-alone NTP server. The NTP process daemon starts and the NTP status information is displayed on the screen.

Figure 23-5: Local Clock Source



```
--------------------------------------------------------------------------------------------------------------------------------
 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
==============================================================================
*LOCAL(0)        .LOCL.          13 l    1   64    1    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
```

Stopping and Starting the NTP Server

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

➢ **To start NTP services:**

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

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

Restrict Access to NTP Clients

When the OVOC server is configured as a Stand-alone NTP server, you configure NTP rules to authorize which clients can synchronize with the OVOC NTP clock.

➢ **To allow access to NTP clients:**

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

Activate DDoS Protection

This option enables you to activate DDos protection for preventing Distributed Denial of Service attacks on the OVOC server. For example, attacks resulting from security scans. This is relevant for both when the OVOC server is configured as a Stand-alone clock source and when an external clock source is used.

➢ **To activate DDoS protection:**

- From the NTP menu, select **Activate/Deactivate DDoS Protection.**

Authorizing Subnets to Connect to OVOC NTP

When the OVOC server is configured as a Stand-alone NTP server, you can configure NTP rules to authorize which subnets can synchronize with the OVOC NTP clock.

➢ **To authorize subnets:**

- From the NTP menu, select **Add Authorized Subnet to Sync by NTP**

➢ **To remove authorized subnet from NTP rules:**

- From the NTP menu, select **Remove Subnet from NTP Rules**.

Timezone Settings

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

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

➢ To change the system timezone:

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

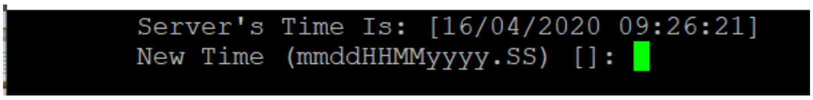
Date and Time Settings

You can set the date and time for the OVOC server system clock.

➢ **To configure data and time:**

1. From the Date & Time menu, select **Date & Time Settings**, and then press Enter.

Figure 24-1: New Server Time



```
Server's Time Is: [16/04/2020 09:26:21]
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.

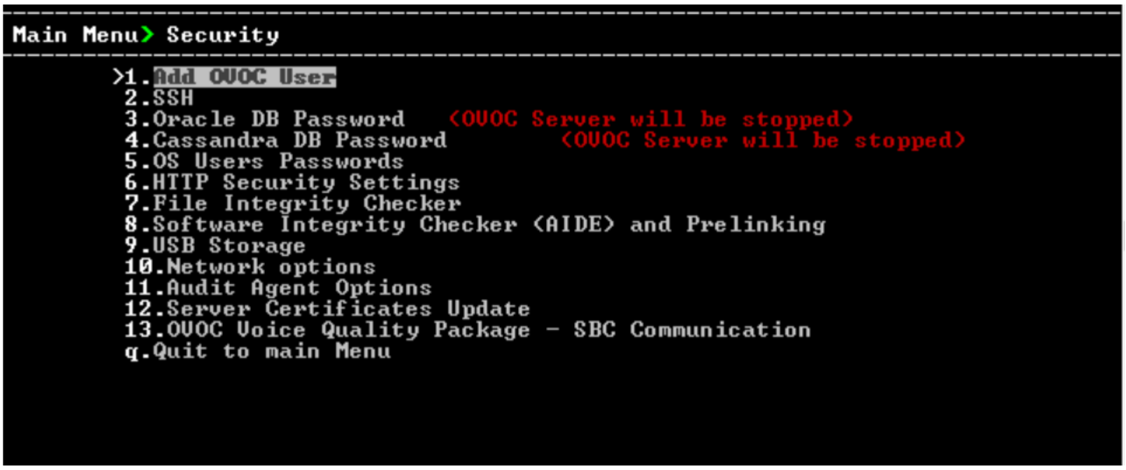
25 Security

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

➢ **To configure security settings:**

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

Figure 25-1: Security Settings



```
--------------------------------------------------------------------------------
Main Menu> Security
--------------------------------------------------------------------------------
        >1.Add OVOC User
         2.SSH
         3.Oracle DB Password    <OVOC Server will be stopped>
         4.Cassandra DB Password        <OVOC Server will be stopped>
         5.OS Users Passwords
         6.HTTP Security Settings
         7.File Integrity Checker
         8.Software Integrity Checker (AIDE) and Prelinking
         9.USB Storage
         10.Network options
         11.Audit Agent Options
         12.Server Certificates Update
         13.OVOC Voice Quality Package - SBC Communication
         q.Quit to main Menu
```

This menu includes the following options:

- Add OVOC User (OVOC User on the next page)
- SSH (SSH on the next page)
- Oracle DB Password (DB Password)
- Cassandra Password (Cassandra Password on page 226)
- OS Users Password (OS Users Passwords on page 227)
- HTTP Security Settings (HTTPS SSL TLS Security on page 233)
    - Server Certificate Update (Server Certificates Update on page 234)
- File Integrity Checker (File Integrity Checker on page 230)
- Software Integrity Checker (AIDE) and Pre-linking (Software Integrity Checker (AIDE) and Pre-linking on page 231)
- USB Storage (USB Storage on page 231)
- Network options (Network Options on page 232)
- Audit Agent Options (Auditd Options on page 233)
- OVOC Voice Quality Package (OVOC Voice Quality Package - SBC Communication on page 239)

OVOC User

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

➢ To add an OVOC user:

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

Note and retain these passwords for future access.

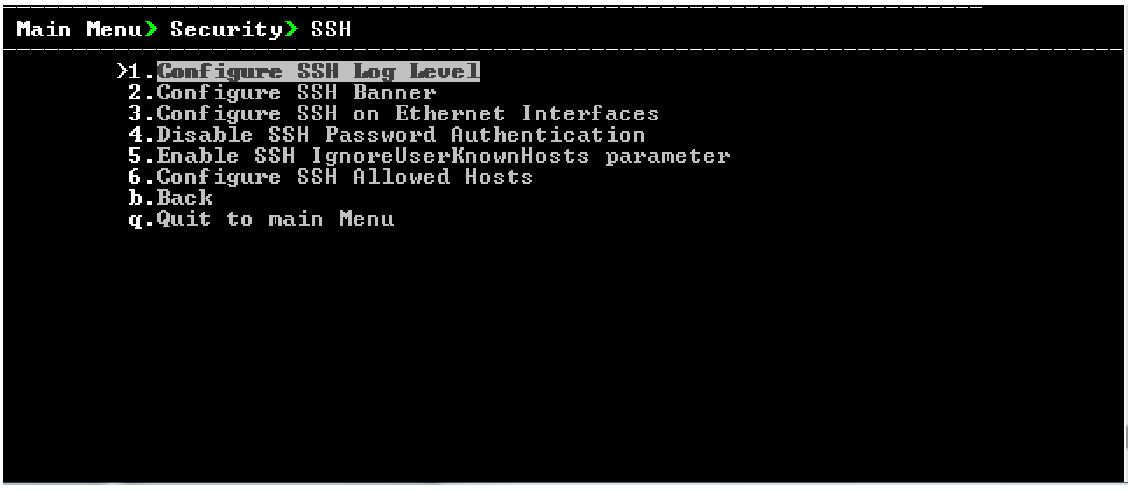
SSH

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

➢ To configure SSH:

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

Figure 25-2: SSH Configuration



```
Main Menu> Security> SSH

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

This menu includes the following options:

- Configure SSH Log Level (SSH Log Level on the next page).
- Configure SSH Banner (SSH Banner on the next page).
- Configure SSH on Ethernet Interfaces (SSH on Ethernet Interfaces on page 220).

- Disable SSH Password Authentication (Enable/Disable SSH Password Authentication on page 222).
- Enable SSH Ignore User Known Hosts Parameter (Enable SSH IgnoreUserKnownHosts Parameter on page 222).
- Configure SSH Allowed Hosts (SSH Allowed Hosts on page 223).

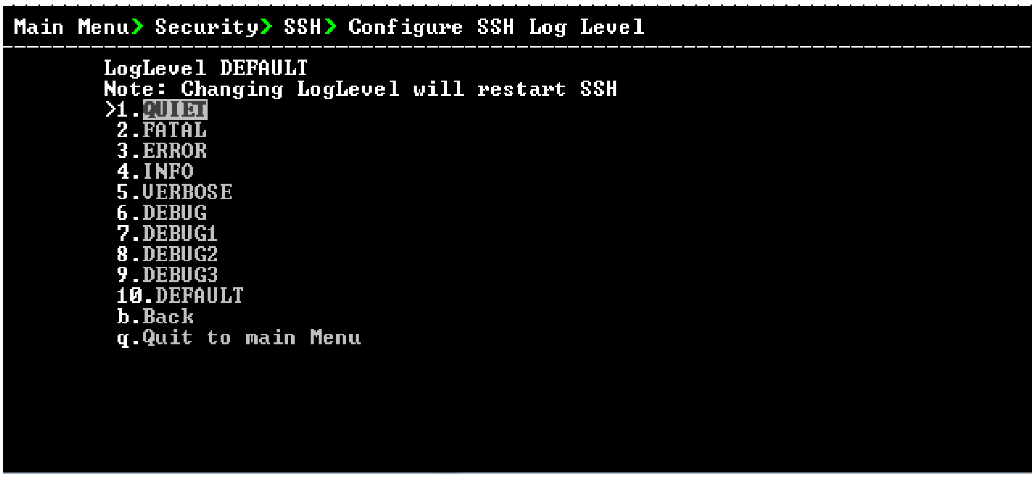
SSH Log Level

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 25-3: SSH Log Level Manager



```
Main Menu> Security> SSH> Configure SSH Log Level

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

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

   The SSH daemon restarts automatically.

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

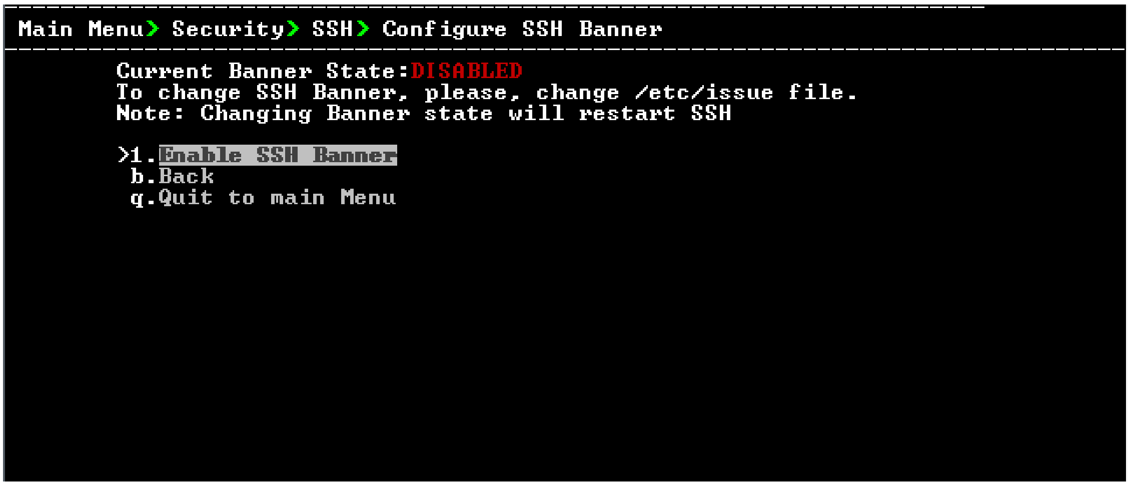
SSH Banner

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

➢ To configure the SSH banner:

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

Figure 25-4: 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.

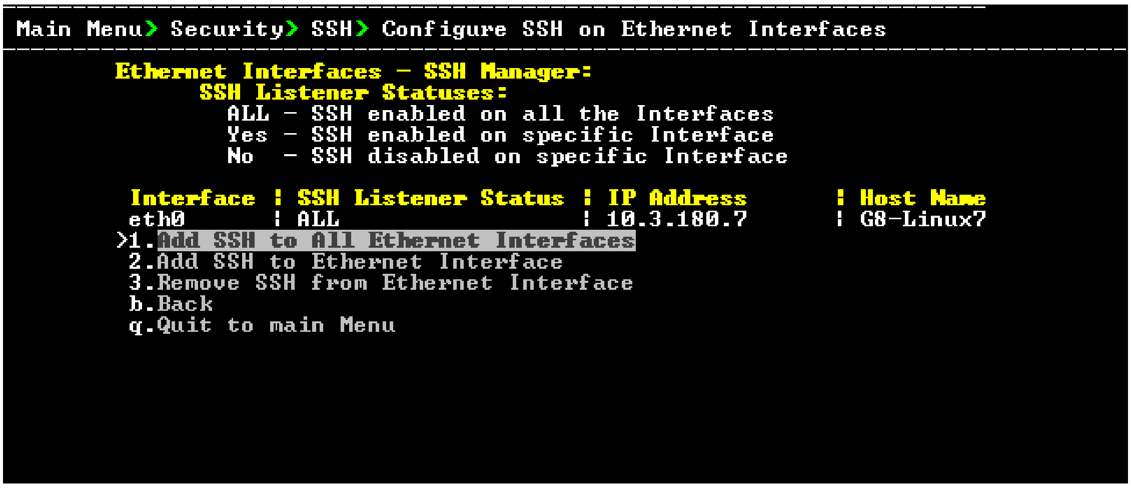
SSH on Ethernet Interfaces

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 25-5: 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-Linux7
        >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 (Add SSH to All Ethernet Interfaces on the next page).
- Add SSH to Ethernet Interface (Add SSH to Ethernet Interface on the next page).

- Remove SSH from Ethernet Interface (Remove SSH from Ethernet Interface below).

Add SSH to All Ethernet Interfaces

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

➢ To add SSH to All Ethernet Interfaces:

■ From the Configure SSH on Ethernet Interfaces menu, choose option **1**, and then press Enter.

The SSH daemon restarts automatically to update this configuration action.

The column 'SSH Listener Status' displays ALL for all interfaces.

Add SSH to Ethernet Interface

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

➢ To add SSH to Ethernet Interfaces:

1. From the Configure SSH on Ethernet Interfaces menu, choose option **2**, and then press Enter.

   After entering the appropriate sub-menu, all the interfaces upon which SSH access is currently disabled are displayed.

2. Enter the appropriate interface number, and then press Enter.

   The SSH daemon restarts automatically to update this configuration action.

   The column 'SSH Listener Status' displays 'YES' for the configured interface.

Remove SSH from Ethernet Interface

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

➢ To deny SSH from a specific Ethernet Interface:

1. From the Configure SSH on Ethernet Interfaces menu, choose option **3**, and then press Enter.

   All the interfaces to which SSH access is currently enabled are displayed.

2. Enter the desired interface number, and then press Enter.

   The SSH daemon restarts automatically to update this configuration action.

   The column 'SSH Listener Status' displays 'No' for the denied interface.

⚠ If you attempt to deny SSH access for the only enabled interface, a message is displayed informing you that such an action is not allowed.

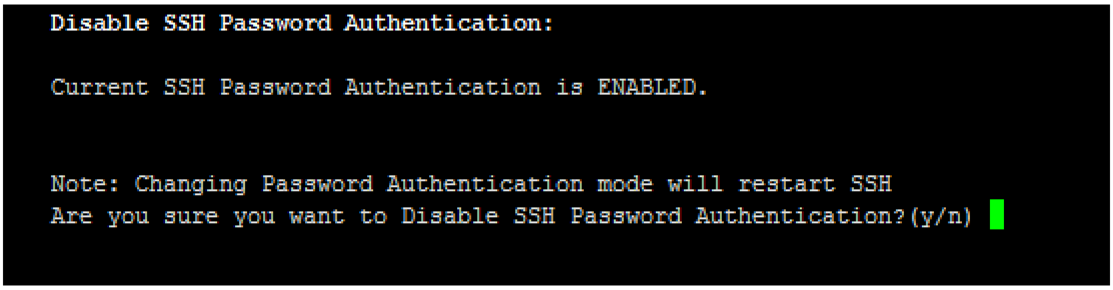
Enable/Disable SSH Password Authentication

This option enables you to disable the username/password authentication method for all network interfaces enabled on the OVOC server.

➢ To disable SSH Password Authentication:

1. From the SSH menu, choose option **4**, and then press Enter; the following is displayed:

Figure 25-6: Disable Password Authentication



```
Disable SSH Password Authentication:

Current SSH Password Authentication is ENABLED.


Note: Changing Password Authentication mode will restart SSH
Are you sure you want to Disable SSH Password Authentication?(y/n)
```

2. Type **y** to disable SSH password authentication or **n** to enable, and then press Enter.

   The SSH daemon restarts automatically to update this configuration action.

⚠ Once you perform this action, you cannot reconnect to the OVOC server using User/Password authentication. Therefore, before you disable this authentication method, ensure that you provision an alternative SSH connection method. For example, using an RSA keys pair. For detailed instructions on how to perform such an action, see www.junauza.com or search the internet for an alternative method.

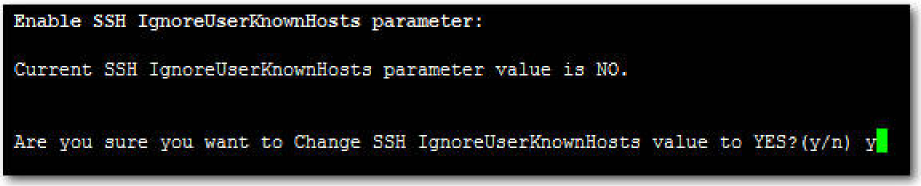
Enable SSH IgnoreUserKnownHosts Parameter

This option enables you to disable the use of the '$HOME/.ssh/known_host' file with stored remote servers fingerprints.

➢ To enable SSH IgnoreUserKnowHosts parameter:

1. From the SSH menu, choose option **5**, and then press Enter; the following is displayed:

Figure 25-7: SSH IgnoreUserKnowHosts Parameter - Confirm



```
Enable SSH IgnoreUserKnownHosts parameter:

Current SSH IgnoreUserKnownHosts parameter value is NO.


Are you sure you want to Change SSH IgnoreUserKnownHosts value to YES?(y/n) y
```

2. Type **y** to change this parameter value to either 'YES' or 'NO' or type **n** to leave as is, and then press Enter.

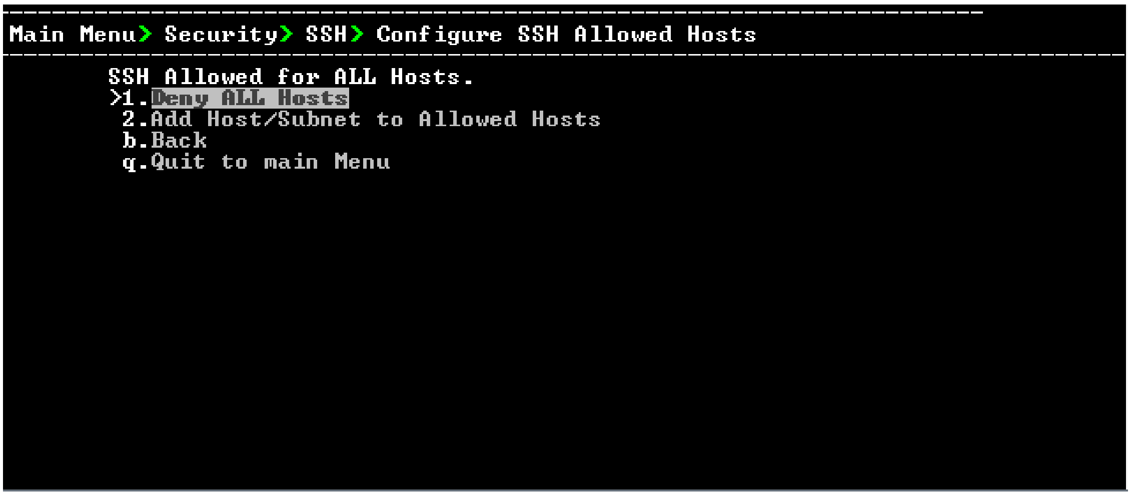
SSH Allowed Hosts

This option enables you to define which hosts are allowed to connect to the OVOC server through SSH.

➢ To Configure SSH Allowed Hosts:

- From the SSH menu, choose option **6**, and then press Enter; the following is displayed:

Figure 25-8: Configure SSH Allowed Hosts



```
Main Menu> Security> SSH> Configure SSH Allowed Hosts

       SSH Allowed for ALL Hosts.
       >1.Deny ALL Hosts
        2.Add Host/Subnet to Allowed Hosts
        b.Back
        q.Quit to main Menu
```

This menu includes the following options:

- Allow ALL Hosts (Allow ALL Hosts below).
- Deny ALL Hosts (Deny ALL Hosts on the next page).
- Add Host/Subnet to Allowed Hosts (Add Hosts to Allowed Hosts on the next page).
- Remove Host/Subnet from Allowed Hosts (Remove Host/Subnet from Allowed Hosts on page 225).

Allow ALL Hosts

This option enables all remote hosts to access this OVOC server through the SSH connection (default).

➢ To allow ALL Hosts:

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter.
2. Type **y** to confirm, and then press Enter.

   The appropriate status is displayed in the screen.

Deny ALL Hosts

This option enables you to deny all remote hosts access to this OVOC server through the SSH connection.

➢ To deny all remote hosts access:

1. From the Configure SSH Allowed Hosts menu, choose option **2**, and then press Enter.
2. Type **y** to confirm, and then press Enter.

   The appropriate status is displayed in the screen.

When this action is performed, the OVOC server is disconnected and you cannot reconnect to the OVOC server through SSH. Before you disable SSH access, ensure that you have provisioned alternative connection methods, for example, serial management connection or KVM connection.

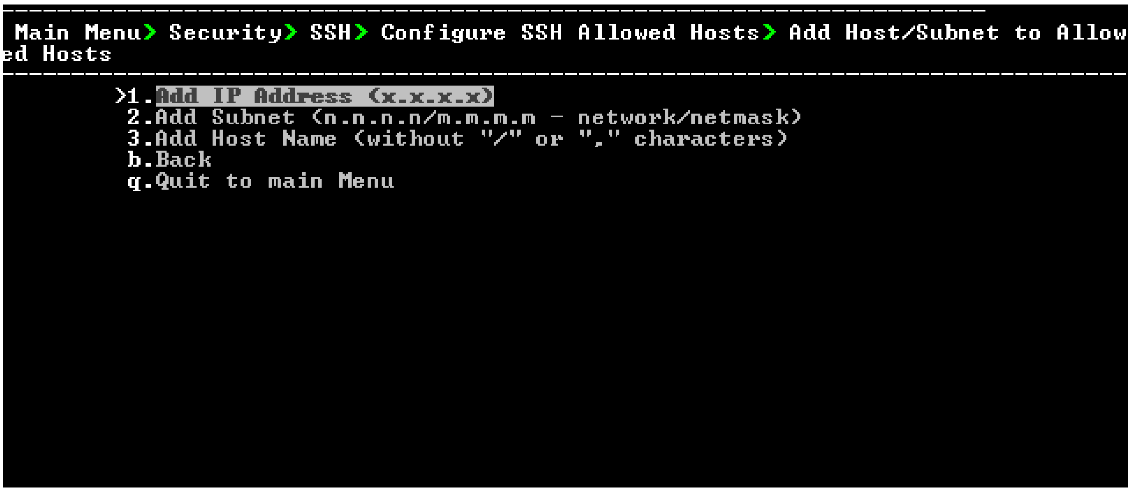
Add Hosts to Allowed Hosts

This option enables you to allow different SSH access methods to different remote hosts. You can provide the desired remote host IP, subnet or host name in order to connect to the OVOC server through SSH.

➢ To add Hosts to Allowed Hosts:

1. From the Configure SSH Allowed Hosts menu, choose option **3**, and then press Enter; the following is displayed:

Figure 25-9: 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.

When adding a Host Name, ensure the following:

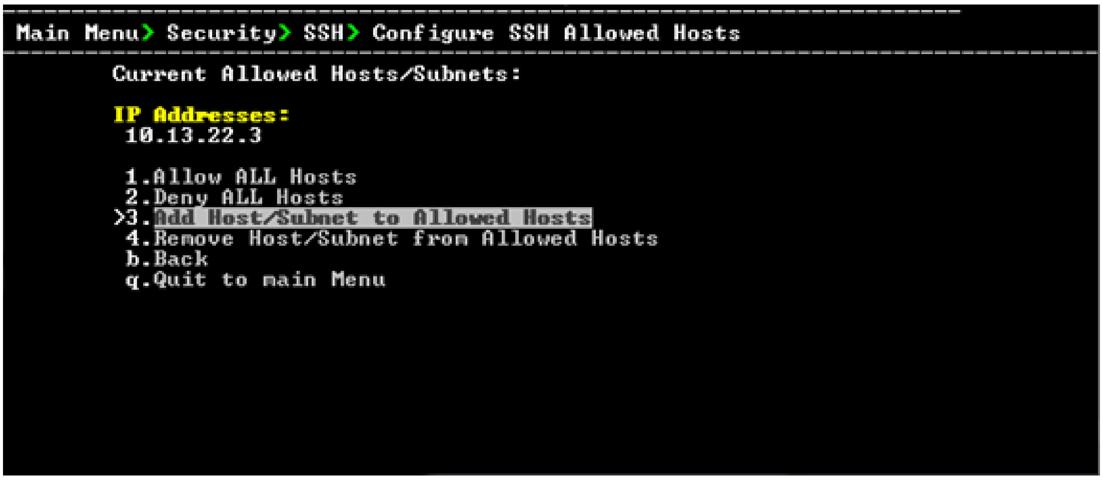
- Verify your remote host name appears in the DNS server database and your OVOC server has an access to the DNS server.
- Provide the host name of the desired network interface defined in “/etc/hosts” file.

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 25-10: Add Host/Subnet to Allowed Hosts-Configured Host



