A MITEL
PRODUCT
GUIDE

OpenScape Voice V11

Service Manual: Installation and Upgrades

Installation Guide
06/2026

A31003-H80B0-J100-11-7631

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2026, Mitel Networks Corporation

All rights reserved

Contents

1 Important Notices . . . 19
1.1 About this Book . . . 19
1.1.1 Audience . . . 19
1.1.2 Prerequisite Knowledge . . . 19
1.1.3 Viewing the Document with Adobe Reader . . . 20
1.1.4 Special Notices . . . 20
1.2 Safety . . . 21
1.2.1 General Safety . . . 21
1.2.2 Safety with Electricity . . . 21
1.2.2.1 High Voltages . . . 21
1.2.2.2 Equipment Room . . . 22
1.2.2.3 Emergencies . . . 23
1.2.3 Reporting Accidents . . . 23
2 Preparing for the Installation . . . 25
2.1 About OpenScape Voice . . . 25
2.1.1 Administration and Media Server Options . . . 26
2.1.2 OpenScape Branch . . . 27
2.2 Installing OpenScape Voice . . . 28
2.2.1 Installation Media . . . 28
2.2.2 Prerequisites and Assumptions . . . 29
2.2.3 Backup License Recommendations . . . 30
2.2.4 OpenScape Voice Installation Checklist . . . 30
2.3 Guidelines for Geographically Separated Nodes . . . 37
2.3.1 Guidelines for Configuration Parameters of Geographically Separated Nodes . . . 37
2.3.1.1 Node Separation = <none, separate> . . . 37
2.3.1.2 StandAloneServiceEnabled = <yes, no> . . . 37
2.3.1.3 Survival Authority = <IP address> . . . 38
2.3.1.4 PreferredNodeToTakeOver = <node1, node2> . . . 38
2.3.1.5 Timezone is the always the same for both nodes . . . 39
2.3.1.6 Cluster Timeout = 15 seconds . . . 39
2.3.1.7 MTU X-Channel . . . 39
2.3.2 Guidelines for Static Routes of Geographically Separated Nodes . . . 39
2.4 Source Based Routes . . . 41
2.5 Flexible Ethernet circuit and IP Address Configuration . . . 44
2.5.1 Overview . . . 44
2.5.2 Merging of IP subnets to common Ethernet ports . . . 45
2.5.3 Sharing of IP addresses . . . 46
2.5.4 Default IPs for the 4 OSV Configuration Variants . . . 48
2.5.5 Default IPs for the 4 OSV configuration variants - Case Merged Admin, Billing and Signaling Subnet 49
2.5.6 Example of a 1 IP subnet configuration with a minimized set of IP addresses . . . 50
2.6 Creating a Node.cfg File . . . 50
2.6.1 Download the "OpenScape Voice Installation Wizard" . . . 53
2.6.2 Section 1: Configuration and Hardware (1/1) screen . . . 54
2.6.2.1 Hardware Platform . . . 54
2.6.2.2 Configuration . . . 55
2.6.2.3 Node Separation . . . 55
2.6.2.4 Software Build ID . . . 56