```
Main Menu> Security> SSH> Configure SSH Allowed Hosts

        Current Allowed Hosts/Subnets:

        IP Addresses:
         10.13.22.3

         1.Allow ALL Hosts
         2.Deny ALL Hosts
        >3.Add Host/Subnet to Allowed Hosts
         4.Remove Host/Subnet from Allowed Hosts
         b.Back
         q.Quit to main Menu
```

Remove Host/Subnet from Allowed Hosts

If you have already configured a list of allowed hosts IP addresses, you can then remove one or more of these host addresses from the list.

➢ **To remove an existing allowed host's IP address:**

1. From the Configure SSH Allowed Hosts menu, choose option **1**, and then press Enter; the following is displayed:
2. Choose the desired entry to remove from the Allowed Hosts list, i.e. to deny access to the OVOC server through SSH connection, and then press Enter again.
3. Type **y** to confirm the entry, and then press Enter again.

   When the allowed hosts entry has been successfully removed, it is displayed in the SSH Allow/Deny Host Manager screen as shown in the figure below:

When you remove either the only existing IP address, Subnet or Host Name in the Allowed Hosts in the Allowed Hosts list, the configuration is automatically set to the default state “Allow All Hosts”.

Oracle DB Password

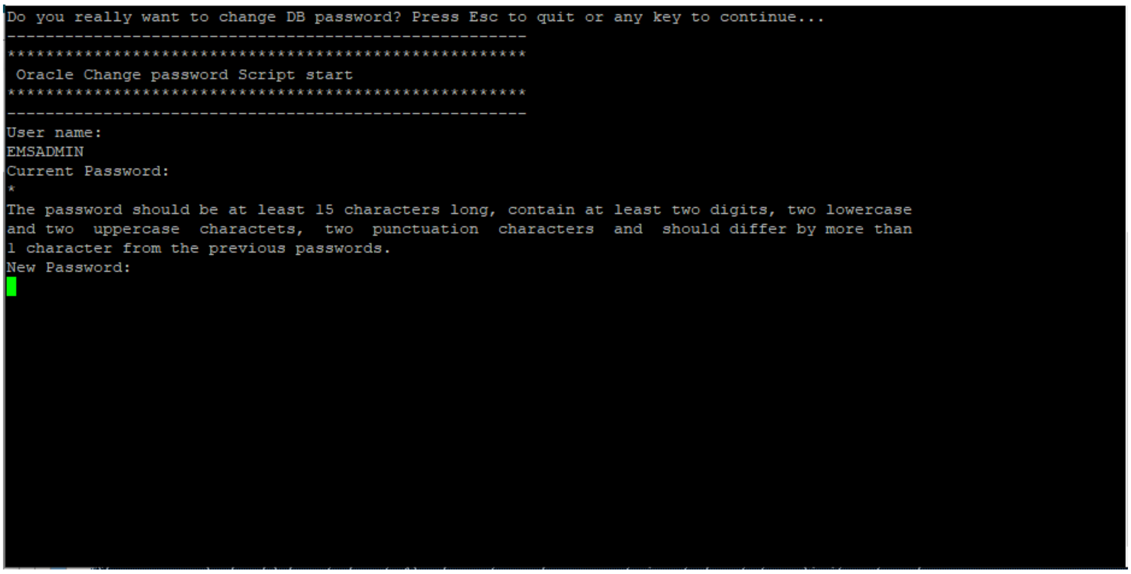
This option enables you to change the default Oracle Database password "pass_1234". The OVOC server shuts down automatically before changing the Oracle Database password.

➢ To change the DB Password:

1. From the Security menu, choose **Oracle DB Password**, and then press Enter; the OVOC server is rebooted.

2. Press Enter until the New Password prompt is displayed.

Figure 25-11: OVOC 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  charactets,  two  punctuation  characters  and  should differ by more than
1 character from the previous passwords.
New Password:
```

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

- The OVOC server is rebooted when you change the Oracle Database password.
- Note and retain these passwords for future access. It is not possible to restore these passwords or to enter the OVOC Oracle Database without them.

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

Cassandra Password

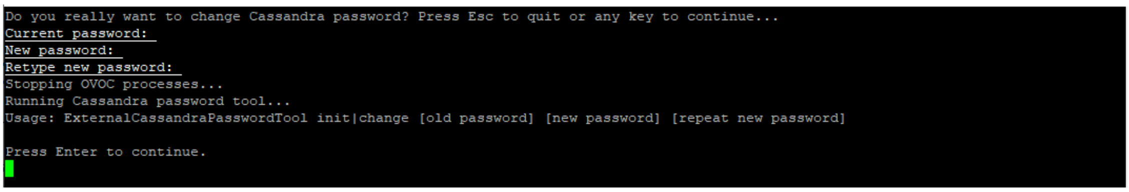
This section describes how to change the Cassandra password.

➢ To change the Cassandra Password:

1. From the Security menu, choose **Cassandra DB Password**, and then press Enter; the OVOC server is rebooted.

2. Press Enter until the New Password prompt is displayed.

Figure 25-12: Change Cassandra Password



```
Do you really want to change Cassandra password? Press Esc to quit or any key to continue...
Current password:
New password:
Retype new password:
Stopping OVOC processes...
Running Cassandra password tool...
Usage: ExternalCassandraPasswordTool init|change [old password] [new password] [repeat new password]

Press Enter to continue.
```

3. Enter the new password and confirm.

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 (General Password Settings below).
   - Operating System User Security Extensions (Operating System User Security Extensions on the next page).

General Password Settings

This option enables you to change the OS general password settings, such as 'Minimum Acceptable Password Length' and 'Enable User Block on Failed Login'. This feature also enables you to modify settings for a specific user, such as 'User’s Password' and 'Password Validity Max Period'.

➢ **To modify general password settings:**

1. The Change General Password Settings prompt is displayed; type **y**, and then press Enter.
2. Do you want to change general password settings? (y/n)y
3. The Minimum Acceptable Password Length prompt is displayed; type 10, and then press Enter.

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

4. The Enable User Block on Failed Login prompt is displayed; type **y**, and then press Enter.

```
Enable User Block on Failed Login (y/n) [y] y
```

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

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

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

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

7. You are prompted if you wish to continue; type **y**, and then press Enter.

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

8. You are prompted if you wish to change the password for a specific user.

```
Do you wish to change this user's password?
```

9. Enter the username whose password you wish to change.

```
Enter Username [username]
```

10. Enter the new password and confirm.

Operating System User Security Extensions

This feature enables the administrator to configure the following additional user security extensions:

- Maximum allowed numbers of simultaneous open sessions.
- Inactivity time period (days) before the OS user is locked.

To configure these parameters, in the OS Passwords Settings menu, configure parameters according to the procedure below (see also green arrows indicating the relevant parameters to configure).

➢ To configure operating system users security extensions:

1. The Change General Password Settings prompt is displayed; type **n**, and then press Enter.

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

2. The Change password for a specific user prompt is displayed; type **y**, and then press Enter.

```
Do you want to change password for specific user ? (y/n) y
```

3. Enter the Username upon which you wish to configure, and then press Enter.

```
Enter Username [acems]:
```

4. The change User Password prompt is displayed; type **n**, and then press Enter.

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

5. An additional Password prompt is displayed, type **y**, and then press Enter.

```
Do you want to change its login and password properties? (y/n) y
```

6. The Password Validity prompt is displayed; press Enter.

```
Password Validity Max Period (days) [90]:
```

7. The Password Update prompt is displayed; press Enter.

```
Password Update Min Period (days) [1]:
```

8. The Password Warning prompt is displayed; press Enter.

```
Password Warning Max Period (days) [7]:
```

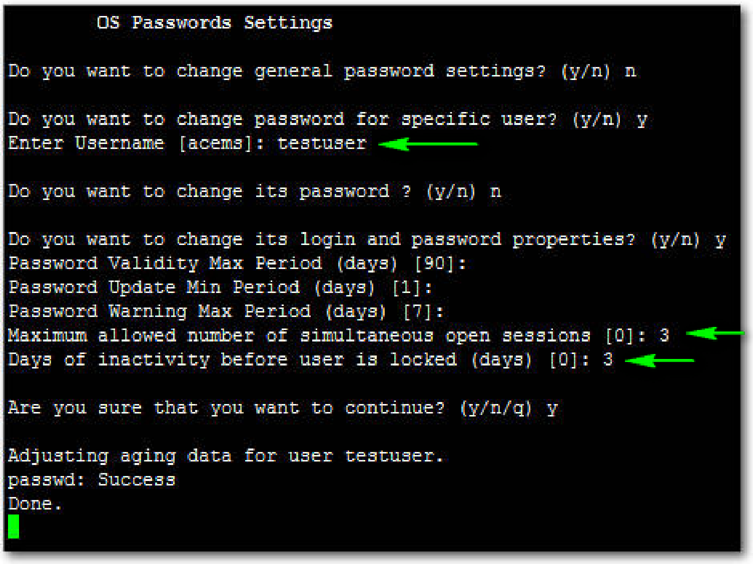
9. The Maximum number of Simultaneous Open Sessions prompt is displayed; enter the number of simultaneous open SSH connections you wish to allow for this user.

```
Maximum allowed number of simultaneous open sessions [0]:
```

10. The Inactivity Days prompt is displayed; enter the number of inactivity days before the user is locked. For example, if you'd like to suspend a specific user if they have not connected to the OVOC server for a week, enter 7 days.

```
Days of inactivity before user is locked (days) [0]:
```

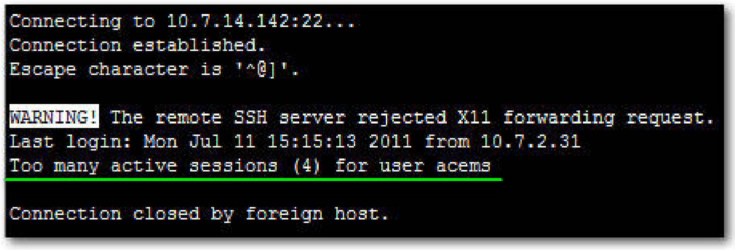
Figure 25-13: OS Passwords Settings with Security Extensions



```
        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 25-14: Maximum Active SSH Sessions



```
Connecting to 10.7.14.142:22...
Connection established.
Escape character is '^@]'.

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Jul 11 15:15:13 2011 from 10.7.2.31
Too many active sessions (4) for user acems

Connection closed by foreign host.
```

By default you can connect through SSH to the OVOC server with user *acems* only. If you configure an inactivity days limitation on this user, the situation may arise, for example, where a user is away for an extended period and has no active user to access the OVOC server. Therefore, we strongly recommend to use this limitation very carefully and preferably to configure this option for each user to connect to the OVOC server through SSH other than with the *acems* user.

File Integrity Checker

The File Integrity checker tool periodically verifies whether file attributes were changed (permissions/mode, inode #, number of links, user id, group id, size, access time, modification time, creation/inode modification time). File Integrity violation problems are reported through OVOC Security Events. The File Integrity checker tool runs on the OVOC server machine.

- From the Security menu, choose **File Integrity Checker**, and then press Enter; the File Integrity Checker is started or stopped.

Software Integrity Checker (AIDE) and Pre-linking

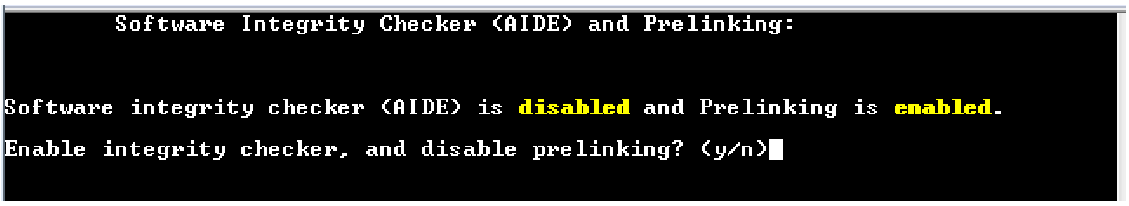
AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. This mechanism creates a database from the regular expression rules that it finds in its configuration file. Once this database is initialized, it can be used to verify the integrity of the files.

Pre-linking is designed to decrease process startup time by loading each shared library into an address for which the linking of needed symbols has already been performed. After a binary has been pre-linked, the address where the shared libraries are loaded will no longer be random on a per-process basis. This is undesirable because it provides a stable address for an attacker to use during an exploitation attempt.

➢ To start AIDE and disable pre-linking:

1. From the Security menu, choose **Software Integrity Checker (AIDE) and Pre-linking**; the current status of these two processes is displayed:

Figure 25-15: Software Integrity Checker (AIDE) and Pre-linking



```
       Software Integrity Checker (AIDE) and Prelinking:

Software integrity checker (AIDE) is disabled and Prelinking is enabled.
Enable integrity checker, and disable prelinking? (y/n)
```

2. Do one of the following:
   - Type **y** to enable AIDE and disable pre-linking
   - Type **n** to disable AIDE and enable pre-linking.

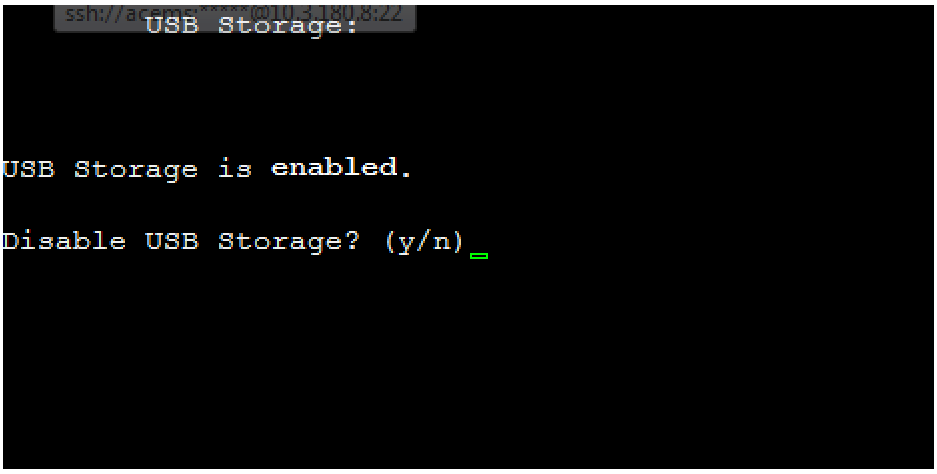
USB Storage

This menu option allows enabling or disabling the OVOC server's USB storage access as required.

➢ To enable USB storage:

1. From the Security menu, choose **USB Storage**; the following prompt is displayed:

Figure 25-16: USB Storage



```
          USB Storage:


USB Storage is enabled.

Disable USB Storage? (y/n)_
```

2. Enable or disable USB storage as required.

Network Options

This menu option provides the following options to enhance network security:

- Ignore Internet Control Message Protocol (ICMP) Echo requests:

  This option ensures that the OVOC server does not respond to ICMP broadcasts, and therefore such replies are always discarded. This prevents attempts to discover the system using ping requests.

- Ignore ICMP Echo and Timestamp requests:

  This option ensures that the OVOC server does not respond to an ICMP timestamp request to query for the current time. This reduces exposure to spoofing of the system time.

- Send ICMP Redirect Messages:

  This option disables the sending of ICMP Redirect Messages, which are generally sent only by routers.

- Ignore ICMP Redirect Messages:

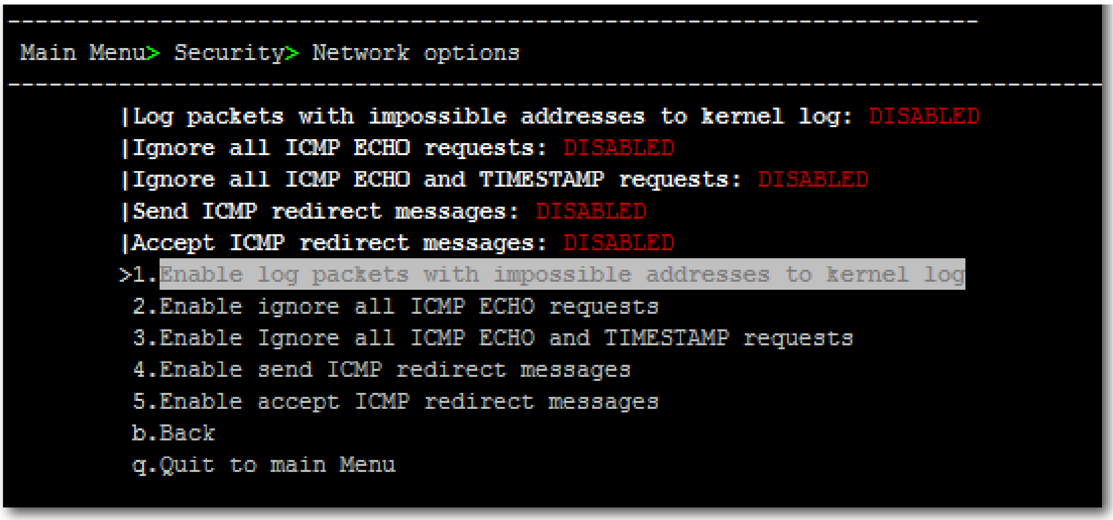
  This option ensures that the OVOC server does not respond to ICMP Redirect broadcasts, and therefore such replies are always discarded.

This prevents an intruder from attempting to redirect traffic from the OVOC server to a different gateway or a non-existent gateway.

➢ To enable network options:

1. From the Security menu, choose **Network Options**; the following screen is displayed:

Figure 25-17: Network Options



```
-----------------------------------------------------------------------
 Main Menu> Security> Network options
--------------------------------------------------------------------------------
        |Log packets with impossible addresses to kernel log: DISABLED
        |Ignore all ICMP ECHO requests: DISABLED
        |Ignore all ICMP ECHO and TIMESTAMP requests: DISABLED
        |Send ICMP redirect messages: DISABLED
        |Accept ICMP redirect messages: DISABLED
        >1.Enable log packets with impossible addresses to kernel log
         2.Enable ignore all ICMP ECHO requests
         3.Enable Ignore all ICMP ECHO and TIMESTAMP requests
         4.Enable send ICMP redirect messages
         5.Enable accept ICMP redirect messages
         b.Back
         q.Quit to main Menu
```

1. Set the required network options.

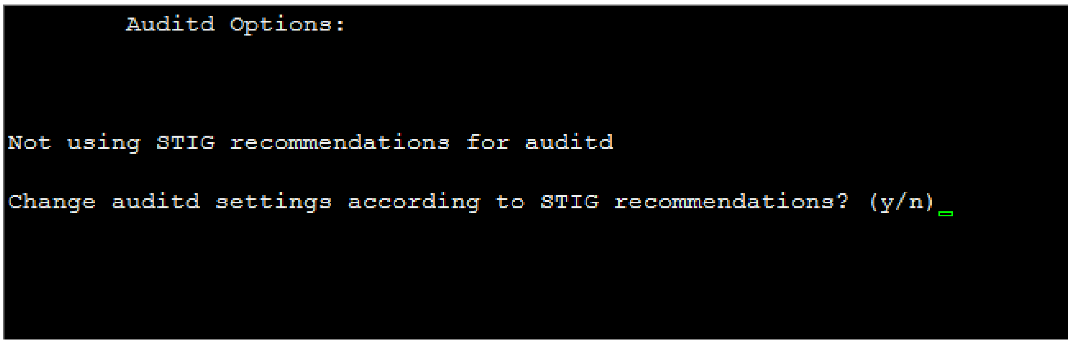
Auditd Options

Auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk. Using the Auditd option, you can change the auditd tool settings to comply with the Security Technical Information Guidelines (STIG) recommendations.

➢ To set Auditd options according to STIG:

1. From the Security menu, choose **Auditd Options**; the following screen is displayed:

Figure 25-18: Auditd Options



```
        Auditd Options:


Not using STIG recommendations for auditd

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

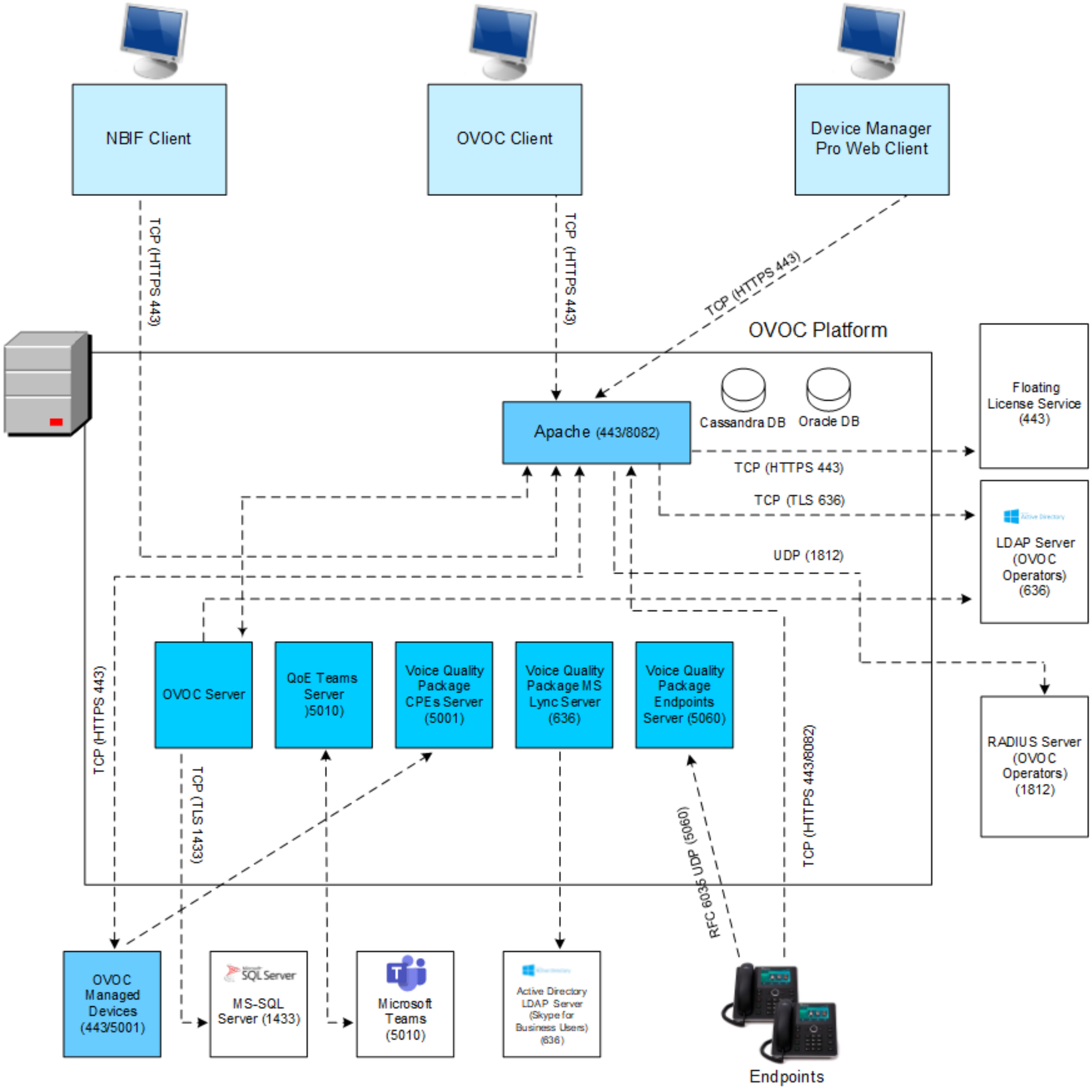
1. Enable or disable Auditd options as required.

   Audit records are saved in the following /var/log/audit/ directory.

HTTPS SSL TLS Security

This section describes the configuration settings for the HTTPS/SSL/TLS connections. The figure below shows the maximum security that can be implemented in the OVOC environment.