2.6.2.5 Survival Authority . . . 57
2.6.2.6 Preferred Node to Takeover . . . 57
2.6.2.7 Timezone . . . 57
2.6.2.8 Keyboard . . . 57
2.6.2.9 Stand Alone Service Enabled . . . 57
2.6.2.10 X-Channel Compression . . . 58
2.6.2.11 Cluster Timeout . . . 58
2.6.2.12 Cluster Name, Node 1 Name and Node 2 Name . . . 58
2.6.2.13 Assistant, Cluster Name . . . 59
2.6.3 Section 2: IP Configuration (1/4) screen . . . 59
2.6.3.1 Share Cluster with Mgmt button . . . 59
2.6.3.2 Subnet Sharing . . . 60
2.6.3.3 Default Router Node 1 . . . 60
2.6.3.4 Management, Signaling, Billing Networks, and CI Group . . . 60
2.6.4 Section 2: IP Configuration (2/4) screen . . . 61
2.6.4.1 Assistant Cluster Name . . . 61
2.6.4.2 Assistant/CMP . . . 61
2.6.4.3 DNS Configuration . . . 62
2.6.4.4 NTP Configuration . . . 62
2.6.5 Section 2: IP Configuration (3/4) screen . . . 62
2.6.5.1 Source/Static Routes . . . 62
2.6.5.2 Broadcast Routes . . . 63
2.6.6 Section 3: IP Configuration (4/4) screen . . . 63
2.6.6.1 Source/Static Routes IPv6 . . . 63
2.6.7 Section 3: IP Security (1/2) screen . . . 63
2.6.7.1 SNMP Servers . . . 63
2.6.7.2 License Servers . . . 64
2.6.7.3 LicenseAgentPort . . . 64
2.6.8 Section 3: IP Security (2/2) screen . . . 64
2.6.9 Finishing the Node.cfg . . . 64
2.7 Including Patch Sets and License files on the USB Memory Stick(s) . . . 66
2.7.1 Loading Patch Sets onto the USB Memory Sticks . . . 66
2.7.2 Including the License file on the Installation USB . . . 67
2.8 Fix Subscriber with Global Numbering Plan (E164NANP) . . . 68
2.8.1 Step 1: Check procedure . . . 68
2.8.1.1 Output 1 . . . 69
2.8.1.2 Output 2 . . . 69
2.8.1.3 Output 3 . . . 70
2.8.2 Step 2: Repair procedure . . . 71

3 Installing the Hardware Platform . . . 73
3.1 Computing Node . . . 74
3.1.1 Lenovo SR530 Server . . . 74
3.1.2 Lenovo SR630 V2 Server . . . 75
3.1.3 OpenScape Voice Hardware - Lenovo SR630 V3 Server . . . 76
3.2 Ethernet Switch . . . 77
3.3 Installing the Lenovo SR630 V2 Server into the Rack . . . 77
3.3.1 KVM Notes . . . 77
3.3.2 Installing the Disk Drive . . . 78
3.3.3 Removing the Top Cover . . . 79
3.3.4 Installing Memory and CPU for the Lenovo SR630 V2 . . . 80
3.3.5 Connection Panel in the rear of the Lenovo SR630 V2 server . . . 82

3.3.6 Installing the PCI . . . 82
3.3.7 Installing the Power Module . . . 83
3.3.8 Wiring the Cluster . . . 83
3.3.9 Setting up the UEFI for the Lenovo SR630 V2 server . . . 84
3.3.10 Creating the LSI RAID for the Lenovo SR630 V2 . . . 89
3.3.11 Activation of IPMI Over LAN for the Lenovo SR630 V2 server . . . 91
3.3.12 Remote Console Startup for the Lenovo SR630 V2 server . . . 92
3.3.13 Memory Verification via the IMM Interface for the Lenovo SR630 V2 server . . . 93
3.3.14 Firmware Updates for Lenovo SR630 V2 . . . 94
3.3.15 Entering USB menu . . . 95
3.4 Installing the Lenovo SR630 V3 Server into the Rack . . . 95
3.4.1 KVM Notes . . . 95
3.4.2 Installing the Disk Drive . . . 96
3.4.3 Removing the Top Cover . . . 97
3.4.4 Installing Memory and CPU for the Lenovo SR630 V3 . . . 98
3.4.5 Connection Panel in the rear of the Lenovo SR630 V3 server . . . 99
3.4.6 Installing the PCI . . . 100
3.4.7 Installing the Power Module . . . 100
3.4.8 Wiring the Cluster . . . 100
3.4.9 Setting up the UEFI for the Lenovo SR630 V3 server . . . 102
3.4.10 Creating the LSI RAID for the Lenovo SR630 V3 . . . 106
3.4.11 Activation of IPMI Over LAN for the Lenovo SR630 V3 server . . . 108
3.4.12 Remote Console Startup for the Lenovo SR630 V3 server . . . 110
3.4.13 Memory Verification via the IMM Interface for the Lenovo SR630 V3 server . . . 110
3.4.14 Firmware Updates for Lenovo SR630 V3 . . . 112
3.4.15 Entering USB menu . . . 112
3.5 Remote Video Redirection and Java 7, Update 51 . . . 113

4 Installing the OpenScape Voice Reference Image . . . 115
4.1 Prerequisites . . . 115
4.2 Installation via USB . . . 115
4.2.1 Overview . . . 115
4.2.2 Prerequisites . . . 116
4.2.3 Installation Procedure . . . 118
4.2.3.1 Physical systems via USB . . . 118
4.2.3.2 Image installation/System Restore USB/Service System Image Write . . . 132
4.2.3.3 Virtual systems via Virtual CD/DVD . . . 147
4.2.4 Backup and Restore via USB . . . 166
4.3 Virtualization Environment Setup . . . 170
4.3.1 Virtualization — Overview . . . 171
4.3.2 Checklist for Virtualization . . . 172
4.3.3 Virtual Machine Guidelines . . . 174
4.3.3.1 Requirements to Underlying Host Hardware . . . 174
4.3.3.2 Virtual Machine Configuration Parameters Overview . . . 175
4.3.3.3 Overview of the OSV Virtual Machine Solutions . . . 177
4.3.3.4 Virtual Machine Network Requirements . . . 177
4.3.3.5 Virtual Machine Memory Requirements . . . 180
4.3.3.6 Virtual Machine CPU Requirements . . . 180
4.3.3.7 Virtual Machine Disk Requirements . . . 180
4.3.3.8 Other Parameters to Consider for the Virtual Machine . . . 181
4.3.4 Creating a Virtual Machine Node.cfg File . . . 181
4.3.4.1 Preparation of the node.cfg files using a Linux or Windows Environment . . . 181

4.3.4.2 Saving the node.cfg, license and patch sets to an Installation ISO Image . . . 183
4.3.4.3 Creating a Virtual Floppy Disk . . . 185
4.3.4.4 Saving the node.cfg File to Virtual Floppy Files . . . 186
4.3.5 VMware - vSphere Client . . . 186
4.3.5.1 Configuration of Login Credentials in VMware vSphere Client . . . 188
4.3.5.2 Uploading a File to the Datastore . . . 189
4.3.6 Preparation of the VMware Virtual Switches . . . 191
4.3.6.1 Preparation of the VMware Virtual Switches: Two Physical Servers Setup (Co-Located or Geo-Separated) . . . 191
4.3.6.2 Preparation of the VMware Virtual Switches: Co-Located with one Physical Server . . . 199
4.3.6.3 Preparation of the VMware Guest Machines - One Physical Server Solution . . . 207
4.3.6.4 Preparation of the VMware Guest Machines - Two Physical Server Solution . . . 221
4.3.6.5 Adding a CD/DVD Drive to the Virtual Machine . . . 223
4.3.6.6 Loading the Image on the VMware Guest Machine . . . 229
4.3.6.7 Virtual Machine Post Installation Best Practices . . . 229
4.3.7 Create a Virtual Machine in Proxmox . . . 230
4.3.7.1 Network choices . . . 239
4.3.7.2 Adding a CD/DVD Drive to the Virtual Machine . . . 241
4.3.7.3 Installing the OpenScape Voice . . . 242
4.3.8 Create a Virtual Machine in Hyper-V . . . 243
4.3.8.1 Adding a CD/DVD Drive to the Virtual Machine . . . 257
4.3.8.2 Installing the OpenScape Voice . . . 259
4.3.9 Migration from VMWare to Hyper-V . . . 261
4.3.9.1 HDD preparations for Hyper-V . . . 261
4.3.10 Migration from VMWare to Proxmox . . . 263
4.3.10.1 HDD preparations for Proxmox . . . 263
4.3.11 Create a Virtual Machine in Nutanix and install OpenScape Voice . . . 265
4.3.12 Migration from VMWare to Nutanix . . . 272
4.4 Post Software Installation Activities . . . 273
4.4.1 Profiles of Users root and srx . . . 274
4.4.2 Verify Remote Access for srx Account in a Standard Duplex . . . 274
4.4.3 Changing the User ID and Password for the IMM/iRMC/BMC Account . . . 276
4.4.4 Configuring the Ethernet NICs for Fixed Operation . . . 288
4.4.5 Checking Ethernet Port Assignments . . . 290
4.4.6 Testing the KVM/Mouse Combination . . . 291
4.4.7 SNMP Community Names on OpenScape Voice . . . 292
4.4.7.1 Changing the Community String for the Emanate Master Agent . . . 293