Figure 25-19: OVOC Maximum Security Implementation


NBIF Client
OVOC Client
Device Manager Pro Web Client
TCP (HTTPS 443)
TCP (HTTPS 443)
TCP (HTTPS 443)
OVOC Platform
Apache (443/8082)
Cassandra DB
Oracle DB
Floating License Service (443)
TCP (HTTPS 443)
TCP (TLS 636)
LDAP Server (OVOC Operators) (636)
UDP (1812)
RADIUS Server (OVOC Operators) (1812)
OVOC Server
QoE Teams Server)5010)
Voice Quality Package CPEs Server (5001)
Voice Quality Package MS Lync Server (636)
Voice Quality Package Endpoints Server (5060)
TCP (HTTPS 443)
TCP (TLS 1433)
RFC 6035 UDP (5060)
TCP (HTTPS 443/8082)
OVOC Managed Devices (443/5001)
SQL Server
MS-SQL Server (1433)
Microsoft Teams (5010)
Active Directory LDAP Server (Skype for Business Users) (636)
Endpoints

- The above figure shows all the HTTPS/SSL/TLS connections in the OVOC network. Use this figure as an overview to the procedures described below. Note that not all of the connections shown in the above figure have corresponding procedures. For more information, refer to the OVOC Security Guidelines document.
- This version supports TLS versions 1.0, 1.1, and 1.2.

Server Certificates Update

This menu option enables you to automatically generate custom SSL server certificates for securing connections between OVOC server and client processes. See . for an illustration of these connections.

If you are using self-generated certificates and private key, you can skip to step 4.

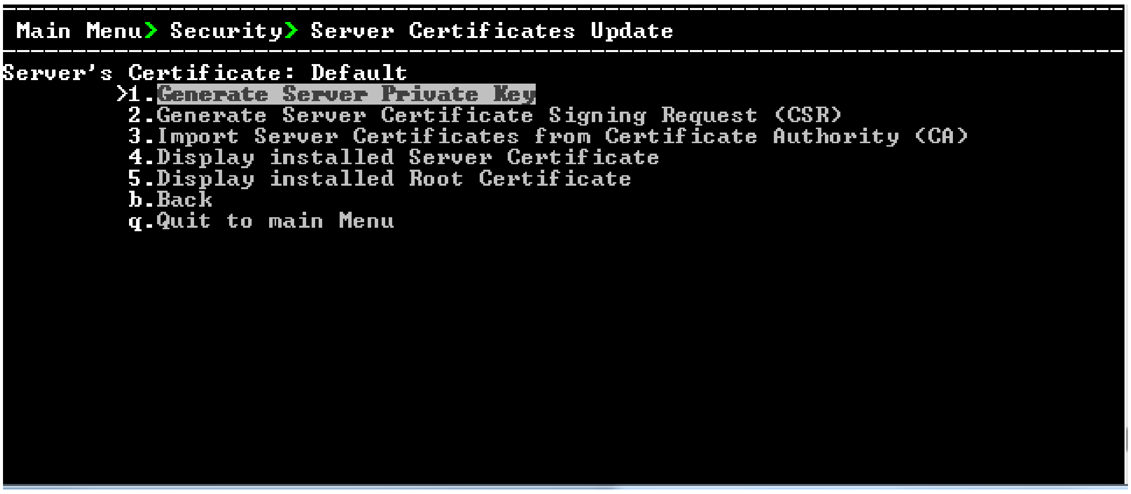
➢ The procedure for server certificates update consists of the following steps:

1. **Step 1:** Generate Server Private Key.
2. **Step 2:** Generate Server Certificate Signing Request (CSR).
3. **Step 3:** Transfer the generated CSR file to your PC and send to CA.
4. **Step 4:** Transfer certificates files received from CA back to OVOC server.
5. **Step 5:** Import new certificates on OVOC server.
6. **Step 6:** Verify the installed Server certificate.
7. **Step 7:** Verify the installed Root certificate.
8. **Step 8:** Perform Supplementary procedures to complete certificate update process (refer to Appendix Supplementary Security Procedures on page 283).

➢ To generate server certificates:

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

Figure 25-20: Server Certificate Updates



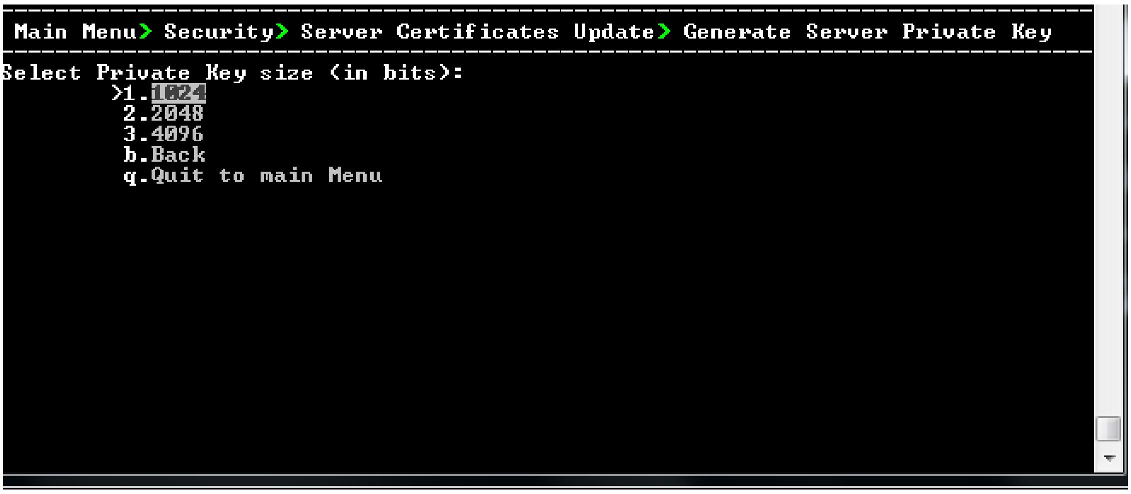
```
 Main Menu> Security> Server Certificates Update

Server's Certificate: Default
        >1.Generate Server Private Key
         2.Generate Server Certificate Signing Request (CSR)
         3.Import Server Certificates from Certificate Authority (CA)
         4.Display installed Server Certificate
         5.Display installed Root Certificate
         b.Back
         q.Quit to main Menu
```

Information on the currently installed certificate is displayed (the currently installed certificate is the installation default).

➢ Step 1: Generate a server private key:

1. Select option **1**. The following screen is displayed:

Figure 25-21: Generate Server Private Key



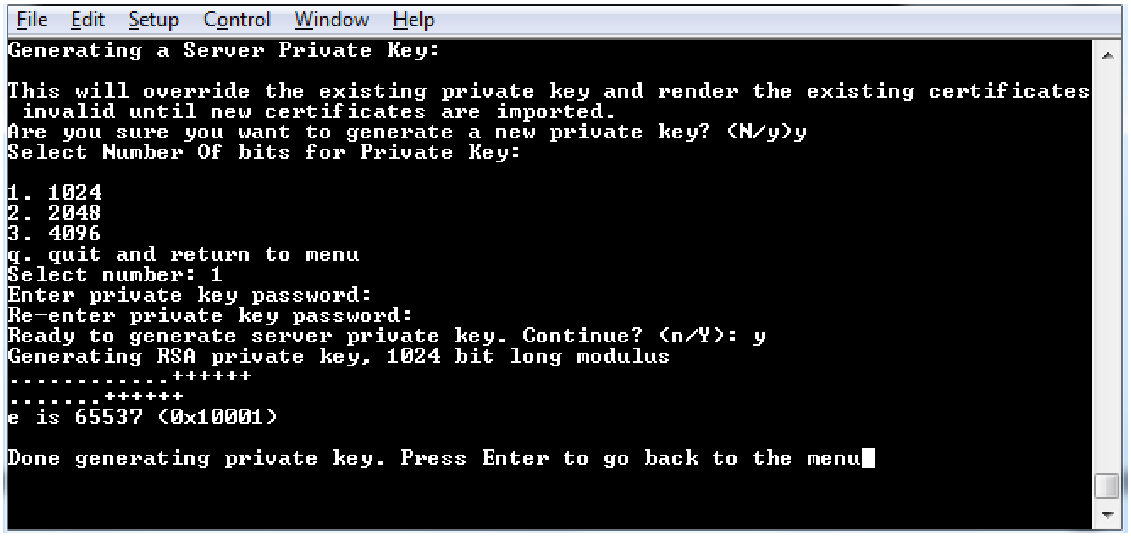
```
 Main Menu> Security> Server Certificates Update> Generate Server Private Key
Select Private Key size (in bits):
              >1.1024
               2.2048
               3.4096
               b.Back
               q.Quit to main Menu
```

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 25-22: 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**.

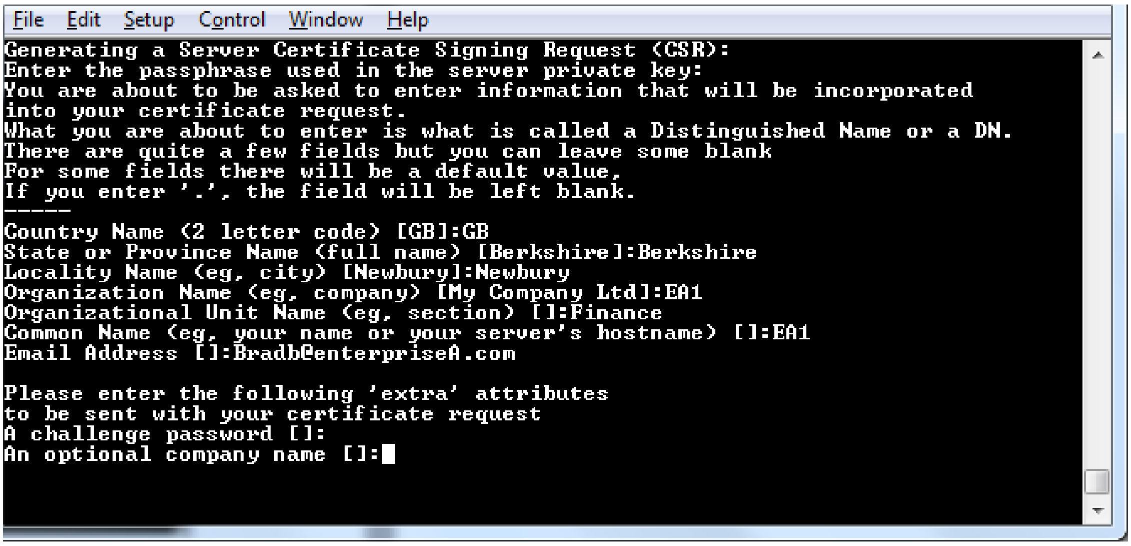
2. Enter the private key password (the password that you entered in the procedure above).

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 25-23: Generating a Server Certificate Signing Request (CSR)

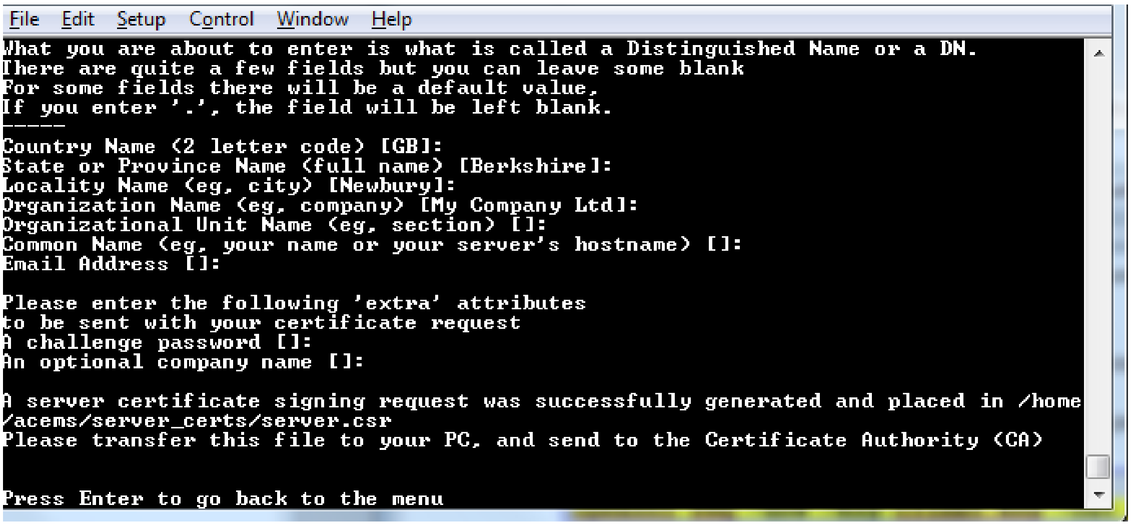


```
Generating a Server Certificate Signing Request (CSR):
Enter the passphrase used in the server private key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are 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 Transferring Files on page 295.

Figure 25-24: 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 Transferring Files on page 295.

Note: If your certificates are self-generated (you did not perform steps 1-3), the /home/acems/server_certs directory does not exist; therefore you must create it using the following commands:

```
mkdir /home/acems/server_certs
chmod 777 /home/acems/server_certs
```

➢ Step 5: Import certificates:

- Select option **3** and follow the prompts.

  The certificate files are installed.

- The root certificate should be named root.crt and that the server certificate should be named server.crt. If you received intermediate certificates then rename them to ca1.crt and ca2.crt.
- Make sure that all certificates are in PEM format and appear as follows (see Verifying and Converting Certificates on page 296 for information on converting files):

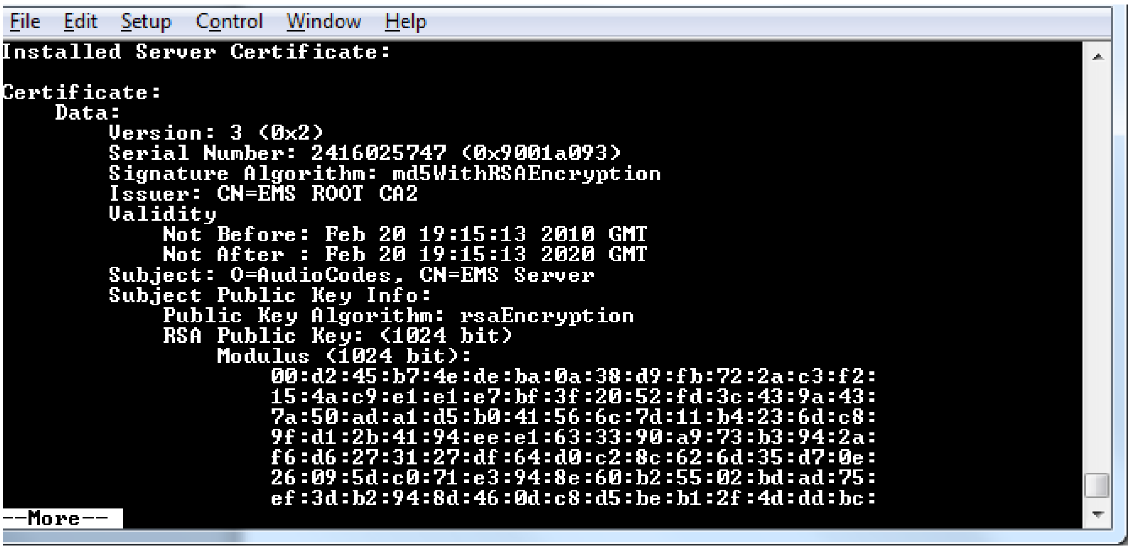
```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMBMGA
1UEAxMM
RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4NTE
0MFowKjET
Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxNJol0
L6V8lzUYOfHrEiq/6g==--
---END CERTIFICATE-----
```

➢ Step 6: Verify the installed server certificate:

- Select option **4**.

  The installed server certificate is displayed:

Figure 25-25: Installed Server Certificate

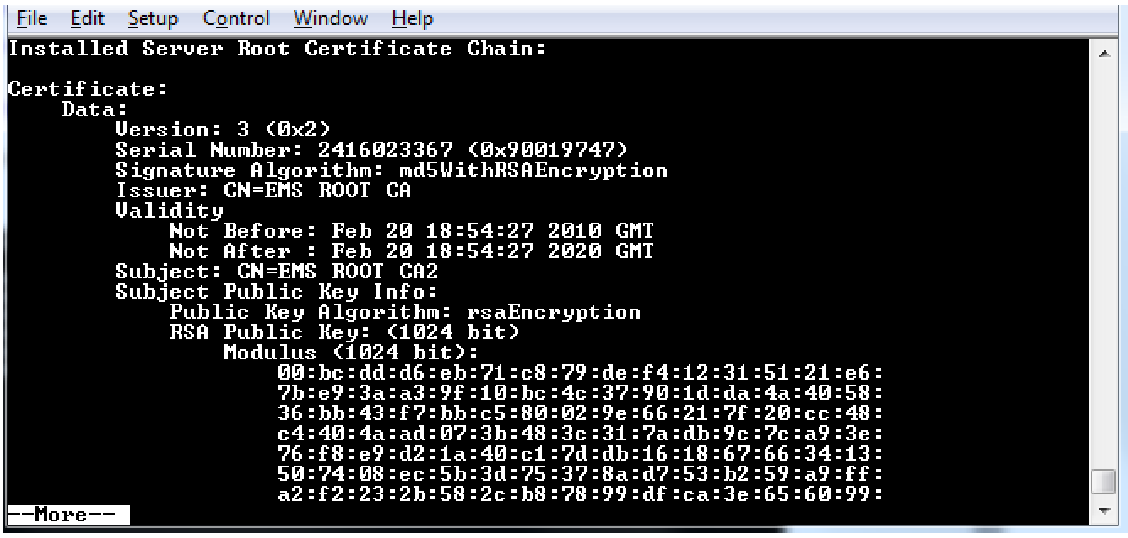


```
Installed Server Certificate:

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 25-26: 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 Supplementary Security Procedures on page 283.

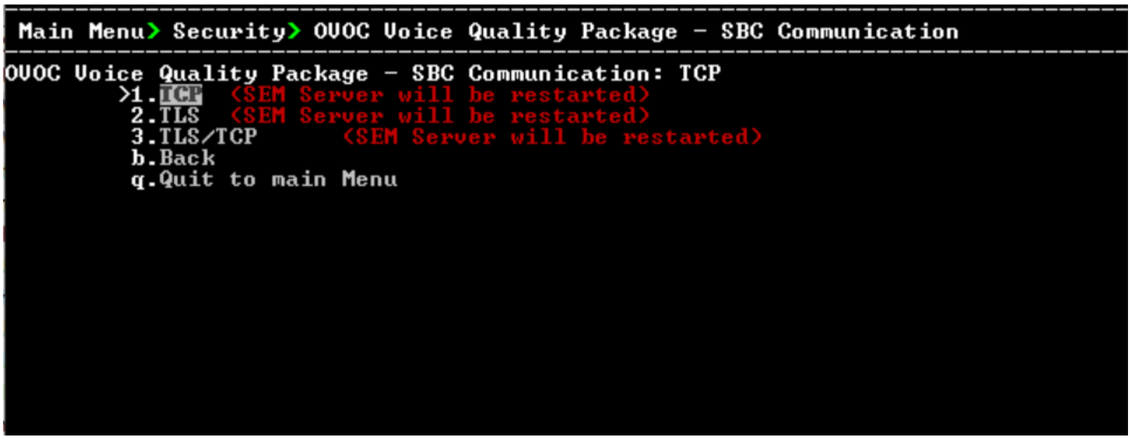
OVOC Voice Quality Package - SBC Communication

This option allows you to configure the transport type for the XML based OVOC Voice Quality Package communication from the OVOC managed devices to the OVOC server. You can enable the TCP port (port 5000), the TLS port (port 5001) connections or both port connections.

➢ To configure the OVOC Voice Quality Package - SBC Communication:

1. From the Security menu, select **OVOC Voice Quality Package – SBC Communication**

Figure 25-27: OVOC Voice Quality Package – SBC Communication



```
 Main Menu> Security> OVOC Voice Quality Package - SBC Communication
OVOC Voice Quality Package - SBC 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
```

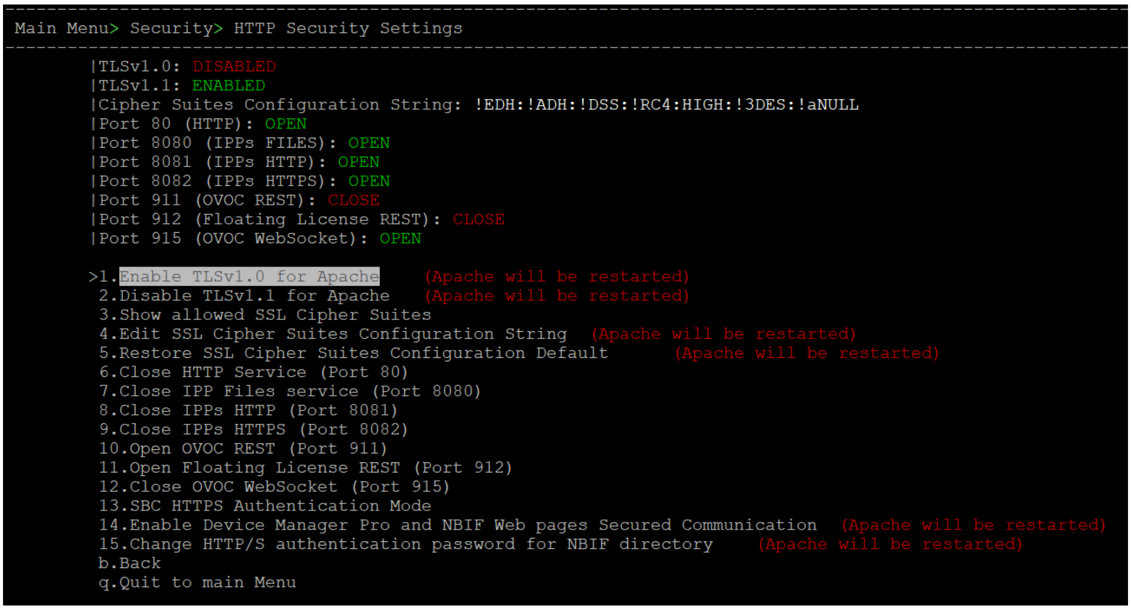
2. Choose one of the following transport types:

   - TCP (opens port 5000)
   - TLS (opens port 5001)
   - TLS/TCP (this setting opens both ports 5000 and 5001).

HTTP Security Settings

From the OVOC Server Managerroot menu, choose **HTTP Security Settings.**

Figure 25-28: HTTP Security Settings



```
 Main Menu> Security> HTTP Security Settings
        |TLSv1.0: DISABLED
        |TLSv1.1: ENABLED
        |Cipher Suites Configuration String: !EDH:!ADH:!DSS:!RC4:HIGH:!3DES:!aNULL
        |Port 80 (HTTP): OPEN
        |Port 8080 (IPPs FILES): OPEN
        |Port 8081 (IPPs HTTP): OPEN
        |Port 8082 (IPPs HTTPS): OPEN
        |Port 911 (OVOC REST): CLOSE
        |Port 912 (Floating License REST): CLOSE
        |Port 915 (OVOC WebSocket): OPEN

        >1.Enable 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)
         5.Restore SSL Cipher Suites Configuration Default       (Apache will be restarted)
         6.Close HTTP Service (Port 80)
         7.Close IPP Files service (Port 8080)
         8.Close IPPs HTTP (Port 8081)
         9.Close IPPs HTTPS (Port 8082)
         10.Open OVOC REST (Port 911)
         11.Open Floating License REST (Port 912)
         12.Close OVOC WebSocket (Port 915)
         13.SBC HTTPS Authentication Mode
         14.Enable Device Manager Pro and NBIF Web pages Secured Communication  (Apache will be restarted)
         15.Change HTTP/S authentication password for NBIF directory     (Apache will be restarted)
         b.Back
         q.Quit to main Menu
```

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

- TLS Version 1.0 (TLS Version 1.0 on the next page)
- TLS Version 1.1 (TLS Version 1.1 on the next page)
- Show Allowed SSL Cipher Suites (Show Allowed SSL Cipher Suites on page 242)

- Edit SSL Cipher Suites Configuration String (Edit SSL Cipher Suites Configuration String on the next page)
- Restore SSL Cipher Suites Configuration Default (Restore SSL Cipher Suites Configuration Default on page 243)
- Manage HTTP Service (Port 80) (Manage HTTP Service Port (80) on page 243)
- Manage IPP Files Service (Port 8080) (Manage IPP Files Service Port (8080) on page 243)
- Manage IPPs HTTP (Port 8081) (Manage IPPs HTTP Port (8081) on page 244)
- Manage IPPs HTTPS (Port 8082) (Manage IPPs HTTPS Port (8082) on page 244)
- OVOC REST (Port 911) (OVOC Rest (Port 911) on page 244
- Floating License REST (Port 912) (Floating License (Port 912) on page 244
- OVOC WebSocket (Port 915) OVOC WebSocket (Port 915) on page 245
- SBC HTTPS Authentication (SBC HTTPS Authentication Mode on page 245)
- Enable Device Manager Pro and NBIF Web Pages Secured Communication (Enable Device Manager Pro and NBIF Web Pages Secured Communication on page 246)
- Change HTTP/S Authentication Password for NBIF Directory (Change HTTP/S Authentication Password for NBIF Directory on page 246)

TLS Version 1.0

This option enables/disables TLS Version 1.0 on port 443 (Apache server is restarted).

➢ To enable or disable TLS Version 1.0:

- From the HTTP Security Settings menu, select option **Enable TLSv1.0 for Apache**.

> When TLS Version 1.1 is disabled, TLS Version 1.0 is also disabled. Likewise, if TLS Version1.0 is enabled, TLS Version 1.1 is also enabled.