5 Installing the OpenScape Applications . . . 295
5.1 Installation Overview . . . 295
5.1.1 Prerequisites . . . 297
5.1.2 External (Offboard) Applications Server Hardware Requirements . . . 298
5.2 Installation Instructions for Applications Servers . . . 299
5.2.1 SLES Partitioning and Installation on the External Applications Server . . . 299
5.2.2 External Applications Server Port List . . . 299
5.2.3 Installation/Update Instructions for Integrated Simplex Systems . . . 301
5.2.3.1 Prepare Installation of Integrated Simplex . . . 301
5.2.3.2 Response File for Integrated Deployments . . . 302
5.2.3.3 Installation of Integrated Applications . . . 305
5.2.3.4 Adding Additional Packages/Languages . . . 307
5.2.3.5 Update/Upgrade of Integrated Applications . . . 310
5.2.3.6 Installing a HotFix - Integrated Apps server . . . 313

5.2.3.7 Special Instructions: How to upgrade OSV Integrated Simplex to an OSV Image with OpenScape Applications lower than the already installed . . . 316
5.2.4 Updating using the CMP (UI Patching) instead of osc-setup . . . 317
5.2.4.1 General Considerations . . . 317
5.2.4.2 Procedure . . . 318
5.2.5 Installation/Update Instructions for Media Server Standalone . . . 323
5.2.5.1 Prepare the Installation Medium of a Standalone Media Server . . . 325
5.2.5.2 Response File for Media Server Standalone deployments . . . 325
5.2.5.3 Installing Media Server Standalone . . . 328
5.2.5.4 Adding Additional Packages/Languages . . . 330
5.2.5.5 Update Media Server StandAlone . . . 330
5.2.5.6 Installing a HotFix - Media Server StandAlone . . . 330
5.2.5.7 Uninstall the Media Server Applications . . . 330
5.2.6 Installation/Update Instructions for Multiple Communications Server Admin deployment . . . 331
5.2.6.1 Providing a Server Standalone Setup Medium . . . 332
5.2.6.2 Response File for Multiple Communication Server Administration deployments . . . 332
5.2.6.3 Installing Multiple Communications Server . . . 335
5.2.6.4 Adding Additional Packages/Languages . . . 337
5.2.6.5 Update Multiple Communications Server . . . 337
5.2.6.6 Installing a HotFix - Multiple Communications Server . . . 337
5.2.6.7 Remote Access for srx Account . . . 337
5.2.6.8 Survival Authority on the Multiple Communications Server Admin deployment . . . 337
5.2.6.9 Uninstall the Multiple Communications Server Admin Applications . . . 337
5.2.7 Configuring the OSV Connectivity in CMP . . . 338
5.2.8 Activating IPSec Between OpenScape Voice and the External Applications Server . . . 339
5.2.9 Configuring Billing Servers and Billing Clients . . . 339
5.2.9.1 Configure Billing Servers . . . 340
5.2.9.2 Configure Billing Clients . . . 341
5.2.10 Providing a Setup Medium for the Applications . . . 341
5.2.10.1 Create Setup medium from ISO files on the server hard disk . . . 343
5.2.10.2 Create Setup medium from ISO files on a USB media . . . 345
5.2.10.3 Create Setup medium from ISO files on a CD/DVD media . . . 347
5.2.10.4 Finish the Installation Medium Setup . . . 349
5.2.11 Cleaning up the Repositories . . . 354
5.2.12 Uninstall External (OffBoard) Applications Server Applications . . . 356
5.2.13 Apply an Update - Offboard (External) Apps Server . . . 356
5.2.14 Installing a HotFix - Offboard (External) Apps Server . . . 359
5.2.15 Adding Additional Packages/Languages - Offboard (External) Apps Server . . . 362
5.2.16 syncUC . . . 365
5.2.16.1 Introducing syncUC . . . 365
5.2.16.2 syncUC Commands . . . 366
5.2.16.3 Switching from File System Backup to syncUC . . . 368
5.2.16.4 Fallback Preparation . . . 370
5.2.16.5 Links back . . . 370
5.3 Starting and Stopping the OpenScape Applications . . . 370
5.4 Accessing the OpenScape Applications . . . 371
5.4.1 Accessing the CMP/OpenScape Voice Assistant . . . 371
5.4.2 Accessing DLS . . . 372
5.4.3 Accessing CLM . . . 372
5.5 Retrieving Trace File Information . . . 373
5.6 Installing a HotFix . . . 376
5.7 Upgrade of Offboard (External) Apps Server . . . 376

5.7.1 Upgrade of V8R1 Offboard Applications to V10 . . . 377
5.7.2 Fallback During Upgrade Procedure . . . 382
5.7.2.1 Fallback of Integrated System . . . 382
5.7.2.2 Fallback of External Applications Server using syncUC . . . 382
5.7.2.3 Fallback of External Applications Server through Restoration in the CMP . . . 383

6 Survival Authority and IPMI Shutdown Agents . . . 387
6.1 Shutdown Agent Overview (Non-Virtual environment) . . . 389
6.2 Shutdown Agent Overview (Virtual environment) . . . 390
6.3 Hints on Survival Authority placement . . . 391
6.4 Survival Authority on the CMP . . . 392
6.5 Installing a Standalone Survival Authority . . . 395
6.5.1 Installing the Java Runtime Environment . . . 396
6.5.2 Minimal Firewall Recommendations for the Standalone Survival Authority . . . 397
6.5.3 Installing the Standalone Survival Authority . . . 400
6.6 Configuring the Standalone Survival Authority for a Network Address Translation (NAT) case . . . 405
6.7 Updating the Standalone Survival Authority . . . 407
6.8 Verifying the Shutdown Agents Configuration . . . 409
6.8.1 Shutdown Agent Verification, Debugging and Data Collection from the OpenScape Voice 'tools' Menu . 410
6.8.1.1 Accessing the 'tools' menu . . . 410
6.8.1.2 Option 53. Failover Model - Displays the Network Configuration for Survivability . . . 411
6.8.1.3 Option 84. System Information - Collects Survival Authority Log Files and Data . . . 411
6.8.2 Monitoring the Shutdown Agents From the Nodes . . . 412
6.8.3 Examples of sa_down.log and sa_ipmi.log Output . . . 413
6.8.4 Activity Log for Survival Authority Action . . . 414

7 Overview of Upgrades and Migrations to OpenScape Voice V11 . . . 417
7.1 Feature Support Notes . . . 420
7.1.1 Source Based Routing . . . 420
7.1.2 Flexible Ethernet circuit and IP Address Configuration . . . 421
7.1.3 Cluster Timeout . . . 421
7.1.4 Broadcast Routes . . . 422
7.2 Solution Upgrade Considerations . . . 422
7.2.1 Servers No Longer Supported . . . 422
7.2.2 Hardware Platform Migrations . . . 422
7.2.3 Additional Servers for Migrations to Standard Duplex . . . 423
7.3 Upgrade and Migration Scenarios . . . 424
7.3.1 Upgrade Scenarios . . . 424
7.3.1.1 Supported Upgrades . . . 425
7.3.1.2 Upgrades Not Supported . . . 425
7.3.1.3 Remote Software Upgrade as an Alternative Upgrade Choice . . . 426
7.3.2 Hardware Migrations . . . 426
7.3.3 Product/Node Deployment Migrations . . . 426
7.4 Completing the Upgrade/Migration to V11 . . . 428
7.5 Post Upgrade Actions . . . 436
7.5.1 Create CLI Users . . . 437
7.5.2 Create Linux Accounts for CLI Users . . . 437
7.5.3 Modifying Node Names . . . 439
7.5.4 Take File System and Database Backups . . . 439
7.5.5 Synchronize the OpenScape Voice Partitions . . . 441