Apache server is restarted. Default (enabled).

TLS Version 1.1

This option enables/disables TLS Version 1.1 on port 443 (Apache server is restarted).

➢ To enable or disable TLS Version 1.1:

- From the HTTP Security Settings menu, select option **Enable TLSv1.1 for Apache**.

  Default (enabled). Apache server is restarted.

> - When TLS Version 1.1 is disabled, TLS Version 1.0 is also disabled. Likewise, if TLS Version 1.0 is enabled, TLS Version 1.1 is also enabled.

Show Allowed SSL Cipher Suites

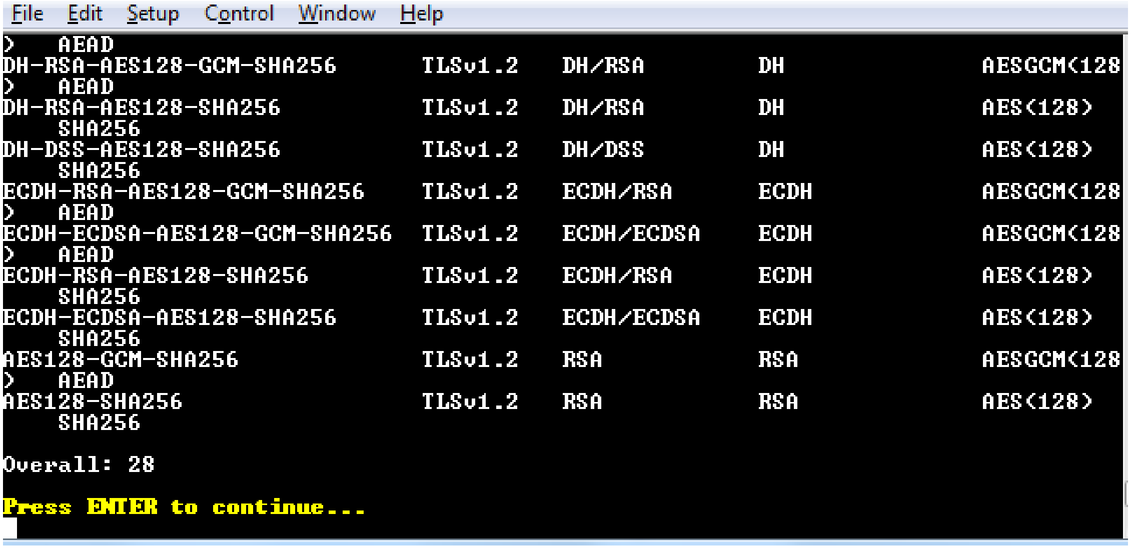
This option allows you to view the currently configured SSL cipher suites.

➢ **To show allowed SSL cipher suites:**

1. From the HTTP Security Settings menu, select option **Show Allowed SSL Cipher Suites**.

   The currently configured SSL cipher suites are displayed. The overall figure indicates the total number of entries.

Figure 25-29: 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...
```

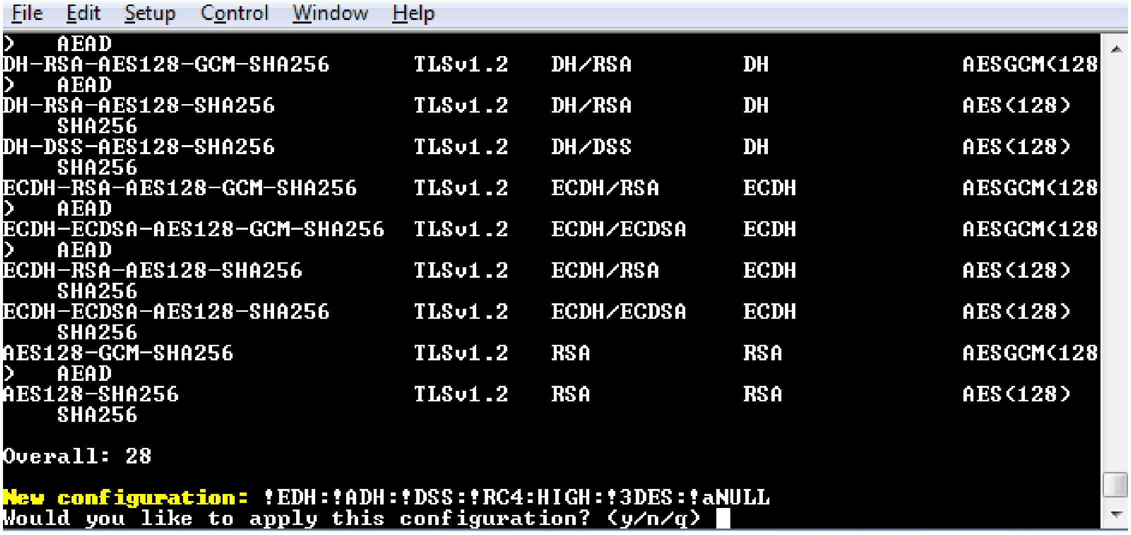
Edit SSL Cipher Suites Configuration String

This option allows you to edit the SSL Cipher Suites configuration string.

➢ **To edit the SSL cipher suites configuration string:**

1. From the HTTP Security Settings menu, select option **Edit SSL Cipher Suites Configuration String**.

Figure 25-30: 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.

Restore SSL Cipher Suites Configuration Default

This option allows you to restore the SSL Cipher Suites to the OVOC default values.

➢ To restore the SSL Cipher Suites Configuration default:

- From the HTTP Security Settings menu, select **Restore SSL Cipher Suites Configuration Default**.

Manage HTTP Service Port (80)

➢ To open/close HTTP Service (Port 80):

- In the HTTP Security Settings menu, choose option **Open/Close HTTP Service (Port 80)**, and then press Enter.

  This HTTP port is used for the connection between the OVOC server and all AudioCodes devices with the Device Manager Pro Web browser

Manage IPP Files Service Port (8080)

➢ To open/close IPPs files service (port 8080):

- In the HTTP Security Settings menu, choose option **Open/Close IPPs files(Port 8080)**, and then press Enter.

  This HTTP port is used for downloading firmware and configuration files from the OVOC server to the endpoints.

⚠ This option is reserved for backward compatibility with older device versions.

Manage IPPs HTTP Port (8081)

➢ To open/close IPPs HTTP (Port 8081):

- In the HTTP Security Settings menu, choose option **Open/Close IPPs HTTP (Port 8081)**, and then press Enter.

  This HTTP port is used for sending REST updates from the endpoints to the OVOC server, such as alarms and statuses.

⚠ This option is reserved for backward compatibility with older device versions.

Manage IPPs HTTPS Port (8082)

➢ To open/close IPPs HTTPS (Port 8082):

- In the HTTP Security Settings menu, choose option **Open/Close IPPs HTTPS (Port 8082)**, and then press Enter.

  This HTTPS port is used for sending secure REST updates from the endpoints to the OVOC server, such as alarms and statuses (HTTPS without certificate authentication).

⚠ This option is reserved for backward compatibility with older device versions.

OVOC Rest (Port 911)

This option allows you to open and close the REST port connection for (internal) port and server debugging.

➢ To configure OVOC REST:

1. From the HTTP Security Settings menu, choose option **Open/Close OVOC REST (Port 911)**.

Floating License (Port 912)

This option allows you to open and close the Floating license REST service (internal) and Floating license service debugging.

➢ To open/close the Floating License port:

1. From the HTTP Security Settings menu, choose option **Open/Close Floating License REST (Port 912)**.

OVOC WebSocket (Port 915)

This option allows you to open and close the OVOC WebSocket (Port 915) connection between the Websocket client and OVOC server.

➢ To open/close the WebSocket port:

1. From the HTTP Security Settings menu, choose option **Open/Close OVOC WebSocket (Port 915)**.

SBC HTTPS Authentication Mode

This option enables you to configure whether certificates are used to authenticate the connection between the OVOC server and the devices in one direction or in both directions:

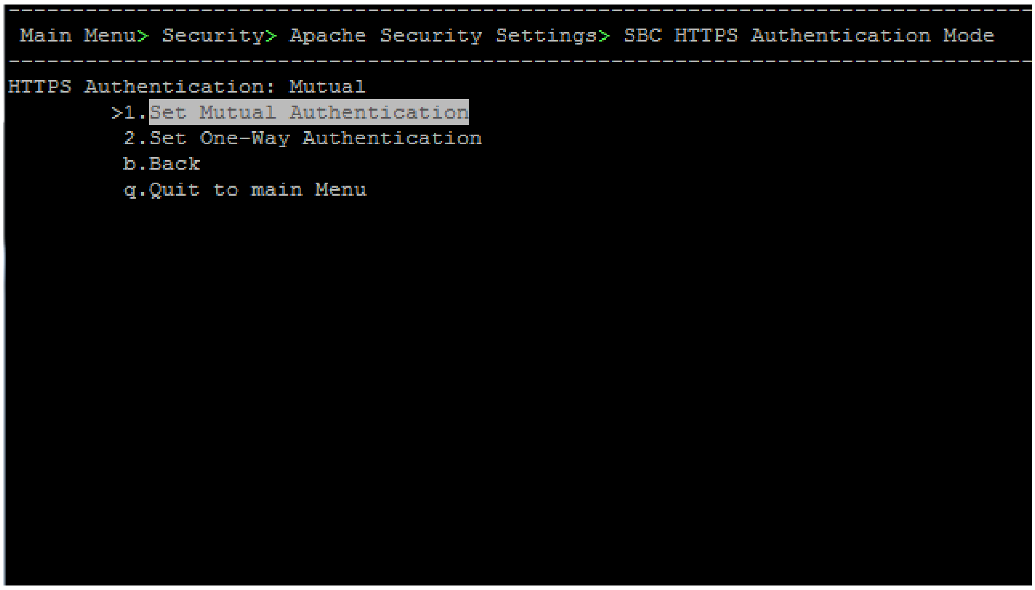
- **Mutual Authentication:** the OVOC authenticates the device connection request using certificates and the device authenticates the OVOC connection request using certificates. When this option is configured:
  - The same root CA must sign the certificate that is loaded to the device and certificate that is loaded to the OVOC server.
  - Mutual authentication must also be enabled on the device (Step 5: Configure HTTPS Parameters on the Device on page 287).
- **One-way Authentication option:** the OVOC does not authenticate the device connection request using certificates; only the device authenticates the OVOC connection request.

> ⚠ You can use the procedure described in Server Certificates Update on page 234 to load the certificate file to the OVOC server.

➢ To enable HTTPS authentication:

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

Figure 25-31: SBC HTTPS Authentication



```
--------------------------------------------------------------------------------
 Main Menu> Security> Apache Security Settings> SBC HTTPS Authentication Mode
--------------------------------------------------------------------------------
HTTPS Authentication: Mutual
        >1.Set Mutual Authentication
         2.Set One-Way Authentication
         b.Back
         q.Quit to main Menu
```

2. Choose one of the following options:

   - 1-Set Mutual Authentication
   - 2. Set One-Way Authentication

Enable Device Manager Pro and NBIF Web Pages Secured Communication

This menu option enables you to secure the connection between the Device Manager Server and NBIF Web pages and the Apache server over HTTPS. When this option is enabled, the connection is secured through HTTPS port 443 (instead of port 80-HTTP).

➢ To secure connection the Device Manager Pro and NBIF Web pages connection:

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

Change HTTP/S Authentication Password for NBIF Directory

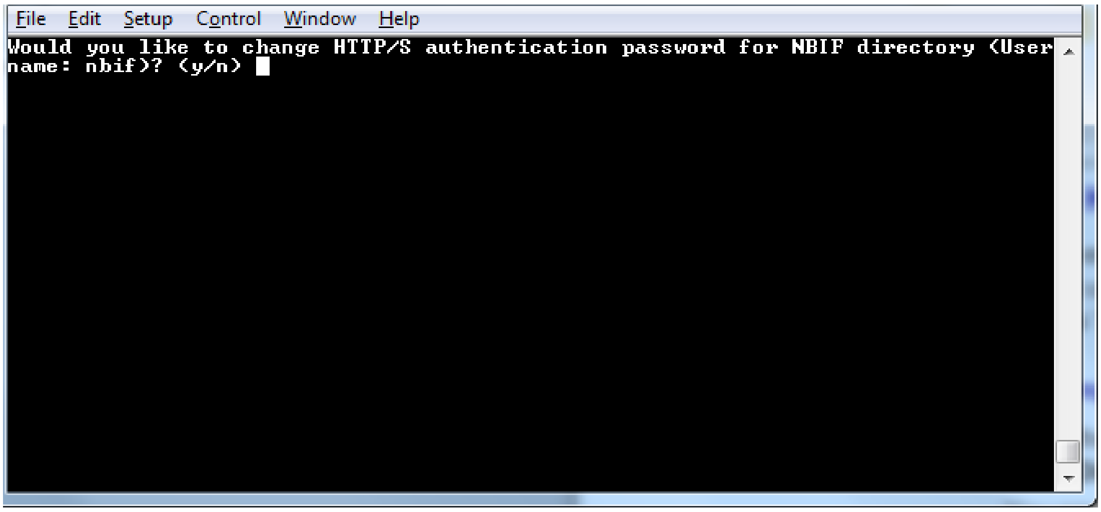
This option enables you to change the password for logging to the OVOC client from a NBIF client over an HTTP/S connection. The default user name is “nbif” and default password is “pass_1234”.

➢ To change the HTTP/S authentication password:

1. From the HTTP Security Settings menu, select **Change HTTP/S Authentication Password for NBIF Directory**.

   You are prompted to change the HTTP/S authentication password. Enter **y** to change the password.

Figure 25-32: Change HTTP/S Authentication Password for NBIF Directory



```
Would you like to change HTTP/S authentication password for NBIF directory (User
name: nbif)? (y/n)
```

2. Enter the new password.
3. Reenter the new password.

A confirmation message is displayed and the Apache server is restarted.

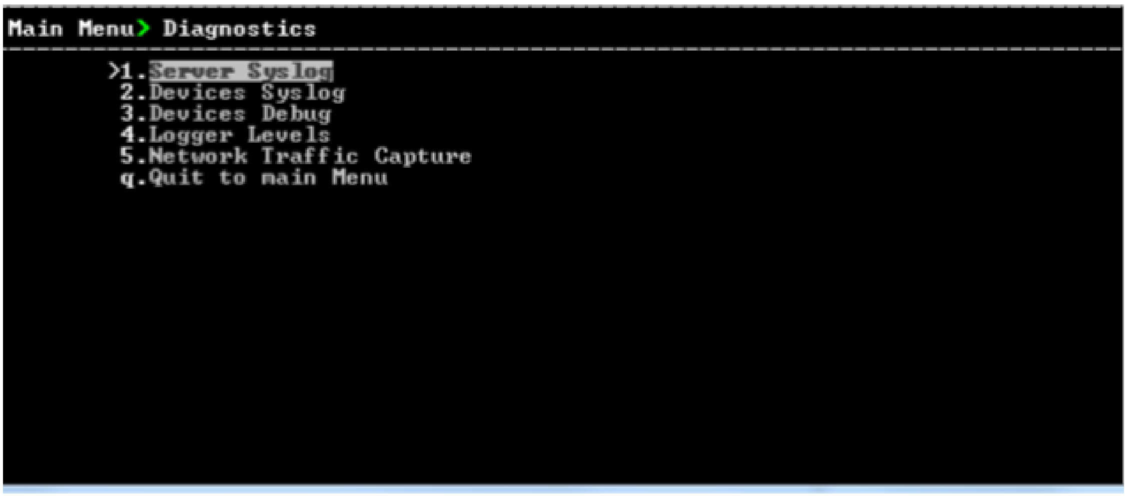
26 Diagnostics

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

➢ **To run OVOC server diagnostics:**

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

Figure 26-1: Diagnostics



```
Main Menu> Diagnostics
        >1.Server Syslog
         2.Devices Syslog
         3.Devices Debug
         4.Logger Levels
         5.Network Traffic Capture
         q.Quit to main Menu
```

This menu includes the following options:

- Server Syslog Configuration (Server Syslog Configuration below).
- Devices Syslog Configuration (Devices Syslog Configuration on page 250).
- Devices Debug Configuration (Devices Debug Configuration on page 251).
- ServerLogger Levels (Server Logger Levels on page 252)
- Network Traffic Capture (see Network Traffic Capture on page 253)

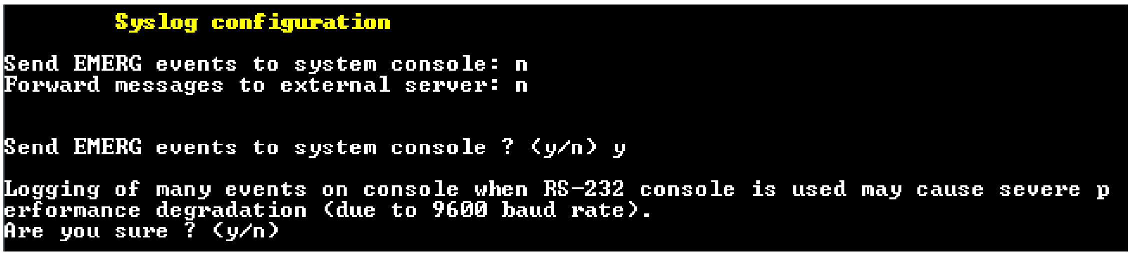
Server Syslog Configuration

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:**

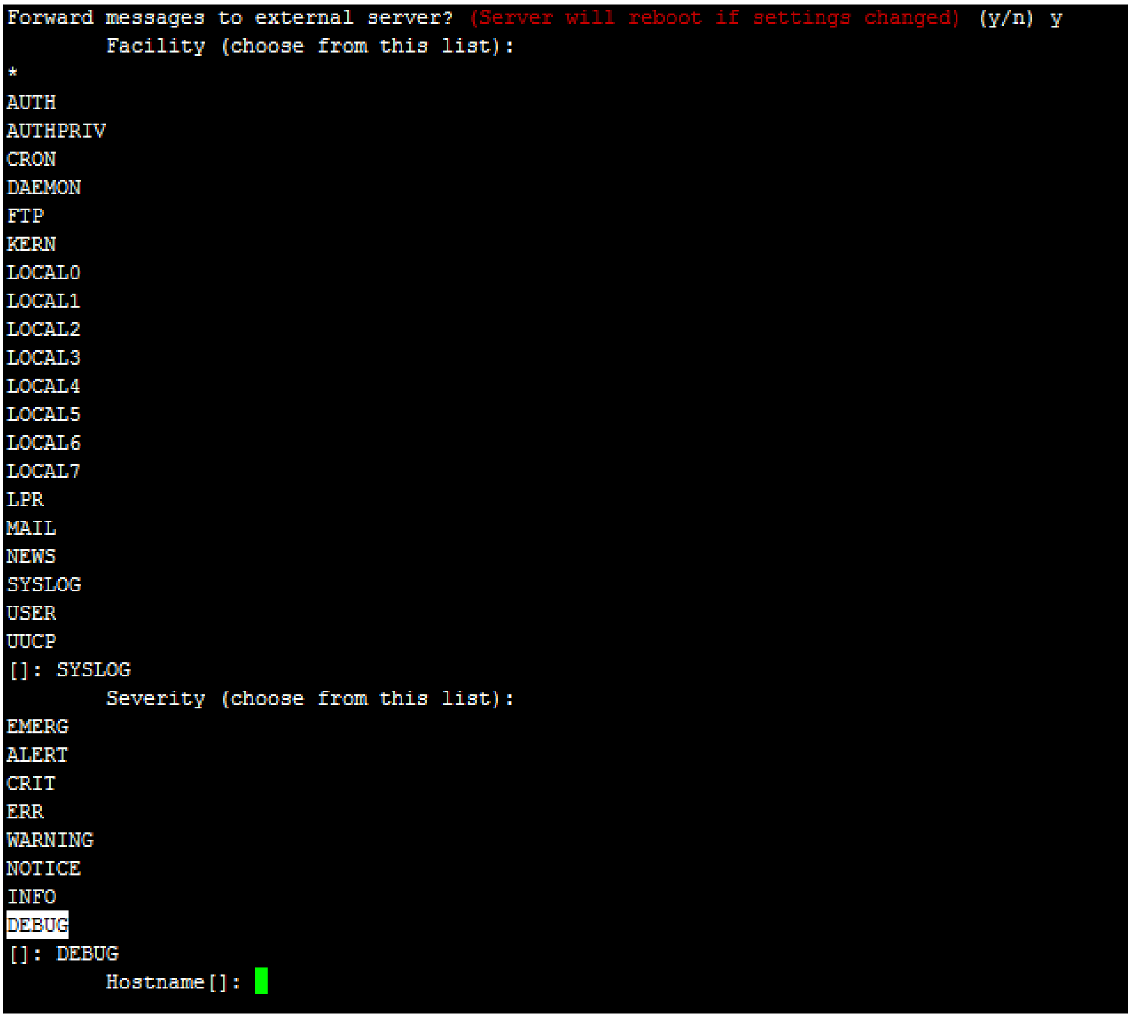
1. From the Diagnostics menu, choose **Server Syslog**, and then press Enter.
2. To send EMERG events to the system console, type **y**, press Enter, and then confirm by typing **y** again.

Figure 26-2: 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 26-3: Forward Messages to an External Server