8 Upgrades to OpenScape Voice V11 443
8.1 Procedure Descriptions 444
8.1.1 Applicable Upgrade Scenarios 445
8.1.2 Preparation Checklist 445
8.1.3 Required Documents 447
8.1.4 Outage Free Toolkit Upgrade (Live Upgrade) Overview 449
8.1.5 Outage Free Toolkit Upgrade (Live Upgrade) Operational Impacts 451
8.1.5.1 Provisioning 451
8.1.5.2 Call Processing 452
8.2 Prerequisites 454
8.2.1 System Information and Access Rights 454
8.2.2 Logging 454
8.2.3 Verify the 'fstab' File Permissions in Virtual OSV Deployments 454
8.2.4 Change vNIC type from E1000 to VMXNET3 455
8.3 Preparation Phase 455
8.3.1 Create the Node.cfg for the Target System 456
8.3.1.1 Overview of Creating Node.cfg for the Target Release 456
8.3.1.2 Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release 457
8.3.2 Prepare Files for the Upgrade 458
8.3.2.1 Prepare Upgrade Files in Repository of OSV Node(s) 458
8.3.3 Verify Prerequisites Met According to Release Notes 461
8.3.4 Obtain Licenses for the Target Release 462
8.4 Pre-Maintenance Window Activities 463
8.4.1 Run RapidStat on Both Nodes and Analyze Output 463
8.4.2 Make Test Calls and Document Results 463
8.4.3 Perform Any Customer Specific System Checks 464
8.4.4 Verify Source Release Patch Set Level 465
8.4.5 Perform a Database and File System Backup 465
8.4.6 Verify the Ethernet Configuration of the External Applications Server 465
8.4.7 Verify the Hosts File Configuration 465
8.4.8 Verify Presence of IP Address and FQDN of External CMP 467
8.4.9 Save Cron Tables Data 468
8.4.10 Save CLM Data for an Integrated Simplex System 468
8.4.11 Executive Assistant with Cockpit 469
8.4.12 Disable SIP Session Timer 469
8.4.13 List the Languages Installed on the Applications Server 470
8.4.14 Record any Scheduled CMP Backup or Export Tasks 471
8.5 Upgrade of an OSV Integrated Simplex System 471
8.5.1 Overview 471
8.5.2 Upgrade Steps for an Integrated Simplex System 476
8.6 Upgrade of an OSV Duplex System Using Live Upgrade 483
8.6.1 Overview 483
8.6.2 Upgrade Steps for a Duplex System 486
8.7 Upgrade of an OSV System Using Remote SW Upgrade 491
8.7.1 Overview 491
8.7.2 Upgrade Steps for Remote SW Upgrade 493
8.8 Invoking Upgrade 498
8.8.1 Simplex Configuration: Invoke Upgrade from the CMP/Assistant (UI Method) 498
8.8.2 Simplex Configuration: Invoke Upgrade from Console or VM Console with Upgrade Files on Node's Repository 500
8.8.3 Simplex Configuration: Invoke Upgrade from the Console with Upgrade Files on External Media . . 501

8.8.4 Duplex Configuration: Invoke Live Upgrade from the CMP/Assistant . . . 503
8.8.5 Duplex Configuration: Invoke Live Upgrade from Console or VM Console with Upgrade Files on Nodes' Repository . . . 505
8.9 Fallback Procedures . . . 507
8.9.1 Fallback Procedure 1 for Outage Free Toolkit . . . 508
8.9.2 Fallback Procedure 2 for Outage Free Toolkit . . . 508
8.9.3 Manual Fallback on Failed Upgrade . . . 509
8.9.4 Fallback when Console is not Responsive . . . 510
8.9.5 Fallback Due to Failure During Installation for Remote SW Upgrade . . . 512
8.9.6 Fallback Due to Failure During Import for Remote SW Upgrade . . . 513
8.9.7 Fallback using File System Restore . . . 515
8.10 Resolving Migration Toolkit node.cfg File Creation Issues . . . 517
8.10.1 Correct the node.cfg using the IFGUI Update (EZIP) . . . 518
8.10.2 Correct the node.cfg using the create_node.cfg.pl Script . . . 518
8.10.3 Links to the Upgrade/Migration Procedures . . . 519