```
Forward messages to external server? (Server will reboot if settings changed) (y/n) y
        Facility (choose from this list):
*
AUTH
AUTHPRIV
CRON
DAEMON
FTP
KERN
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7
LPR
MAIL
NEWS
SYSLOG
USER
UUCP
[]: SYSLOG
        Severity (choose from this list):
EMERG
ALERT
CRIT
ERR
WARNING
NOTICE
INFO
DEBUG
[]: DEBUG
        Hostname[]:
```

3. You are prompted to forward messages to an external server, type **y**, and then press Enter. If this is changed, the server is rebooted.

4. Type one of the following **Facilities** from the list (case-sensitive) or select the wildcard * to select all facilities in the list, and then press Enter:

   - auth and authpriv: for authentication;
   - cron: comes from task scheduling services, cron and atd;
   - daemon: affects a daemon without any special classification (DNS, NTP, etc.)
   - ftp: concerns the FTP server;

- kern: message coming from the kernel;
- lpr: comes from the printing subsystem;
- mail: comes from the e-mail subsystem;
- news: Usenet subsystem message (especially from an NNTP — Network News Transfer Protocol — server that manages newsgroups);
- syslog: messages from the syslogd server, itself;
- user: user messages (generic);
- uucp: messages from the UUCP server (Unix to Unix Copy Program, an old protocol notably used to distribute e-mail messages);
- local0 to local7: reserved for local use.

5. Each message is also associated with a **Severity** or priority level. Type one of the following severities (in decreasing order) and then press Enter:
   - **emerg**: “Help!” There's an emergency, the system is probably unusable.
   - **alert**: hurry up, any delay can be dangerous, action must be taken immediately;
   - **crit**: conditions are critical;
   - **err**: error;
   - **warn**: warning (potential error);
   - **notice**: conditions are normal, but the message is important;
   - **info**: informative message;
   - **debug**: debugging message.
6. Type the external server Hostname or IP address to which you wish to send the syslog.

Devices Syslog Configuration

The capture of the device's Syslog can be logged directly to the OVOC server without the need for a third-party Syslog server in the same local network. The OVOC Server Manageris used to enable this feature.

Syslog is captured according to the device's configured Syslog parameters. For more information, see the relevant device User's manual.

The user needs to also enable the monitored device to send syslog messages to the standard syslog port (UDP 514) on the OVOC server machine.

The syslog log file 'syslog' is located in the following OVOC server directory:

/data/NBIF/mgDebug/syslog

The syslog file is automatically rotated once a week or when it reaches 100 MB. Up to four syslog files are stored.

➢ **To enable device syslog logging:**

1. From the Diagnostics menu, choose **Devices Syslog**, and then press Enter.
2. You are prompted whether you wish to send EMER events to system console; type **Y** or **N**.
3. You are prompted whether you wish to send events to an external server; type **Y** or **N**.

Devices Debug Configuration

Debug recordings packets from all managed machines can be logged directly to the OVOC server without the need for a 3rd party network sniffer in the same local network.

⚠ Debug recording packets are collected according to the AudioCodes device's configured Debug parameters. For more information, see the relevant device User's Manual.

The OVOC server runs the Wireshark network sniffer, which listens on a particular configured port. The sniffer records the packets to a network capture file in the Debug Recording (DR) directory. You can then access this file from your PC through FTP.

The OVOC Server Manageris used to enable this feature. The user should configure the monitored device to send its debug record messages to a specific port (UDP 925) on the OVOC server IP.

The DR capture file is located in the following OVOC server directory:

/data/NBIF/mgDebug/DebugRecording

The file ‘TPDebugRec<DATE>.cap’ is saved for each session. The user is responsible for closing (stopping) each debug recording session. In any case, each session (file) is limited to 10MB or one hour of recording (the first rule which is met causes the file to close i.e. if the file reaches 10MB in less than an hour of recording, it is closed). A cleanup process is run daily, deleting capture files that are 5 days old.

The user is able to retrieve this file from the OVOC server and open it locally on their own PC using Wireshark with the debug recording plug-in installed (Wireshark version 1.6.2 supports the Debug Recording plug-in).

➢ **To enable or disable devices debug:**

1. From the Diagnostics menu, choose **Devices Debug**, and then press Enter.

   A message is displayed indicating that debug recording is either enabled or disabled.

2. Type **y**, and then press Enter.

   Recording files are saved in /data/NBIF/mgDebug directory on the server.

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

Server Logger Levels

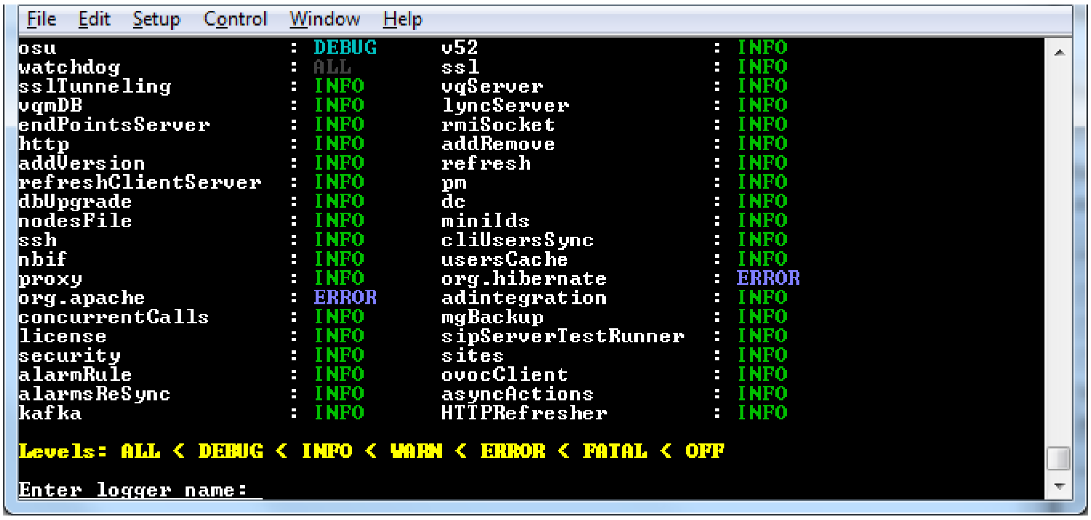
This option allows you to change the log level for the different OVOC server log directories.

After completing the debugging, revert to the previous configuration to prevent over utilization of CPU resources.

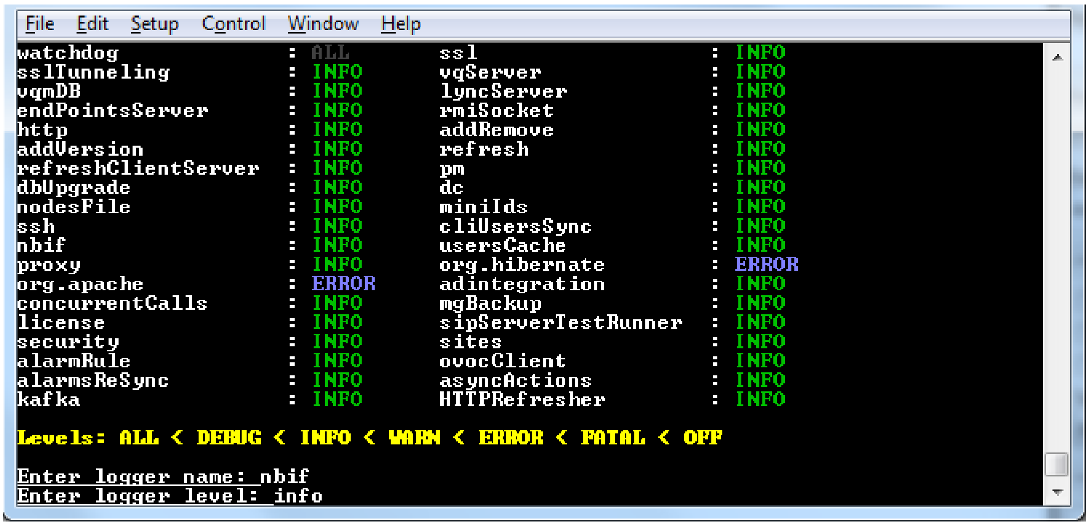
➢ To change the <tc> server logger level:

1. From the Diagnostics menu, choose **Logger Levels**.
2. Enter the name of the log whose level you wish to change.
3. Enter the desired logger level.
4. Select **Yes** at the prompt to confirm the change.

Figure 26-4: Server Logger Name and Level



```
osu                    : DEBUG     v52                   : INFO
watchdog               : ALL       ssl                   : INFO
sslTunneling           : INFO      vqServer              : INFO
vqmDB                  : INFO      lyncServer            : INFO
endPointsServer        : INFO      rmiSocket             : INFO
http                   : INFO      addRemove             : INFO
addVersion             : INFO      refresh               : INFO
refreshClientServer    : INFO      pm                    : INFO
dbUpgrade              : INFO      dc                    : INFO
nodesFile              : INFO      miniIds               : INFO
ssh                    : INFO      cliUsersSync          : INFO
nbif                   : INFO      usersCache            : INFO
proxy                  : INFO      org.hibernate         : ERROR
org.apache             : ERROR     adintegration         : INFO
concurrentCalls        : INFO      mgBackup              : INFO
license                : INFO      sipServerTestRunner   : INFO
security               : INFO      sites                 : INFO
alarmRule              : INFO      ovocClient            : INFO
alarmsReSync           : INFO      asyncActions          : INFO
kafka                  : INFO      HTTPRefresher         : INFO

Levels: ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

Enter logger name: _
```



```
watchdog                : ALL       ssl                    : INFO
sslTunneling            : INFO      vqServer               : INFO
vqmDB                   : INFO      lyncServer             : INFO
endPointsServer         : INFO      rmiSocket              : INFO
http                    : INFO      addRemove              : INFO
addVersion              : INFO      refresh                : INFO
refreshClientServer     : INFO      pm                     : INFO
dbUpgrade               : INFO      dc                     : INFO
nodesFile               : INFO      miniIds                : INFO
ssh                     : INFO      cliUsersSync           : INFO
nbif                    : INFO      usersCache             : INFO
proxy                   : INFO      org.hibernate          : ERROR
org.apache              : ERROR     adintegration          : INFO
concurrentCalls         : INFO      mgBackup               : INFO
license                 : INFO      sipServerTestRunner    : INFO
security                : INFO      sites                  : INFO
alarmRule               : INFO      ovocClient             : INFO
alarmsReSync            : INFO      asyncActions           : INFO
kafka                   : INFO      HTTPRefresher          : INFO

Levels: ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

Enter logger name: nbif
Enter logger level: info
```

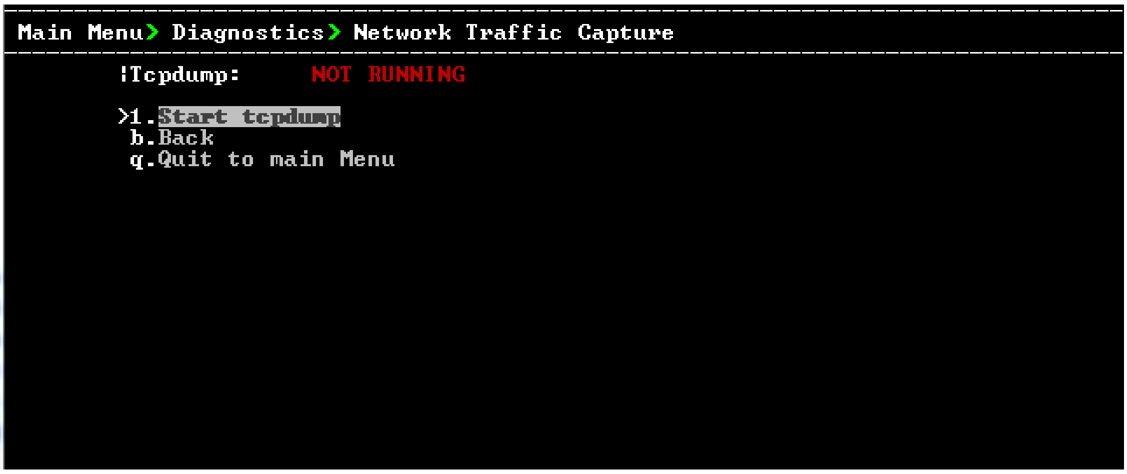
Network Traffic Capture

Network traffic can be captured to a PCAP capture file according to a list of IP addresses and ports and a specified time period. The PCAP files can later be opened with a network sniffer program such as Wireshark.

➢ To capture TCP traffic:

1. From the Diagnostics menu, choose option **Network Traffic Capture.**

Figure 26-5: Network Traffic Capture

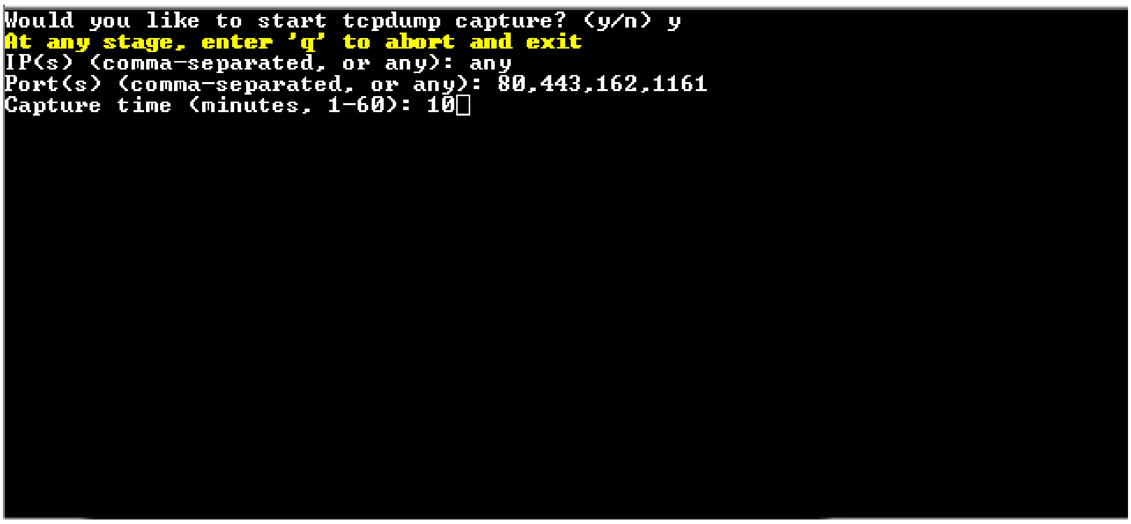


```
---------------------------------------------------------------------------
 Main Menu> Diagnostics> Network Traffic Capture
---------------------------------------------------------------------------
        |Tcpdump:      NOT RUNNING

        >1.Start tcpdump
         b.Back
         q.Quit to main Menu
```

2. Select option **1 Start tcpdump.**

3. Select **y** to start the tcpdump.

Figure 26-6: TCP Dump

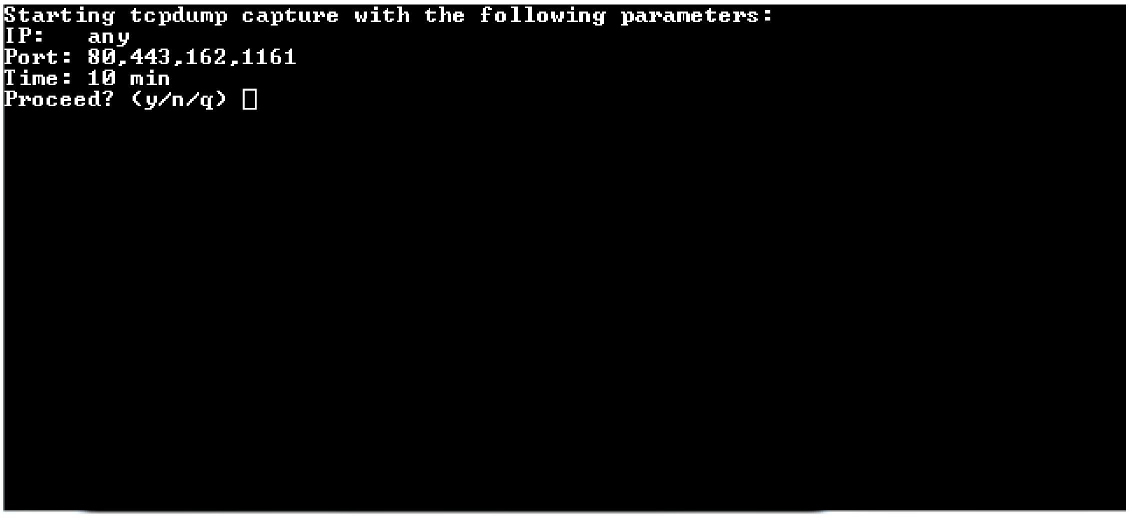


```
Would you like to start tcpdump capture? (y/n) y
At any stage, enter 'q' to abort and exit
IP(s) (comma-separated, or any): any
Port(s) (comma-separated, or any): 80,443,162,1161
Capture time (minutes, 1-60): 10
```

4. Enter comma separated IP address (es) or accept the default "any" IP address.

5. Enter comma separated port (s) or accept the default "any".

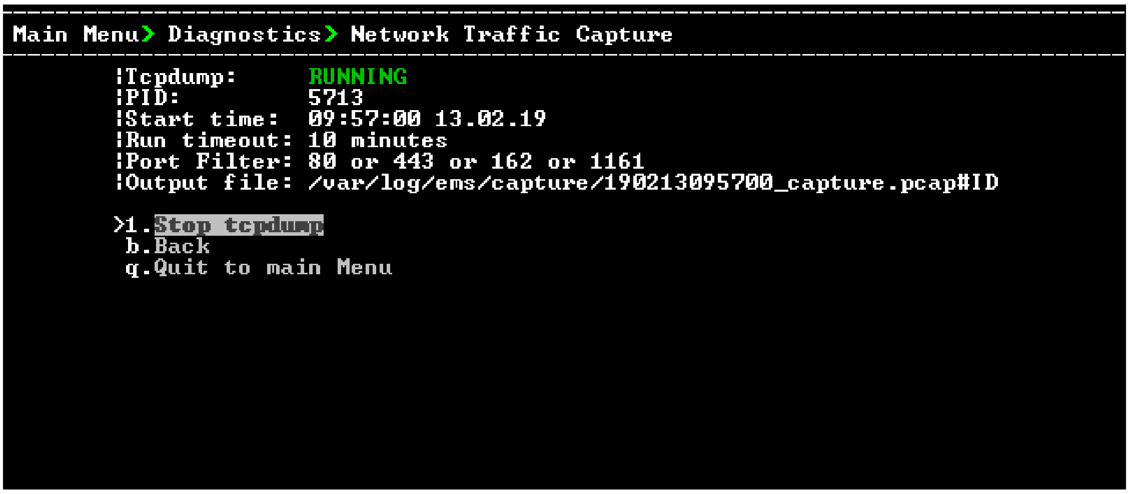
6. Enter the capture time (in minutes). Default: network traffic for the last ten minutes is captured.



```
Starting tcpdump capture with the following parameters:
IP:    any
Port: 80,443,162,1161
Time: 10 min
Proceed? (y/n/q)
```

7. Select **y** to proceed.

Figure 26-7: TCP Dump Running



```
Main Menu> Diagnostics> Network Traffic Capture

        |Tcpdump:      RUNNING
        |PID:          5713
        |Start time:   09:57:00 13.02.19
        |Run timeout:  10 minutes
        |Port Filter:  80 or 443 or 162 or 1161
        |Output file:  /var/log/ems/capture/190213095700_capture.pcap#ID

        >1.Stop tcpdump
         b.Back
         q.Quit to main Menu
```

Part VI

Configuring the Firewall

This part describes how to configure the OVOC firewall.

27 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 27-1: Firewall Configuration Rules

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC clients and OVOC server					
TCP/IP client ↔ OVOC server	TCP	√	22	SSH communication between OVOC server and TCP/IP client. Initiator: client PC	OVOC server side / Bi-directional.
HTTPS/NBIF Clients ↔ OVOC server	TCP (HTTPS)	√	443	Connection for OVOC/ NBIF clients. Initiator: Client	OVOC server side / Bi-directional
REST client	TCP (HTTP)	×	911	Connection for OVOC server REST (internal) port and server debugging. Initiator (internal): OVOC server Initiator (debugging): REST client	OVOC server side / Bi-directional
	TCP (HTTP)	×	912	Floating license REST service	OVOC server side / Bi-

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				(internal) communication and Floating license service debugging. Initiator (internal): OVOC server Initiator (debugging): REST client	directional
Microsoft Teams↔ OVOC Communication	TCP (HTTPS)	√	5010	Connection to Microsoft Teams Intiator: Microsoft Teams	OVOC server side / Receive only
WebSocket Client ↔ OVOC Server Communication	TCP (HTTP)	√	915	WebSocket Client and OVOC Server communication (internal) according to RFC 6455, used for managing the alarm and task notification mechanism in the OVOC Web. Initiator (internal): WebSocket Client	OVOC server side / Bi-directional
OVOC server and OVOC Managed Devices					
Device ↔ OVOC server (SNMP)	UDP	√	1161	Keep-alive - SNMP trap listening port (used	OVOC server side / Receive only

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				predominantly for devices located behind a NAT). Used also by Fixed License Pool and Floating License Service. Initiator: AudioCodes device	
	UDP	√	162	SNMP trap listening port on the OVOC. Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	√	161	SNMP Trap Manager port on the device that is used to send traps to the OVOC server. Used also by Fixed License Pool and Floating License Service. Initiator: OVOC server	MG side / Bi-directional
Device↔ OVOC server (NTP Server)	UDP (NTP server)	✗	123	NTP server synchronization for external clock. Initiator: MG (and OVOC server, if	Both sides / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				configured as NTP client) Initiator: Both sides	
Device ↔ OVOC server	TCP (HTTP)	×	80	HTTP connection for files transfer and REST communication. Initiator: OVOC server	OVOC server side / Bi-directional
	TCP (HTTPS)	√	443	HTTPS connection for files transfer (upload and download) and REST communication. Initiator: OVOC server	OVOC server side / Bi-directional
Device↔ OVOC server Floating License Management	TCP (HTTPS)	√	443	HTTPS connection for files transfer (upload and download) and REST communication for device Floating License Management. Initiator: Device	OVOC server side / Bi-directional
Devices Managed by the Device Manager					
OVOC server ↔ Device Manager Pro	TCP (HTTP)	×	80	HTTP connection between the OVOC server and the Device Manager Pro	OVOC server side / Bi-Directional.

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				Web browser. Initiator: Client browser	
				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 Device 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	
OVOC server ↔ Endpoints (used for backward compatibility)	TCP (HTTP)	×	8080	HTTP connection that is used by endpoints for downloading firmware and	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				configuration files from the OVOC server. Initiator: Endpoint	
	TCP (HTTP)	×	8081	HTTP REST updates connection. It is recommended to use this connection when managing more than 5000 IP Phones. In this case, you should change the provisioning URL port from 80 to 8081 in the phone's configuration file. Initiator: Endpoint	OVOC server side / Bi-directional
	TCP (HTTPS)	√	8082	HTTPS REST updates connection (encryption only without SSL authentication). It is recommended to use this connection when managing more than 5000 IP Phones. In	OVOC server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				this case, you should change the provisioning URL port from 443 to 8082 in the phone's configuration file. Initiator: Endpoint	
OVOC Voice Quality Package Server and Devices					
Media Gateways ↔ Voice Quality Package	TCP	×	5000	XML based communication for control, media data reports and SIP call flow messages. Initiator: Media Gateway	OVOC server side / Bi-directional
	TCP (TLS)	√	5001	XML based TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device	OVOC server side / Bi-directional
Skype for Business MS-SQL Server					
OVOC Voice Quality Package server ↔ Skype for	TCP	√	1433	Connection between the OVOC server and the MS-SQL	Skype for Business SQL server side /

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Business MS-SQL Server				Skype for Business Server. This port should be configured with SSL. Initiator: OVOC server	Bi-directional
LDAP Active Directory Server					
Voice Quality Package ↔ Active Directory LDAP server (Skype for Business user authentication)	TCP	×	389	Connection between the Voice Quality Package server and the Active Directory LDAP server. Initiator: OVOC server	Active Directory server side/ Bi-directional
	TCP (TLS)	√	636	Connection between the Voice Quality Package server and the Active Directory LDAP server with SSL configured. Initiator: OVOC server	Active Directory server side/ Bi-directional
OVOC server ↔ Active Directory LDAP server (OVOC user authentication)	TCP	×	389	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users). Initiator: OVOC server	Active Directory server side/ Bi-directional

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
RADIUS Server					
OVOC server ↔ RADIUS server	TCP	×	1812	Direct connection between the OVOC server and the RADIUS server (when OVOC user is authenticated using RADIUS server). Initiator: OVOC server	OVOC server side / Bi-directional
AudioCodes Floating License Service					
OVOC server ↔AudioCodes Floating License Service	TCP	√	443	HTTPS for OVOC/ Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi-directional
External Servers					
OVOC server ↔ Mail Server	TCP	×	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC server ↔ Syslog Server	TCP	✗	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side /Bi-directional
OVOC server ↔ Debug Recording Server	UDP	✗	925	Trap Forwarding to Debug Recording server. Initiator: OVOC server	Debug Recording server /Bi-directiona
Voice Quality					
Voice Quality Package ↔ Endpoints (RFC 6035)	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-directiona l

Table 27-2: Northbound Interfaces Flows: NOC/OSS → OVOC

Source IP Address Range	Destination IP Address Range	Protocol	Secure	Source Port Range	Destination Port Range
NOC/OSS	OVOC	SFTP	√	1024 - 65535	20
		FTP	✗	1024 - 65535	21
		SSH	√	1024 - 65535	22

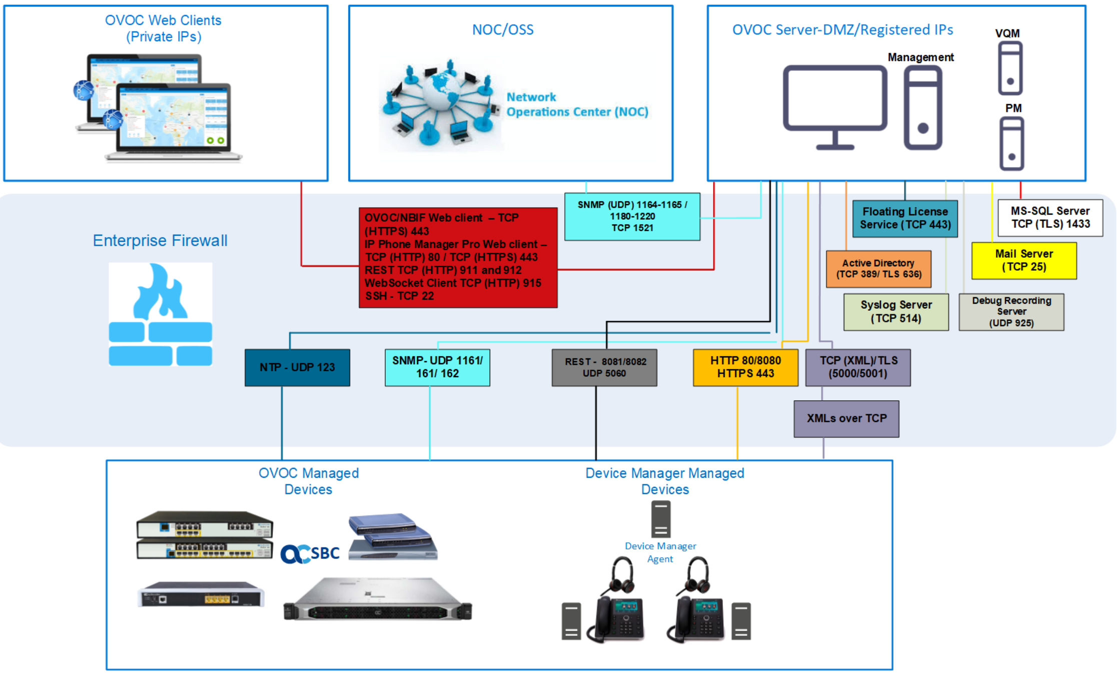
		Telnet	✗	1024 - 65535	23
		NTP	✗	123	123
		HTTP/HTTPS	✗/√	N/A	80/443
		SNMP (UDP) Set for the Active alarms Resync feature.	✗	N/A	161
		TCP connection for Data Analytics DB Access Initiator: DB Access client This port is open when the "Data Analytics" Voice Quality feature license has been purchased and the feature has been enabled (see Analytics API on page 187)	✗	N/A	1521

Table 27-3: OAM Flows: OVOC → NOC/OSS

Source IP Address Range	Destination IP Address Range	Protocol	Secure	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 - 1174	-
		SNMP (UDP) port for alarm forwarding	×	1180-1220	-

Figure 27-1: Firewall Configuration Schema


OVOC Web Clients
(Private IPs)
NOC/OSS
Network
Operations Center (NOC)
OVOC Server-DMZ/Registered IPs
Management
VQM
PM
Enterprise Firewall
OVOC/NBIF Web client – TCP (HTTPS) 443
IP Phone Manager Pro Web client – TCP (HTTP) 80 / TCP (HTTPS) 443
REST TCP (HTTP) 911 and 912
WebSocket Client TCP (HTTP) 915
SSH - TCP 22
SNMP (UDP) 1164-1165 / 1180-1220
TCP 1521
Floating License Service (TCP 443)
MS-SQL Server TCP (TLS) 1433
Active Directory (TCP 389/ TLS 636)
Mail Server (TCP 25)
Syslog Server (TCP 514)
Debug Recording Server (UDP 925)
NTP - UDP 123
SNMP- UDP 1161/ 161/ 162
REST - 8081/8082 UDP 5060
HTTP 80/8080 HTTPS 443
TCP (XML)/TLS (5000/5001)
XMLs over TCP
OVOC Managed Devices
SBC
Device Manager Managed Devices
Device Manager Agent

⚠ The above figure displays images of devices. For the full list of supported products, see Managed VoIP Equipment on page 3.

Configuring Firewall for Cloud Architecture Mode

When the OVOC server is deployed in a public cloud and the Cloud Architecture feature is enabled (see Configure OVOC Cloud Architecture Mode on page 115), all proprietary connections between SBC devices and the OVOC server are bundled into an HTTP/S tunnel overlay network over ports 80/443, therefore these ports must be open on the Enterprise firewall. Configuring other Enterprise firewall rules for SBC and OVOC server connections is not necessary.

Configuring Firewall for NAT Deployment

The table below describes the mandatory firewall rules to configure in the Enterprise firewall for connecting devices behind a NAT as described in Section Managing Device Connections on page 113.

Configuration Option	Ports to Configure	Port side / Flow Direction
SBC Devices		
Cloud Architecture Mode (Device > OVOC Server)	■ TCP HTTP 80 ■ TCP HTTPS 443	OVOC server side / Bi-directional
OVOC Server NAT Mode (OVOC > Devices)	SNMP UDP port 1161	OVOC server side / Receive only
	SNMP UDP port 162	OVOC server side / Receive only
	TCP 5000	OVOC server side / Bi-directional
	TCP 5001 (Voice Quality Management over TLS)	OVOC server side / Bi-directional
	NTP 123 NTP server port (configure the OVOC server's Public IP address as the NTP server)	Both sides / Bi-directional
Phones		
Device Manager Agent	TCP HTTPS Port 443	OVOC server side / Bi-Directional

Configuring Firewall for Service Provider Cluster

The table below describes the ports for the OVOC Service Provider Cluster mode.This table is applicable for the Management Server when Service Provider Cluster mode is enabled.

Table 27-4: OVOC Service Provider Cluster Mode

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
OVOC Clients and OVOC Server				
HTTP/REST	80	Public (MGMT)	×	OVOC Management server side / Bi-directional
	443	Public (MGMT)	√	OVOC Management server side / Bi-directional
REST	911	Private (MGMT)	×	OVOC Management server side / Bi-directional
Floating License	912	Private (MGMT)	×	OVOC Management server side / Bi-directional
Websocket	915	Private (MGMT)	×	OVOC Management server side / Bi-directional
OVOC Server and Managed Devices				
SNMP / Traps	1161	Public (MGMT)	√ (v3)	OVOC Management server side / Bi-directional
SNMP	161	Public (MGMT)	√ (v3)	OVOC Management server side / Bi-directional
SNMP Traps	162	Public (MGMT)	√ (v3)	OVOC Management server side / Bi-directional

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
NTP	123	Public (MGMT)	×	OVOC Management server side / Bi-directional
PM Server and Managed Devices				
HTTP REST connection used for polling managed devices.	80	Public (MGMT)	×	OVOC Management server side / Send only
HTTPS REST connection used for polling managed devices.	443	Public (MGMT)	√	OVOC Management server side / Send only
OVOC Voice Quality Package and SIP Publish				
Voice Quality Package	5000	Public (MGMT)	×	OVOC Management server side / Receive only
	5001	Public (MGMT)	√	OVOC Management server side / Receive only
SIP 6035	5060	Public (MGMT)	×	OVOC Management server side / Receive only
Phones				
IPP Files	8080	Public (MGMT)	×	OVOC Management server side / Bi-directional
IPP REST	8081	Public (MGMT)	×	OVOC Management

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
				server side / Bi-directional
IPP REST	8082	Public (MGMT)	√	OVOC Management server side / Bi-directional
External Servers				
Skype for Business	1433	Skype For Business Server	√	OVOC Management server side / Bi-directional
LDAP	389	LDAP Server	×	OVOC Management server side / Bi-directional
LDAP	636	LDAP Server	√	OVOC Management server side / Bi-directional
RADIUS	1812	On RADIUS Server	×	OVOC Management server side / Bi-directional
Mail Server (forwarding)	25	Mail Server	×	OVOC Management server side/ Bi-directional
Syslog Server	514	Syslog Server	×	OVOC Management server side / Bi-directional
Dedicated Cluster Node Ports				
Akka platform used for	2551..2555	Private (All)	×	OVOC

Connection Type	Ports to Configure	Access	Secured	Port side / Flow Direction
inter-process communication		Required access from cluster servers		Management server side/ Bi-directional
Java Database Connectivity (JDBC) used for communication with the PM server.	1521	Private (MGMT)	✗	OVOC Management server side / Bi-directional Accessible only from other PM/VQM servers
Kafka platform used for inter-process communication	9092	Private (All) Required access from cluster servers	✗	OVOC Management server side / Bi-directional
ZooKeeper	2181	Private (All) Required access from cluster servers	✗	OVOC Management server side / Bi-directional

Part VII

Appendix

This part describes additional OVOC server procedures.

28 Configuring RAID-0 for AudioCodes OVOC on HP ProLiant DL360p Gen10 Servers

This appendix describes the required equipment and the steps for configuring the HP ProLiant server to support RAID-0 Disk Array configuration for the OVOC server installation.

- This procedure erases any residual data on the designated disk drives.
- If you have purchased the server hardware from AudioCodes then this procedure is not necessary.

RAID-0 Prerequisites

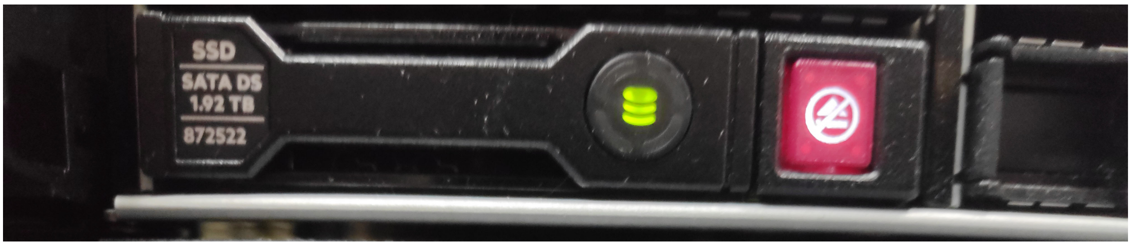
This procedure requires the following:

- ProLiant DL360p Gen10 server pre-installed in a compatible rack and connected to power.
- Two SATA DS 1.92 TB SSD disk drives
- A VGA display, USB keyboard, and USB mouse must be connected to the server back I/O panel.

RAID-0 Hardware Preparation

Make sure that two SATA DS 1.92 TB SSD disk drives are installed on slot 1 and 2 of the server. If required, refer to the *HP Service Manual*.

Figure 28-1: SATA DS 1.92 TB SSD Disks



Configuring RAID-0

The following procedures describe how to configure RAID-0 using the HP Smart Storage Administrator utility:

- Step 1 Create Logical Drive below
- Step 2 Set Logical Drive as Bootable Volume on the next page

Step 1 Create Logical Drive

This section describes how to create a logical drive on RAID-0.

➢ To create a logical drive on 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.
3. During reset, press <**F9**> to open the System Utilities.
4. Choose **Embedded Applications** > **Intelligent Provisioning** > **Smart Storage Administrator.**
5. Wait for the Smart Storage Administrator utility to finish loading.
6. In the left-hand pane, choose **HPE Smart Array Controllers** > **HPESmart Array E208i-a SRGen10**; an Actions menu is displayed.
7. Click **Configure**, and then click **Clear Configuration** to clear any previous configuration.
8. Click **Clear** to confirm; a summary display appears.
9. Click **Finish** to return to the main menu.
10. In the left-hand pane, select **Unassigned Drives (2)**; make sure that both the drives are selected, and then click **Create Array**.
11. Select **RAID 0** for RAID Level.
12. Select the 'Custom Size' check box, and then enter **2000GiB**.
13. At the bottom of the screen, click **Create Logical Drive**.

    After the array is created, a logical drive should be created.
14. Click **Finish**.
15. Proceed to Section Step 2 Set Logical Drive as Bootable Volume below

Step 2 Set Logical Drive as Bootable Volume

This section describes how to set the new logical drive as a bootable volume.

➢ To set new logical drive as bootable volume:

1. In the left-hand pane, select **HPE Smart Array E208i-a SR Gen10**, and then click **Set Bootable Logical Drive/Volume.**
2. Select the "Local - Logical Drive 1" as **Primary Boot Logical Drive/Volume**, and then click **Save**.

    A summary window is displayed.
3. Click **Finish**.
4. Exit the Smart Storage Administrator utility by clicking the **X** sign on the top right-hand side of the screen, and then confirm.
5. Click **Exit** at the bottom left-hand corner of the screen.

6. Click the **Power** icon in the upper right-hand corner of the screen.
7. Click **Reboot** to reboot the server.

   The Disk Array configuration is now complete.
8. Install the OVOC server (Installing the OVOC server on Dedicated Hardware).

29 Managing Clusters

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

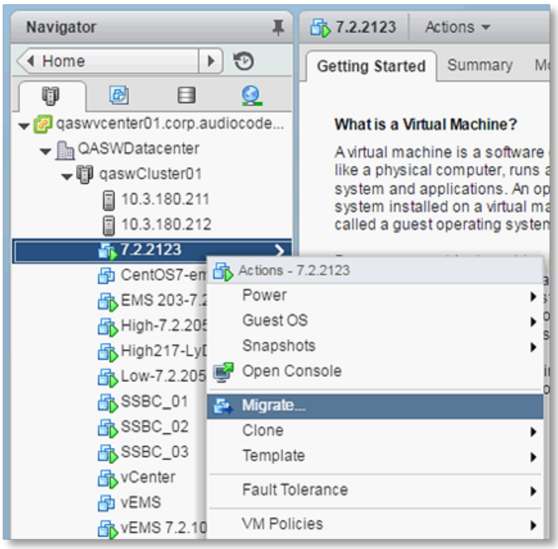
Migrating OVOC Virtual Machines in a VMware Cluster

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

➢ To migrate your OVOC VM:

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

Figure 29-1: Migration

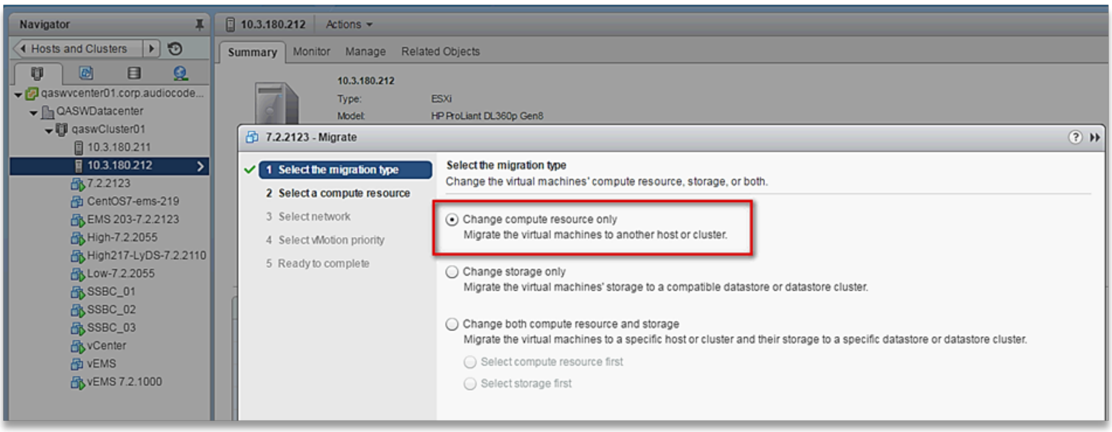


What is a Virtual Machine?

A virtual machine is a software
like a physical computer, runs a
system and applications. An op
system installed on a virtual ma
called a guest operating systen

2. Change a cluster host for migration:

Figure 29-2: Change Host



10.3.180.212
Type: ESXi
Model: HP ProLiant DL360p Gen8

Select the migration type
Change the virtual machines' compute resource, storage, or both.

● Change compute resource only
Migrate the virtual machines to another host or cluster.

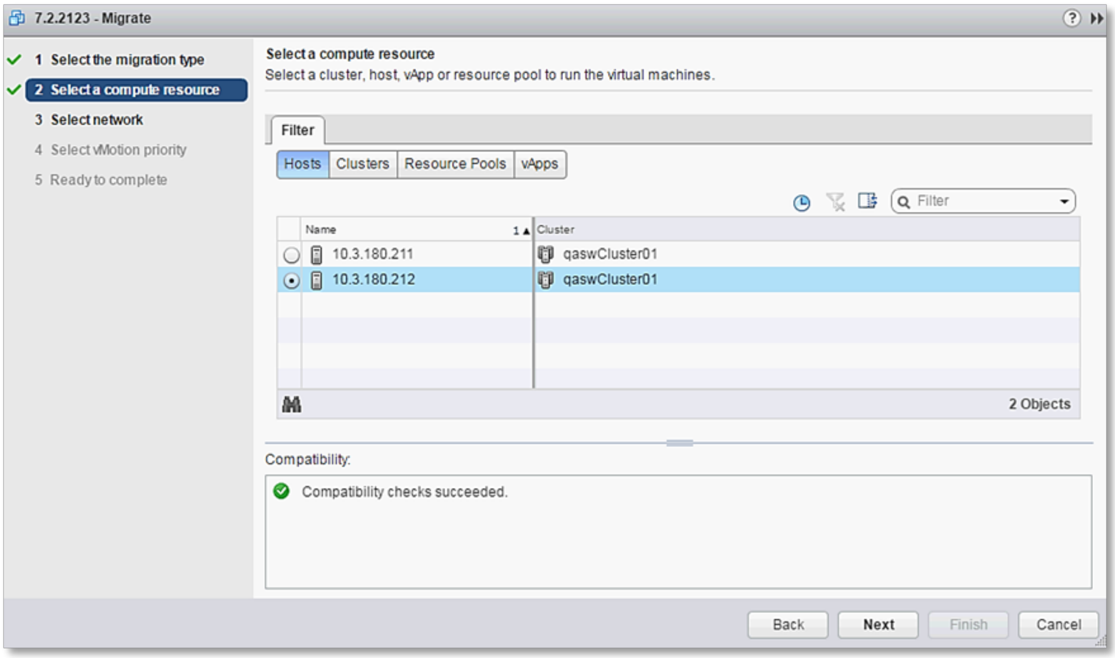
○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Select compute resource first
○ Select storage first

3. Choose the target host for migration:

Figure 29-3: Target Host for Migration



Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

	Name	Cluster
○	10.3.180.211	qaswCluster01
●	10.3.180.212	qaswCluster01

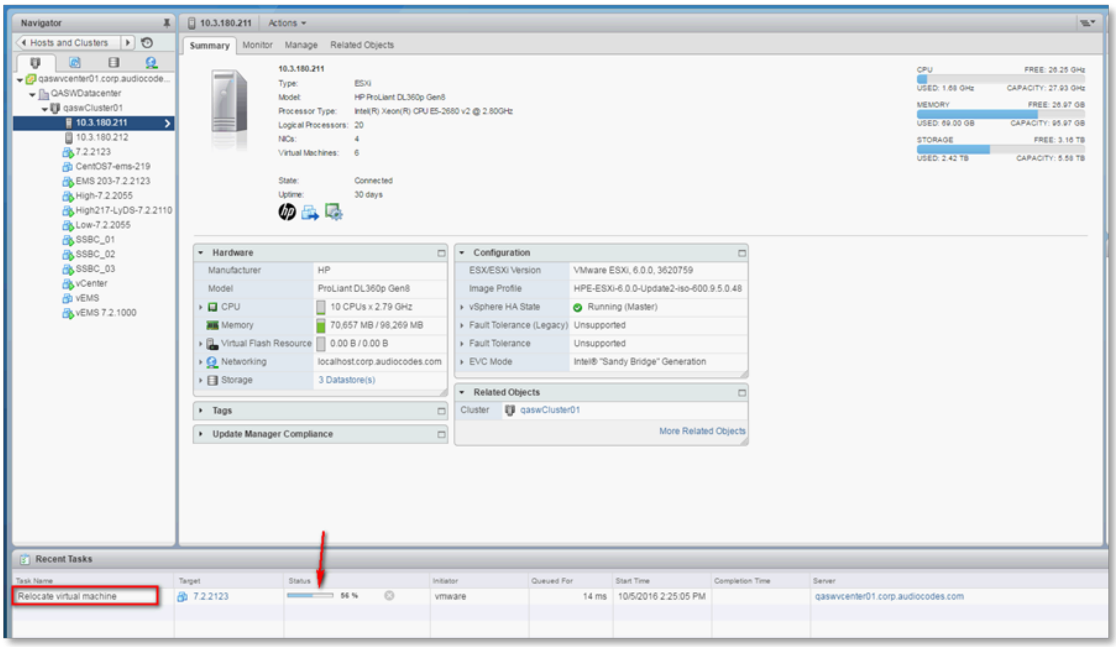
2 Objects

Compatibility:

✓ Compatibility checks succeeded.

The migration process commences:

Figure 29-4: Migration Process Started



10.3.180.211

Type: ESXi
Model: HP ProLiant DL360p Gen8
Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors: 20
NICs: 4
Virtual Machines: 6

State: Connected
Uptime: 30 days

CPU FREE: 26.25 GHz
USED: 1.68 GHz CAPACITY: 27.93 GHz
MEMORY FREE: 26.97 GB
USED: 69.00 GB CAPACITY: 95.97 GB
STORAGE FREE: 3.16 TB
USED: 2.42 TB CAPACITY: 5.58 TB

Hardware	
Manufacturer	HP
Model	ProLiant DL360p Gen8
CPU	10 CPUs x 2.79 GHz
Memory	70,657 MB / 98,269 MB
Virtual Flash Resource	0.00 B / 0.00 B
Networking	localhost.corp.audiocodes.com
Storage	3 Datastore(s)

Configuration	
ESX/ESXi Version	VMware ESXi, 6.0.0, 3620759
Image Profile	HPE-ESXi-6.0.0-Update2-iso-600.9.5.0.48
vSphere HA State	Running (Master)
Fault Tolerance (Legacy)	Unsupported
Fault Tolerance	Unsupported
EVC Mode	Intel® "Sandy Bridge" Generation

Related Objects	
Cluster	qaswCluster01

More Related Objects

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Relocate virtual machine	7.2.2123	56 %	vmware	14 ms	10/5/2016 2:25:05 PM		qaswvcenter01.corp.audiocodes.com

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

Moving OVOC VMs in a Hyper-V Cluster

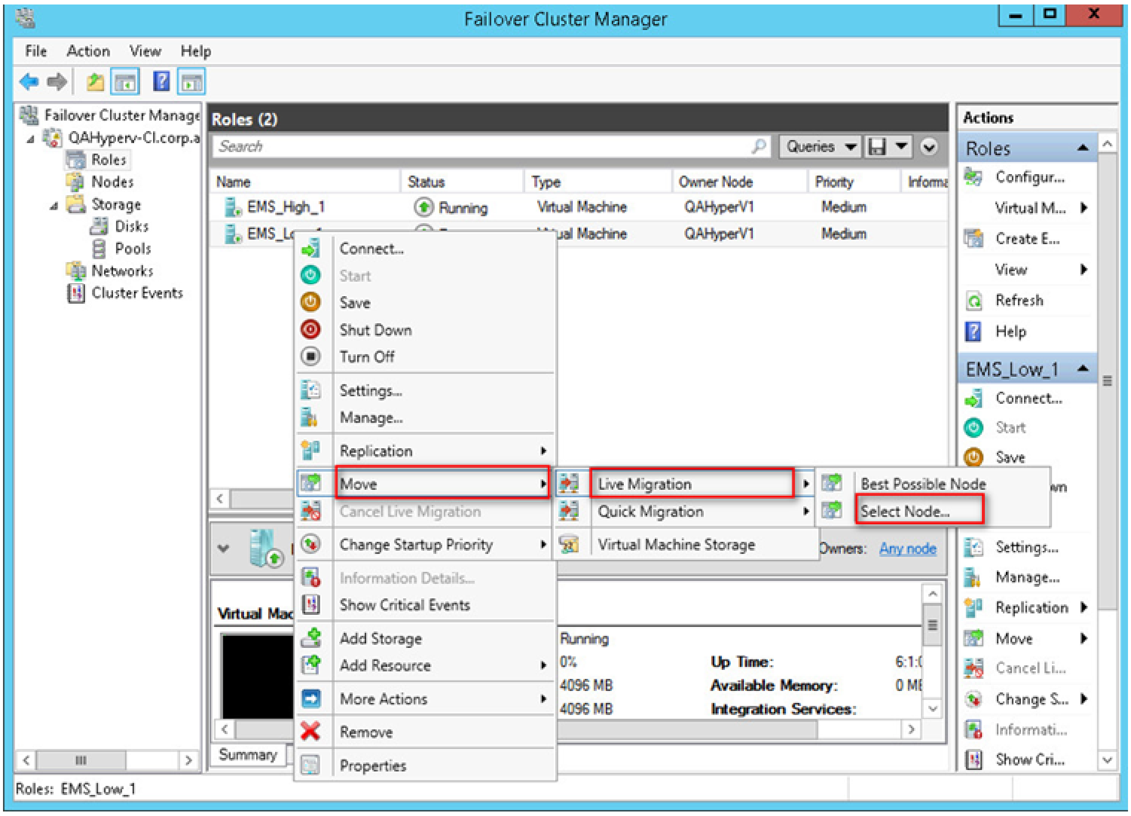
Moving OVOC VMs in a Hyper-V Cluster

This section describes how to move a Virtual Machine to another host node in a Hyper-V cluster.

➢ To move a Virtual Machine to another node of the cluster:

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

Figure 29-5: Hyper-V Live Migration

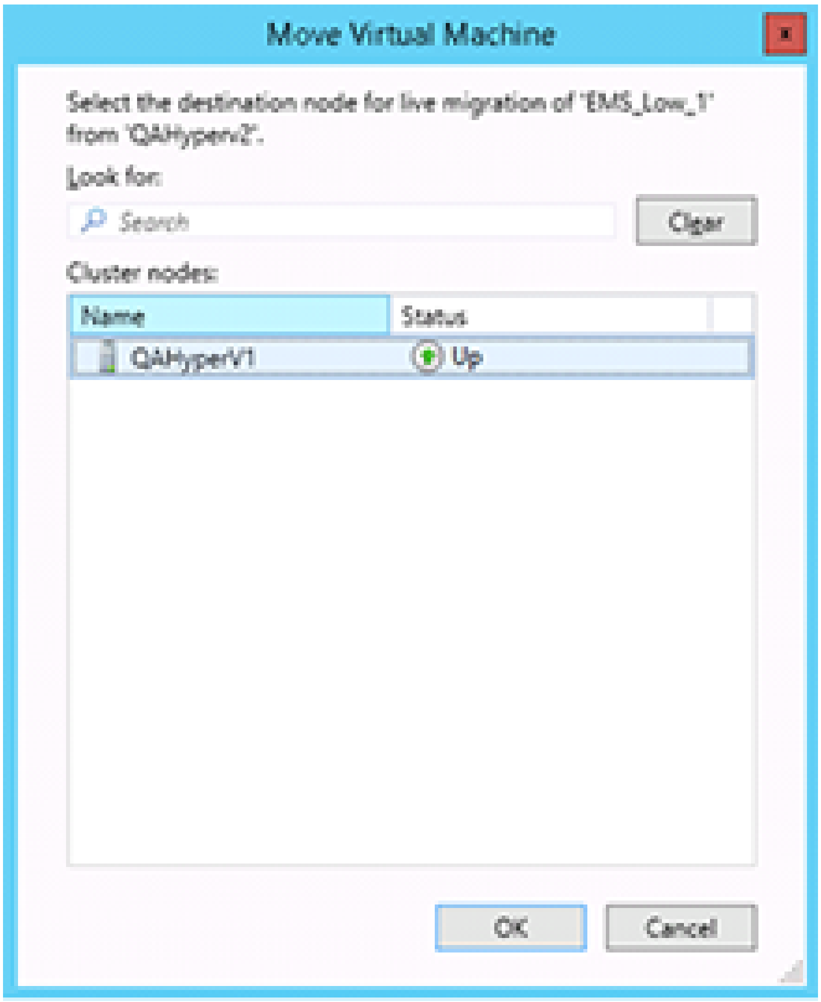


Name	Status	Type	Owner Node	Priority	Informa
EMS_High_1	Running	Virtual Machine	QAHyperV1	Medium	
EMS_L		ual Machine	QAHyperV1	Medium	

Running			
0%		Up Time:	6:1:(
4096 MB		Available Memory:	0 ME
4096 MB		Integration Services:	

The following screen is displayed:

Figure 29-6: Move Virtual Machine



Select the destination node for live migration of 'EMS_Low_1' from 'QAHyperv2'.

Look for:

Search

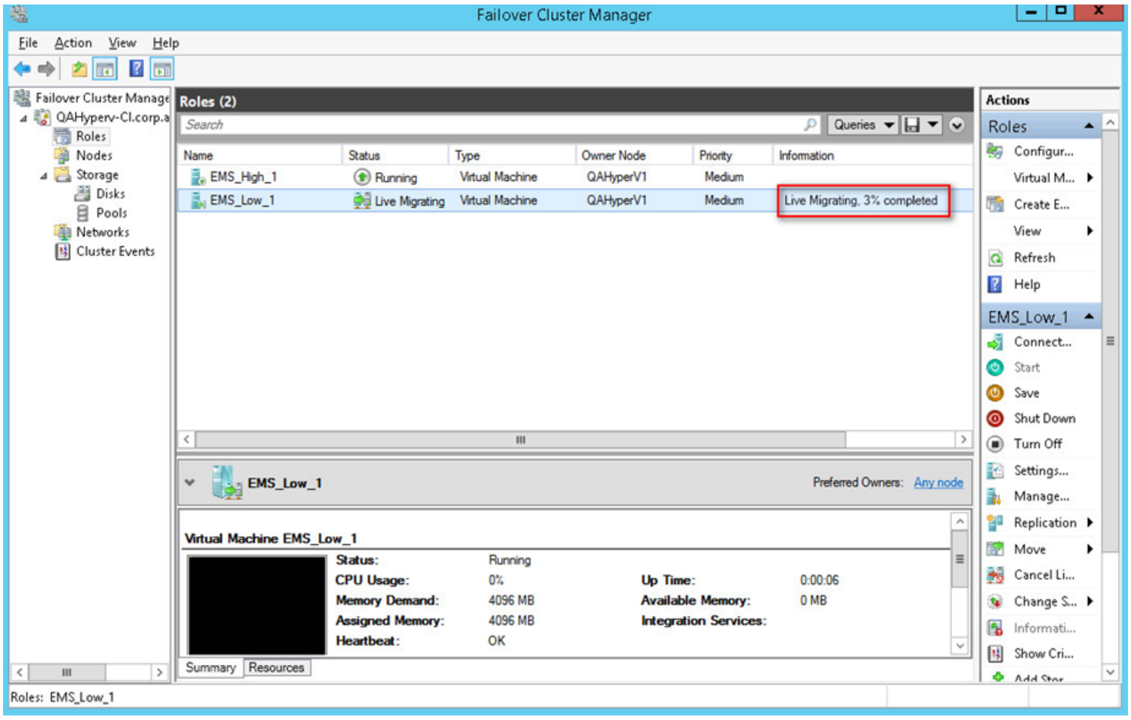
Cluster nodes:

Name	Status
QAHyperV1	Up

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

   The migration process starts.

Figure 29-7: Hyper-V Migration Process Started



Name	Status	Type	Owner Node	Priority	Information
EMS_High_1	Running	Virtual Machine	QAHyperV1	Medium	
EMS_Low_1	Live Migrating	Virtual Machine	QAHyperV1	Medium	Live Migrating, 3% completed

EMS_Low_1 Preferred Owners: Any node

Virtual Machine EMS_Low_1

Status:	Running		
CPU Usage:	0%	**Up Time:**	0:00:06
Memory Demand:	4096 MB	**Available Memory:**	0 MB
Assigned Memory:	4096 MB	**Integration Services:**	
Heartbeat:	OK		

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

30 Supplementary Security Procedures

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

> For more information on the implementation of custom certificates, refer to the OVOC Security Guidelines document.

This appendix describes the following procedures:

- Downloading certificates to the AudioCodes device (Installing Custom Certificates on OVOC Managed Devices below)
- Cleaning up Temporary files on the OVOC server (Cleaning up Temporary Files on OVOC Server on page 294)

Installing Custom Certificates on OVOC Managed Devices

This section describes how to install Custom certificates on OVOC managed devices. These certificates will be used to secure the connection between the device and OVOC server. This procedure is performed using the device's embedded Web server. This section describes how to install certificates for the following devices:

- Enterprise gateways and SBC devices (Gateways and SBC Devices below).
- MP-1xx devices (MP-1xx Devices on page 289).

> - When securing the device connection over HTTPS, the certificate loaded to the device must be signed by the same CA as the certificate loaded to the OVOC server.
> - The Single-Sign On mechanism is used to enable automatic login to the devices embedded Web server tool from the device's status screen in the OVOC. This connection is secured over port 443. OVOC logs into the OVOC managed device using the credentials that you configure in the AudioCodes device details or Tenant Details in the OVOC Web. You can also login to the AudioCodes device using the RADIUS or LDAP credentials (for more information, refer to the OVOC User’s Manual).

Gateways and SBC Devices

This section describes how to install custom certificates on gateways and SBC devices. The device uses TLS Context #0 to communicate with the OVOC server. Therefore, the configuration described below should be performed for **TLS Context #0.**

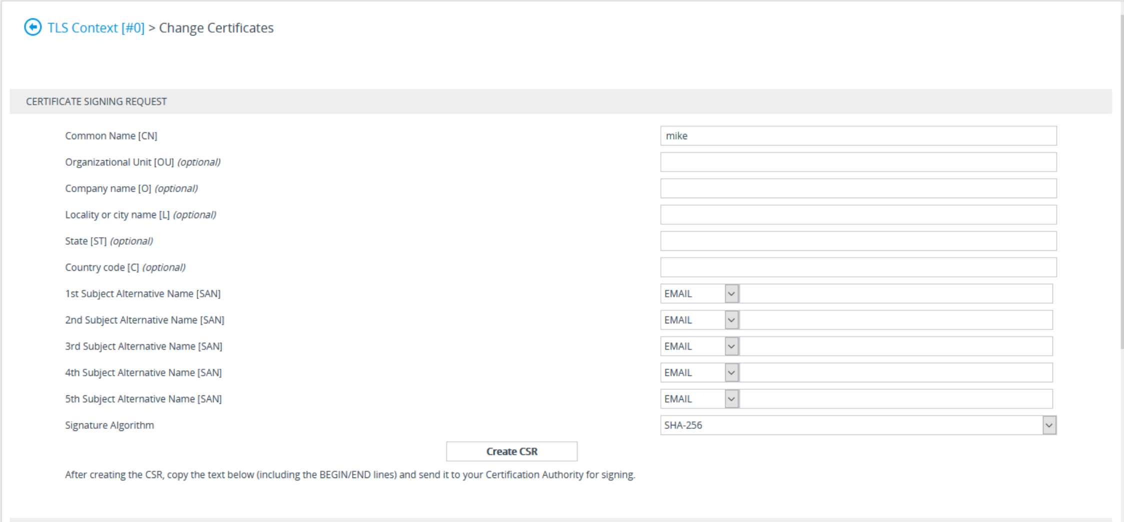
Step 1: Generate a Certificate Signing Request (CSR)

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

➢ To generate certificate signing request:

1. Login to the device's Web server.
2. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
3. In the table, select the **TLS Context Index #0**, and then click the **TLS Context Certificate** button, located below the table; the Context Certificates page appears.

Figure 30-1: Context Certificates



TLS Context [#0] > Change Certificates

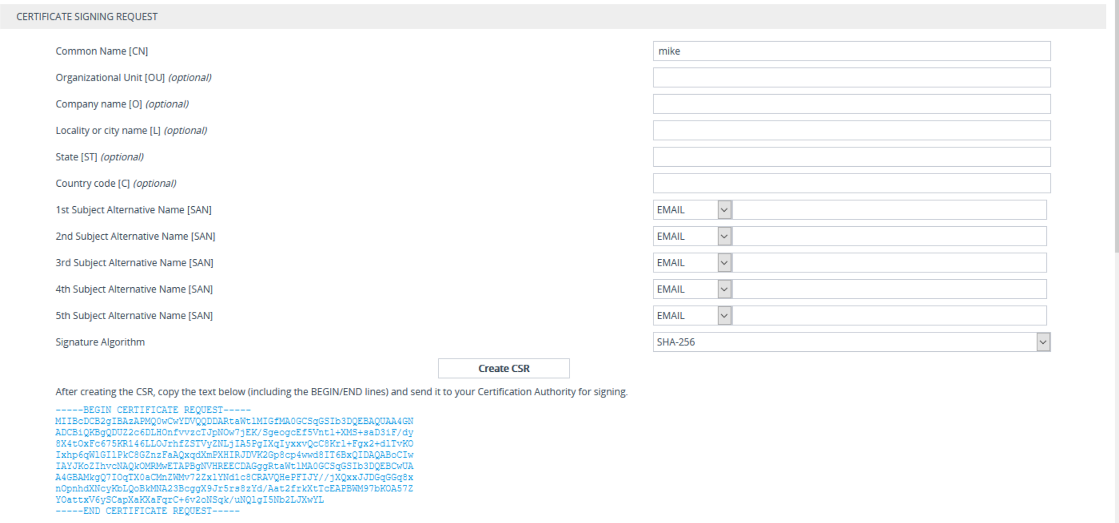
CERTIFICATE SIGNING REQUEST

Common Name [CN]	mike
Organizational Unit [OU] *(optional)*	
Company name [O] *(optional)*	
Locality or city name [L] *(optional)*	
State [ST] *(optional)*	
Country code [C] *(optional)*	
1st Subject Alternative Name [SAN]	EMAIL
2nd Subject Alternative Name [SAN]	EMAIL
3rd Subject Alternative Name [SAN]	EMAIL
4th Subject Alternative Name [SAN]	EMAIL
5th Subject Alternative Name [SAN]	EMAIL
Signature Algorithm	SHA-256

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

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 30-2: Certificate Signing Request Group



CERTIFICATE SIGNING REQUEST

Common Name [CN]	mike
Organizational Unit [OU] *(optional)*	
Company name [O] *(optional)*	
Locality or city name [L] *(optional)*	
State [ST] *(optional)*	
Country code [C] *(optional)*	
1st Subject Alternative Name [SAN]	EMAIL
2nd Subject Alternative Name [SAN]	EMAIL
3rd Subject Alternative Name [SAN]	EMAIL
4th Subject Alternative Name [SAN]	EMAIL
5th Subject Alternative Name [SAN]	EMAIL
Signature Algorithm	SHA-256

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-----
MIIBcDCB2gIBAzAPMQ0wCwYDVQQDDARtaWtlMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQDUZ2c6DLHOnfvvzcTJpNOw7jEK/SgeogcEf5Vntl+XMS+saD3iF/dy
8X4tOxFc675KR146LLOJrhfZSTVyZNLjIA5PgIXqIyxxvQcC8Krl+Fgx2+dlTvKO
Ixhp6qWlGIlPkC8GZnzFaAQxqdXmPXHIRJDVK2Gp8cp4wwd8IT6BxQIDAQABoCIw
IAYJKoZIhvcNAQkOMRMwETAPBgNVHREECDAGggRtaWtlMA0GCSqGSIb3DQEBCwUA
A4GBAMkgQ7IOqTX0aCMnZWMv72ZxlYNd1c8CRAVQHePFIJY//jXQxxJJDGqGGq8x
nOpnhdXNcyKbLQoBkMNA23BcggX9Jr5rs8zYd/Aat2frkXtTcEAPBWM97bKOA57Z
YOattxV6ySCapXaKXaFqrC+6v2oNSqk/uNQlgI5Nb2LJXwYL
-----END CERTIFICATE REQUEST-----
```