9 Migrations to OpenScape Voice V11 . . . 521
9.1 Migration Scenarios . . . 523
9.1.1 Simplex to Simplex Migration . . . 523
9.1.2 Simplex to Standard Duplex Migration . . . 529
9.1.3 Standard Duplex to Standard Duplex Migration . . . 537
9.2 Create the Node.cfg for the Target System . . . 542
9.3 Download and Install the Migration Toolkit Software to the Source System . . . 548
9.4 Exporting Source System Data . . . 549
9.5 Downloading and Installing the Migration Toolkit Software to the Target System . . . 551
9.6 Importing the Source System Data to the Target System . . . 552
9.6.1 Restore the data of the VM source . . . 553
9.7 Remove the Migration Toolkit Software from the Target System . . . 554
9.8 Configure the OpenScape Applications Server for Access to the Nodes . . . 554
9.9 Create the Node.cfg for the Target System (Source system = Low Cost) . . . 557
9.10 Restrictions for Migrations In Which The Network Configuration Is Changed . . . 559
9.11 Simplex System response.cfg.primary File Creation . . . 562
9.11.1 Building Simplex Response File from Older Response File . . . 562
9.11.2 Building Simplex Response File from Template . . . 563
9.11.3 How to Determine Admin IP Address of Node 1 (nafo0 IP) . . . 564
9.12 Customization of Nodes . . . 565
9.12.1 Customizing Node 1 . . . 565
9.12.1.1 Log In to Node 1 . . . 565
9.12.1.2 Customize Node 1 . . . 567
9.12.2 Customizing Node 2 . . . 568
9.12.2.1 Log In to Node 2 . . . 568
9.12.2.2 Customize Node 2 . . . 570

10 Basic Traffic Tool . . . 573
10.1 Installation (Server) . . . 573
10.2 Installing (Client) . . . 573
10.3 Using the Tool . . . 573
10.3.1 Graphical and Numerical Data Screens . . . 574
10.3.2 Menu Structure . . . 574
10.4 Feature Considerations . . . 575

11 Example Install_Time.log . . . 577

12 Changing NTP Server or DNS Configurations . . . 579

13 Updating the Node.cfg File (Also Known as EZIP) . . . 581
13.1 **Verify the System Health before EZIP Configuration Change . . . 582**
13.2 EZIP Methods . . . 583
13.2.1 EZIP Method Using the CMP . . . 583
13.2.2 EZIP Method Using the NCPE Tool in Update Mode . . . 584
13.2.2.1 Preparation . . . 584
13.2.2.2 Update the node.cfg file for the OpenScape Voice system . . . 585
13.3 Verify the System Health after EZIP Configuration Change . . . 590
13.4 Data Collection for EZIP issues . . . 590
13.4.1 Accessing the 'tools' Menu and Example Session Collecting the EZIP log files and data . . . 591

14 Media Server Hardware Requirements and Prefix Access Code Installation . . . 597
14.1 Hardware Recommendations for the OpenScape Media Server at OpenScape Voice . . . 597
14.2 How to Add/Delete Default PACs for Vertical Services . . . 598
14.2.1 Add Default PACs for Vertical Services Using the pac.sh Script . . . 598
14.2.2 Delete the Default PACs (Prefix Access Codes) for Vertical Services Using the pac.sh Script . . . 602