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

Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to "device.crt"
- Root certificate – rename this file to "root.crt"
- Intermediate CA certificates (if such files exist) – rename these files to "ca1.crt", "ca2.crt" etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:

```
-----BEGIN CERTIFICATE-----

MIIBuTCCASKgAwIBAgIFAKKIMbgwDQYJKoZIhvcNAQEFBQAwFzEVMB
MGA1UEAxMM

RU1TIFJPT1QgQ0EyMB4XDTE1MDUwMzA4NTE0MFoXDTI1MDUwMzA4
NTE0MFowKjET
...

Tl6vqn5I27Oq/24KbY9q6EK2Yc3K2EAadL2IF1jnb+yvREuewprOz6TEEuxN
JoI0
L6V8IzUYOfHrEiq/6g==
-----END CERTIFICATE-----
```

- The above files are required in the following steps. Make sure that you obtain these files before proceeding and save them to the desired location.
- Use the exact filenames as mentioned above.

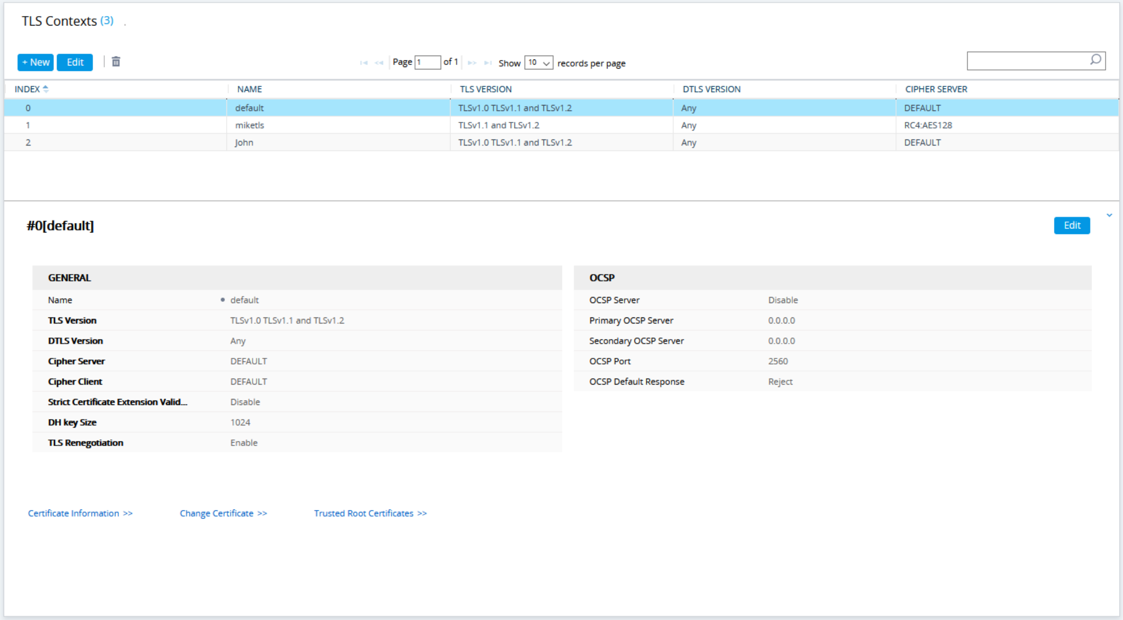
Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

➢ **To update device with new certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the table, select **TLS Context #0**, and then click the **Change Certificate** button, located below the table; the Context Certificates page appears.

Figure 30-3: TLS Contexts Table



TLS Contexts (3)

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT
1	miketls	TLSv1.1 and TLSv1.2	Any	RC4:AES128
2	John	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT

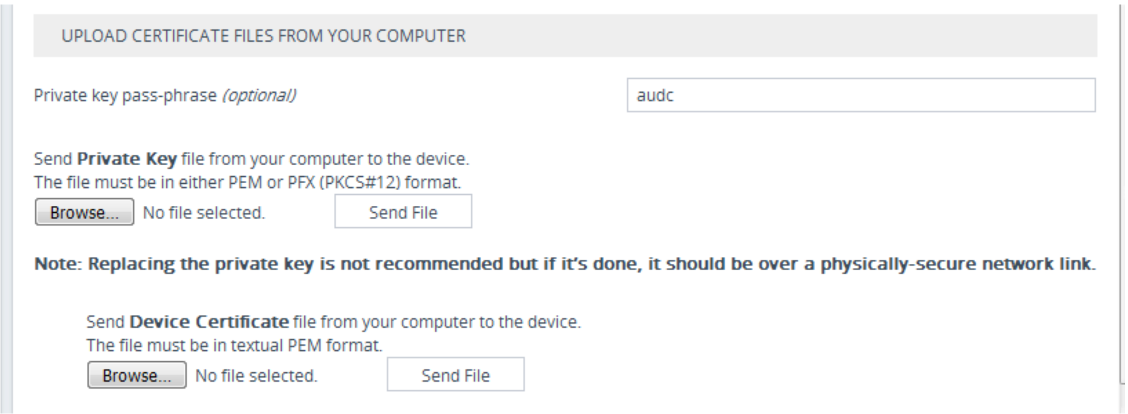
#0[default]

GENERAL	
Name	default
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2
DTLS Version	Any
Cipher Server	DEFAULT
Cipher Client	DEFAULT
Strict Certificate Extension Valid...	Disable
DH key Size	1024
TLS Renegotiation	Enable

OCSP	
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

3. Under the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field and then navigate to the device.crt file, and click **Send File**.

Figure 30-4: Upload Certificate Files from your Computer Group



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*: audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

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.

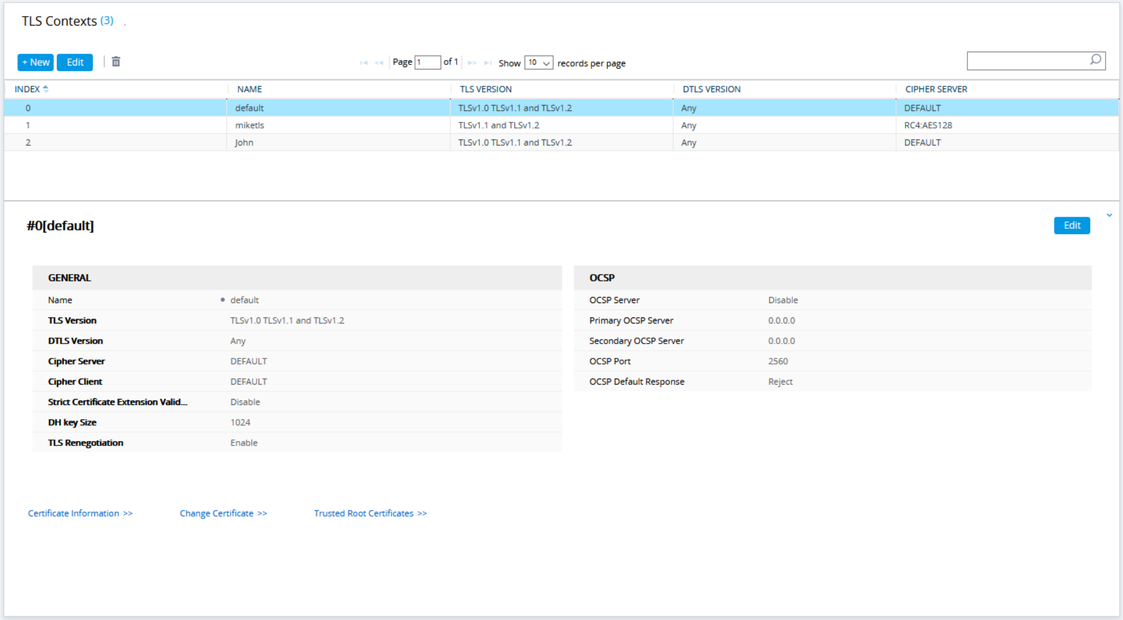
Step 4: Update Device's Trusted Certificate Store

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 **Trusted Root Certificates** button, located below the table; the Trusted Certificates page appears.

Figure 30-5: Trusted Root Certificates



TLS Contexts (3)

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT
1	miketls	TLSv1.1 and TLSv1.2	Any	RC4:AES128
2	John	TLSv1.0 TLSv1.1 and TLSv1.2	Any	DEFAULT

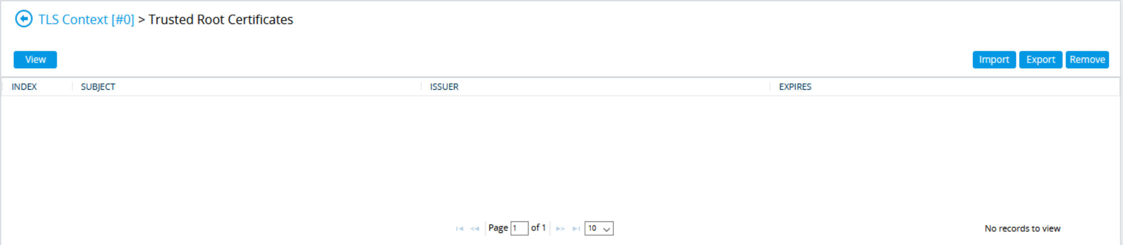
#0[default]

GENERAL	
Name	default
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2
DTLS Version	Any
Cipher Server	DEFAULT
Cipher Client	DEFAULT
Strict Certificate Extension Valid...	Disable
DH key Size	1024
TLS Renegotiation	Enable

OCSP	
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

3. Click the **Import** button, and then browse to the root.crt file. Click **OK** to import the root certificate.

Figure 30-6: Importing Certificate into Trusted Certificates Store



TLS Context [#0] > Trusted Root Certificates

INDEX	SUBJECT	ISSUER	EXPIRES

No records to view

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

Step 5: Configure HTTPS Parameters on the Device

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

- You can optionally pre-stage the device with a pre-loaded ini file including this configuration (for more information, contact your AudioCodes representative).
- If you have enabled the Interoperability Automatic Provisioning feature, ensure that your template file is also configured as described in this procedure to maintain an active HTTPS connection after the template file has been loaded to the device.
- When you setup an HTTPS connection on the device, you must also enable HTTPS ("Enable HTTPS Connection") when adding the device to the OVOC (refer to the *OVOC User's manual*).

➢ To configure HTTPS parameters on the device:

1. Create a new text file using a text-based editor (e.g., Notepad).

2. Include the following ini file parameters for server-side authentication:

   - For Media Gateway and SBC devices:

     AUPDVerifyCertificates=1

   - For MP-1xx devices, the ini file should include the following two lines::

     AUPDVerifyCertificates=1
     ServerRespondTimeout=10000

   - When working with SEM TLS (OVOC Voice Quality Package - SBC Communication on page 239), add the following parameter.

     QOEENABLETLS=1

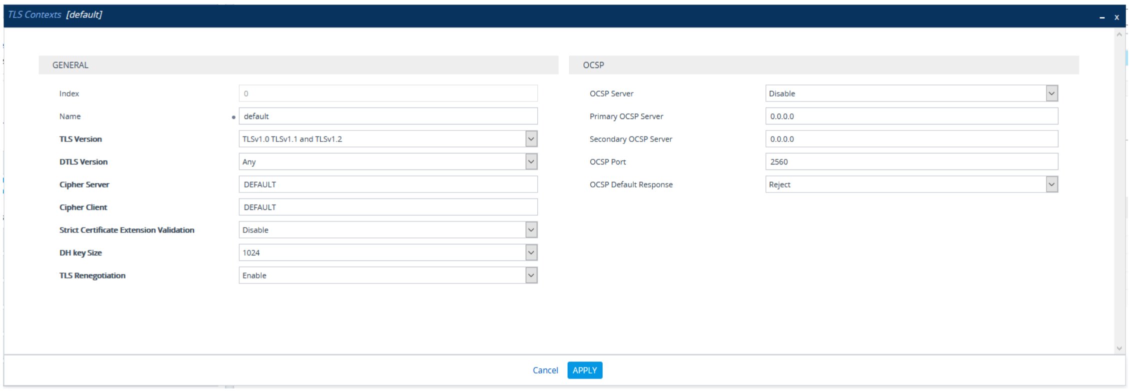
3. Save and close the file.

4. Load the generated file as “Incremental INI file” (Maintenance menu > Software Update > Load Auxiliary Files > INI file (incremental).

5. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).

6. In the table, select the TLS Context #0, and then click **Edit** . The following screen is displayed:

Figure 30-7: TLS Contexts: Edit Record



GENERAL

Index: 0
Name: default
TLS Version: TLSv1.0 TLSv1.1 and TLSv1.2
DTLS Version: Any
Cipher Server: DEFAULT
Cipher Client: DEFAULT
Strict Certificate Extension Validation: Disable
DH key Size: 1024
TLS Renegotiation: Enable

OCSP

OCSP Server: Disable
Primary OCSP Server: 0.0.0.0
Secondary OCSP Server: 0.0.0.0
OCSP Port: 2560
OCSP Default Response: Reject

7. Set the required 'TLS Version' (default TLS Version 1.0).

8. Set 'HTTPS Cipher Server' to ALL.

9. Set 'HTTPS Cipher Client' to ALL.

Step 6: Reset Device to Apply the New Configuration

This step describes how to reset the device to apply the new configuration.

➢ To save the changes and reset the device:

1. Reset the device with a save-to-flash for your settings to take effect (Setup menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

MP-1xx Devices

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

> ⚠ For installing certificates on MP2xx devices, refer to Section "Securing Remote Management with Certificates" in the *MP-20x Telephone Adapter User's Manual*.

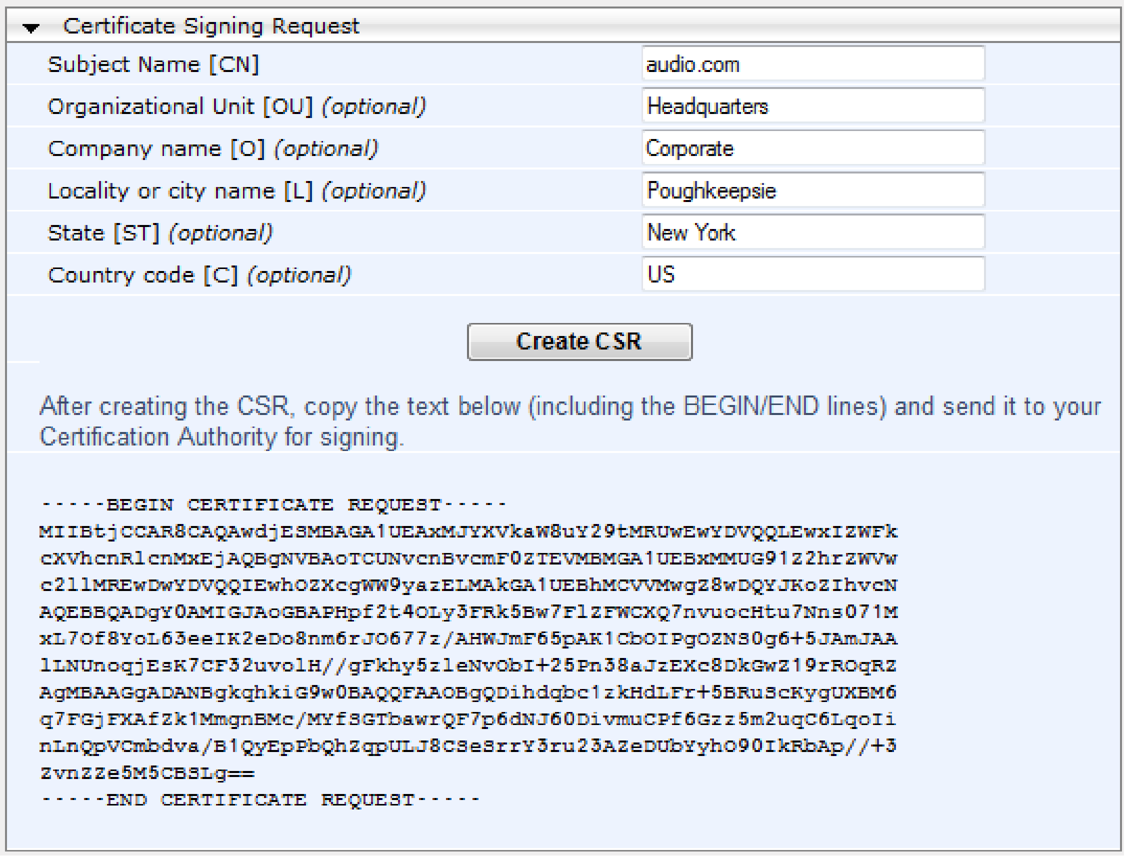
Step 1: Generate a Certificate Signing Request (CSR)

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 30-8: 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

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
cXVhcnRlcnMxEjAQBgNVBAoTCUNvcnBvcmF0ZTEVMBMGA1UEBxMMUG91z2hrZWVw
c2llMREwDwYDVQQIEwhOZXcgWW9yazELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPHpf2t4OLy3FRk5Bw7FlZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1CbOIPgOZN30g6+5JAmJAA
lLNUnoqjEsK7CF32uvolH//gFkhy5zleNvObI+25Pn38aJzEXc8DkGwZ19rROqRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbc1zkHdLFr+5BRu3cKygUXBM6
q7FGjFXAfZk1MmgnBMc/MYf3GTbawrQF7p6dNJ60DivmuCPf6Gzz5m2uqC6LgoIi
nLnQpVCmbdva/B1QyEpPbQhZqpULJ8C3e3rrY3ru23AZeDUbYyhO90IkRbAp//+3
ZvnZZe5M5CB3Lg==
-----END CERTIFICATE REQUEST-----
```

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

Step 2: Receive the New Certificates from the CA

You will receive the following files from the Certificate Authority (CA):

- Your (device) certificate – rename this file to “device.crt”
- Root certificate – rename this file to “root.crt”
- Intermediate CA certificates (if such files exist) – rename these files to “ca1.crt”, “ca2.crt” etc.

Save the signed certificate to a file (e.g., device.crt). Make sure that all certificates are in PEM format and appear as follows:
-----BEGIN CERTIFICATE-----

```
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDV
QQGEwJGUjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2Vy
dGlwb3N0ZSBTZXJ2ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyND
A4MDAwMFowPzELMAkGA1UEBhMCRlIxEzARBgNVBAoTCkNlcnRpcG9zdG
UxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCCASEwDQYJKoZIhvcN
AQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkonWnNm`+
Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7JPM5n6
```

```
cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3IRefiXDmuOe+FhJ
gHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+
w==
```

-----END CERTIFICATE-----

- The above files are required in the following steps. Make sure that you obtain these files before proceeding.
- Use the exact filenames as mentioned above.

Step 3: Update Device with New Certificate

This step describes how to update the device with the new certificate.

➢ To update the device with the new certificate:

1. In the Certificates page, scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the device.crt file, and then click **Send File**.
2. After the certificate successfully loads to the device, save the configuration with a device reset (Step 6: Reset Device to Apply the New Configuration on page 294 below).

Step 4: Update Device's Trusted Certificate Store

For the device to trust a whole chain of certificates you need to combine the contents of the root.crt and ca.crt certificates into a single text file (using a text editor).

➢ To update the device with the new certificate:

1. Open the root.crt file (using a text-based editor, e.g., Notepad).
2. Open the ca.crt file (using a text-based editor, e.g., Notepad).
3. Copy the content of the ca.crt file and paste it into the root.crt file above the existing content.

Below is an example of two certificate files combined (the file "ca2.crt" and the "root.crt") where the ca2.crt file contents are pasted above the root.crt file contents:

```
-----BEGIN CERTIFICATE-----

MIIDNjCCAh6gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQK
EwNBQ0wx

ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIw
MDEwMTAwMDAw
```

```
MFowIDEMMAoGA1UEChMDQUNMMRAwDgYDVQQDFAdFTVNfQ0EyMIIBIj
ANBgkqhkiG

9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4CmsdZNpWo6Gg5UgxflPjJeNggwnlQ
iUYhOK
kPEvS6yWH7tr8+TwnIzjT58kuuy+fFVLDyZzp117J53FIsgnCSxpVqcYfMoBbCL/

0fmXKHWlPIIbovWpZddgz8U1pEzD+5eGMUwCnqw99rbUseAHdwkxsXtOquwq
E4yk

ihiWesMp54LwX5dUB46GWKUfT/pdQYqAuunM76ttLpUBc6yFYeqpLqj9OgKkR
4cu

5B6wYNPoTjJX5OXgd9Yf+0IQYB2EiP06uzLtlyWL3AENGwDVeOvlfZgppLEZP
BKI

hfULeMjay4fzE4XnS9LDxZGjJ+nV9ojA7WaRB5tl6nEJQ/7sLQIDAQABo3oweDA
M

BgNVHRMEBTADAQH/MB0GA1UdDgQWBBRy2JQ1yZrvN4GifsXUB7AvctWvr
TBJBgNV

HSMEQjBAgBThf6GbMQbO5b0CkLV8kW+Rg0AAhqEIpCMwITEMMAoGA1UE
ChMDQUNM

MREwDwYDVQQDFAhFTVNfUk9PVIIBATANBgkqhkiG9w0BAQUFAAOCAQE
AdAsYyfcg

TdkF/uDxlOGk0ygXrRAXHG2WFOS6afrcJHoZCCH3PNsvftRrEAwroGwx7tsn1/
o+
CNV5YalstIz7BDIEIjTzCDrpO9sUsiHqxGuOnNhjLDUoLre1GDC0OyiKb4BOhlCq

hiemkXRe+eN7xcg0IfUo78VLTPuFMUhz0Bdn7TuE7QbiSayq2fY2ktHHOyDEKJ
GO

RUosIqgVwSZIsCnRZFumkKJtrT4PtnNYluYJHej/SHcsOWtgtCQ8cPdNJCZAW
Z+V

XoAhN6pH17PMXLPclm9L/MIkVkmf0tp1bPmefrEBIO+np/O8F+P551uH0iOYA6
Cc
Cj6oHGLq8RIndA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

```
MIIDNzCCAh+gAwIBAgIBATANBgkqhkiG9w0BAQUFADAhMQwwCgYDVQQK
EwNBQ0wx

ETAPBgNVBAMUCEVNU19ST09UMB4XDTEwMDEwMTAwMDAwMFoXDTIw
MDEwMTAwMDAw

MFowITEMMAoGA1UEChMDQUNMMREwDwYDVQQDFAhFTVNfUk9PVDCC
ASIwDQYJKoZI

hvcNAQEBBQADggEPADCCAQoCggEBANCsaGivTMMcSv57+j5Hya3t6A6FS
FhnUQrS

667hVpbQ1Eaj02jaMh8hNv9x8SFDT52hvgVXNmLBmpZwy+To1VR4kqbAEoIs+
7/q

ebESJyW8pTLTszGQns2E214+U18sKHItpUZvs1dVUIX6xQiSYFDG1CDIPR5/7
0pq
zwtdbIipSsKgYijos0yRV3roVqNi4e+hmLVZA9rOIp6LR72Ta9HMJFJ4gyxJPUQA

jV3Led2Y4JObvBTNIka18WI7KORJigMMp7T8ewRkBQlJM7nmeGDPUf1wRjDW
gI4G

BRw2MACYsu/M9z/H821UOICtsZ4oKUJMqbwjQ9lXI/HQkKRSTf8CAwEAAaN6
MHgw

DAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU4X+hmzEGzuW9ApC1fJFvkYN
AAIYwSQYD

VR0jBEIwQIAU4X+hmzEGzuW9ApC1fJFvkYNAAIahJaQjMCExDDAKBgNVBA
oTA0FD

TDERMA8GA1UEAxQIRU1TX1JPT1SCAQEwDQYJKoZIhvcNAQEFBQADggE
BAHqkg4F6

wYiHMAjjH3bqxUPHt2rrrALaXA9eYWFCz1q4QVpQNYAwdBdEAKENznZttoP3
aPZE

3EOx1C8Mw2wU4pOxD7B6pH0XO+oJ4LrxLB3SAJd5hW495X1RDF99BBA9e
GUZ2nXJ
9pin4PWbnfc8eppq8Tpl8jJMW0ZI3prfPt012q93iEalkDEZX+wxkHGZEqS4ayBn

8bU3NHt5qh0Egpai8hB/nth1xnA1m841wxCbJW86AMRs2NznROyG695InAYaN
llo
```

```
HU9zBRdRRASV5vmBN/q5JnDhshZhL1Bm+M6QxOyGoNjL1DqE+aWZkmsw2
k9STOpN
itSUgGYwEagnsMU=
-----END CERTIFICATE-----
```

⚠ The maximum supported size of the combined file of trusted chain of certificates is 100,000 bytes (including the certificate's headers).

4. Save the combined content to a file named "chain.pem" and close the file.
5. Open the Certificates page and upload chain.pem file using the 'Trusted Root Certificate Store' field.

Step 5: Configure HTTPS Parameters on Device

- Configure HTTPS Parameters on the device (Step 5: Configure HTTPS Parameters on the Device on page 287 above).

Step 6: Reset Device to Apply the New Configuration

This section describes how to apply the new configuration.

➢ **To save the changes and reset the device:**

1. Reset the device with a save-to-flash for your settings to take effect (Setup menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

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
```

31 Transferring Files

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

⚠ FTP by default is disabled on the OVOC server.

➢ To transfer files to and from the OVOC server:

1. Open your SFTP/SCP application, such as WinSCP or FileZilla.
2. Login with the acems/acems credential (all files transferred to the OVOC server host machine are then by default saved to /home/acems directory).
3. Copy the relevant file(s) from your PC to the host machine (or vice-versa). For example, using the FileZilla program, you drag the relevant file from the left pane i.e. in your PC directory to the right pane i.e. the /home/acems directory on the OVOC server host machine.

32 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
```

33 Self-Signed Certificates

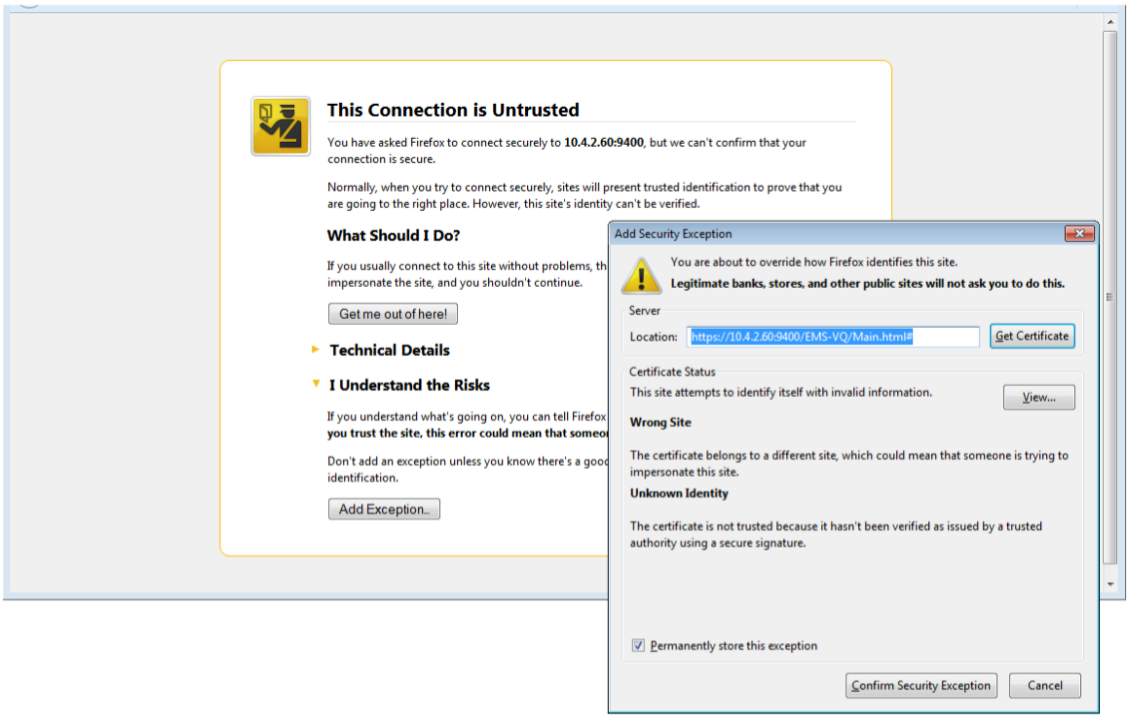
When using self-signed certificates, use the following instructions for recognizing the secure connection with the OVOC server from your OVOC client browsers.

Mozilla Firefox

When you are prompted with a message that the web page that you are trying to open using Mozilla Firefox is insecure, do the following:

1. Click the “I Understand the Risks” option.
2. Click the **Add Exception** button, and then click the **Confirm Security Exception** button.

Figure 33-1: Mozilla Firefox Settings



This Connection is Untrusted

You have asked Firefox to connect securely to **10.4.2.60:9400**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, th impersonate the site, and you shouldn't continue.

Technical Details

I Understand the Risks

If you understand what's going on, you can tell Firefox **you trust the site, this error could mean that someo**

Don't add an exception unless you know there's a good identification.

Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.4.2.60:9400/EMS-VQ/Main.html#

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

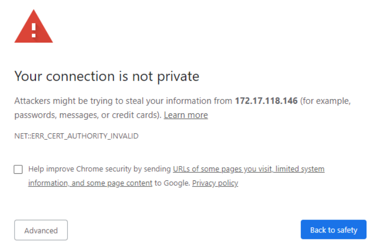
☑ Permanently store this exception

Google Chrome

When you are prompted with a message that the web page that you are trying to open using Google Chrome is insecure, do the following:

1. Click **Advanced** and then click the “Proceed to <Server IP> (unsafe)” link.

Figure 33-2: Chrome Browser Settings



Your connection is not private

Attackers might be trying to steal your information from **172.17.118.146** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

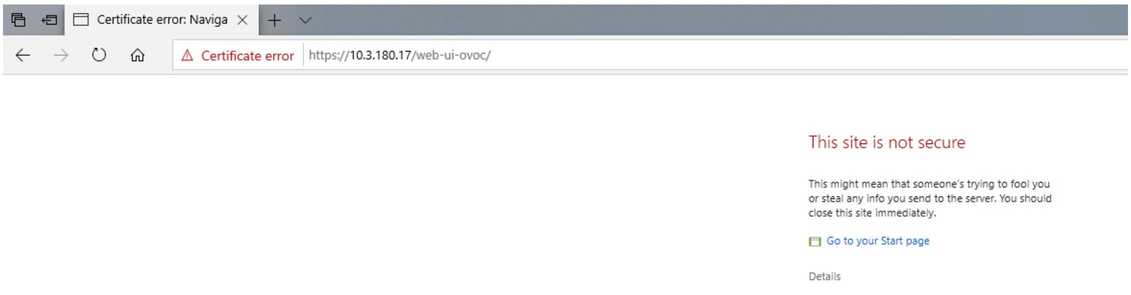
□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Microsoft Edge

When you are prompted with a message that the web page that you are trying to open using Microsoft Edge is insecure, do the following:

- Click **Details** and then click the link **Go on to the webpage**.

Figure 33-3: Microsoft Edge Browser

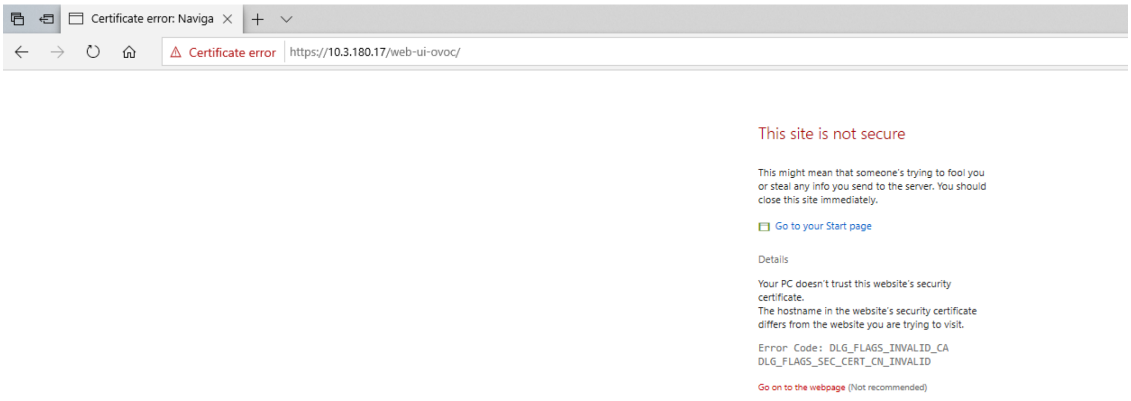


https://10.3.180.17/web-ui-ovoc/

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Figure 33-4: Go on to the Web Page



https://10.3.180.17/web-ui-ovoc/

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

```
Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID
```

Go on to the webpage (Not recommended)

34 Datacenter Disaster Recovery

Introduction

This appendix describes the OVOC Disaster Recovery procedure for deployments where OVOC is deployed in two separately geographically located datacenters with two different network spaces, in which minimal impact on the SBC/Gateway and OVOC downtime is desired.

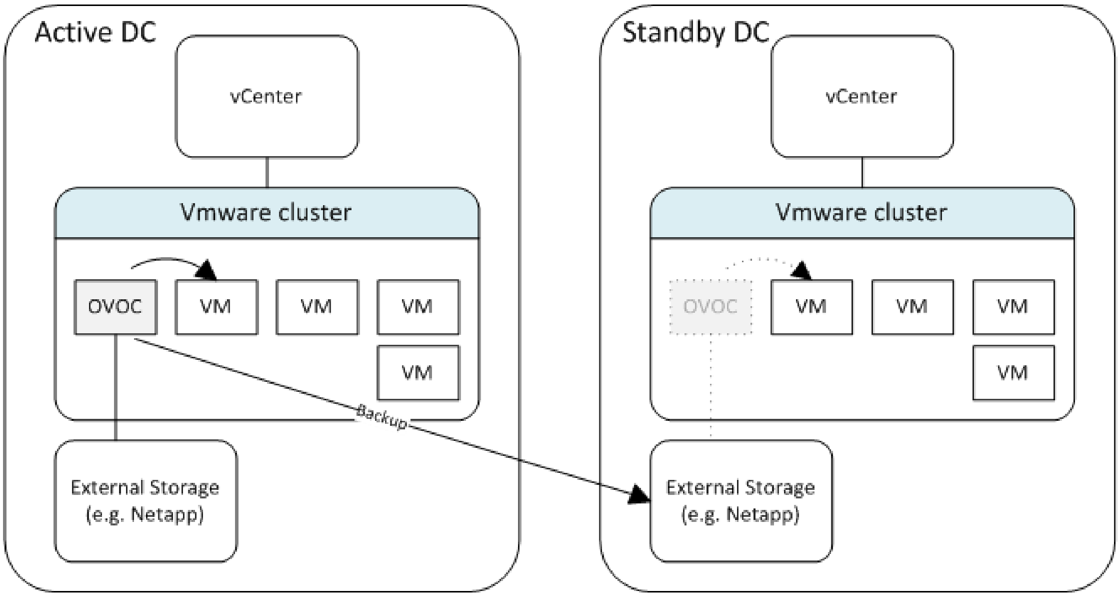
> ⚠ Examples shown in this Appendix are for the VMware platform; however, these procedures are also relevant for Hyper-V platform.

Solution Description

The Disaster Recovery solution is composed of two virtual machines in accordance with the OVOC system requirements (see Hardware and Software 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 is 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 34-1: Disaster Recovery Between Two DataCenters with VMware HA



Initial Requirements

The following initial requirements need to be adhered to before implementing the Disaster Recovery procedure:

- Both machines should have identical hardware (CPU, Memory, Disk, IO).
- An identical Linux OS (the same DVD), database, and the OVOC software version should be used.
- Identical database passwords need to be configured on both servers.
- Identical OVOC Server Manager settings must be configured on both servers (e.g., HTTP/HTTPS communication, etc.).
- If non-default certificates are used, they must be pre-installed on both servers.
- Both machines should have a valid license per each Machine ID with identical capabilities.
- When upgrading the OVOC server software, both machines should be upgraded. Make sure that redundant machine is not rebooted after the upgrade process and the OVOC application remains closed.

> When upgrading OVOC, the backup that was created before the upgrade cannot be used anymore. You should only use the backups created after the upgrade process. For more information on backing up the OVOC server, see OVOC server Backup.

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

New Customer Configuration

The procure below describes the steps for a New Customer configuration.

➢ To perform a New Customer configuration:

1. Install and properly configure both servers.
2. Make sure the primary OVOC server is up and running.
3. For each device added and managed by the OVOC server, the following features should be provisioned with both primary and secondary servers’ IP addresses:
   - Trap Destination Server
   - Session Experience Manager
   - NTP Server Address

Data Synchronization Process

To save recovery time, it is advised that at the end of the daily / weekly backup, transfer the latest backup files from the primary to the secondary server machine. The data transfer may be performed automatically using a customer- defined script.

⚠ The data transfer is the responsibility of the Enterprise's IT implementation team.

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 OVOC Server Manager, go to the Application Maintenance menu and select the **Restore** option (OVOC Server Restore on page 158).
7. Follow the instructions during the process; you might need to press **Enter** a few times.
8. After the restore operation has completed, you are prompted to reboot the OVOC server.
9. If you have installed custom certificates prior to the restore, you must re-install them.
10. Login to the OVOC Web client and verify that there is connectivity and the application is functioning correctly.
11. If you are using one or more features which are marked in the table below as ‘Not Supported’, please provision all the managed devices with a new Management Server IP address.
12. For SBC Fixed and Floating License Pool customers, run the *Update* command for all the managed devices .

See the table below summarizing the features affected byDisaster Recovery functionality.

Table 34-1: Features Affected by Disaster Recovery Functionality

Feature	Status
Management	
Alarms+ NAT communication based on Keepalive traps	Supported
Fixed License Pool and Floating License	Not Supported

Feature	Status
IP Phones Manager Pro: Alarms / Status reports	Not Supported
Advanced Quality Package	-
SBC/Gateway Voice Quality Monitoring	Supported
Endpoint Quality monitoring (RFC 6035)	Not Supported
Server	
Server: Device NTP Server	Supported
Server: Device Syslog Server	Not Supported
Server: Device TP Debug recording server	Not Supported

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-94180