15 Example data collection session with the OSV Tools . . . 603

16 Flexible Ethernet circuit and IP Address Configuration Examples . . . 609
16.1 Static IP notes . . . 609
16.2 Virtual IP notes . . . 609
16.3 Node.cfg file changes on page IP Configuration 1/6 . . . 610
16.4 Co-located Cluster Signaling Subnet . . . 610
16.5 Separated Cluster Signaling Subnet . . . 612

17 Security . . . 615
17.1 Hardware and BIOS Settings . . . 615
17.1.1 Hardware Settings . . . 615
17.1.2 BIOS Settings . . . 616
17.2 Operating System . . . 617
17.2.1 Close Unused IP Ports . . . 617
17.2.2 Password Management . . . 617
17.2.2.1 Change Predefined Passwords for Administrator Accounts . . . 617
17.2.2.2 Change Predefined Passwords for Application Accounts . . . 619
17.2.3 Change Default Password Policies for New Accounts . . . 620
17.2.4 Change Denial of Service Thresholds . . . 625
17.2.5 Allow IPsec Fragmentation . . . 627
17.2.6 Turn on IPsec (Internet Protocol Security) Between Servers . . . 629
17.2.7 TLS (Transport Layer Security) Certificates . . . 631
17.2.7.1 Change the Default TLS Certificates . . . 631
17.2.7.2 Activate Verification for Mutual TLS . . . 631
17.3 Securing Interfaces . . . 634
17.3.1 Securing the Administration Interface . . . 634
17.3.1.1 SNMP Community Name . . . 634
17.3.1.2 Securing SOAP Signaling . . . 637
17.3.1.3 Securing SOAP Signaling via IPsec . . . 637
17.3.1.4 Securing SOAP Signaling via TLS . . . 638
17.3.1.5 Adding Authorization to SOAP . . . 640
17.3.1.6 Firewalling the SOAP Clients . . . 641
17.3.2 Securing the IMM or iRMC Access . . . 641

17.3.2.1 Restrict IPMI to Internal Networks . . . 641
17.3.2.2 Change the Default Passwords for the IMM/iRMC Card . . . 641
17.3.3 Securing the Signaling Interface . . . 642
17.3.3.1 Activate TLS Signaling for SIP Subscribers . . . 642
17.3.4 Activate TLS Keep-Alive for OpenStage Phones . . . 644
17.3.4.1 Activate MTLS Signaling for SIP Endpoints . . . 645
17.3.4.2 Activate Digest Authentication to the SIP Subscribers and SIP Endpoints . . . 645
17.3.4.3 Activate Authentication of SIP Subscribers and SIP Endpoints behind Trusted Endpoints . . . 647
17.3.4.4 Securing Media Servers . . . 648
17.3.4.5 Securing CSTA Applications . . . 649
17.3.5 Securing the Billing Interface . . . 649
17.4 Used IP Ports . . . 650

18 OpenScape Voice Signaling Stream Security . . . 651
18.1 TLS Overview . . . 651
18.1.1 Endpoint Signaling . . . 652
18.1.1.1 TLS Protection of Endpoint Device SIP Signaling . . . 653
18.1.1.2 TLS Protection of SIP and SIP-Q Server Signaling . . . 654
18.1.2 Sample Connection Call Flows . . . 655
18.1.3 OpenScape Voice Platform Signaling Managers . . . 658
18.1.4 DNS Survivability Overview . . . 659
18.1.5 High Availability with SRV . . . 660
18.1.5.1 Simple Example Including DNS Server . . . 661
18.1.6 Interaction of DNS-SRV and TLS . . . 662
18.1.6.1 Example 1 . . . 664
18.1.6.2 Example 2 . . . 665
18.1.6.3 Example 3 . . . 666
18.1.6.4 Example 4 . . . 667
18.1.7 Practical Deployment Recommendations . . . 668
18.2 Client (Endpoint) Authentication . . . 669
18.3 Media Server Signaling . . . 669

19 IPSec Configuration . . . 671
19.1 Using IPSec . . . 671
19.2 Configuring IPSec for CSTA Connections . . . 673
19.2.1 Configuring OpenScape Voice for IPSec-based CSTA Connections . . . 673
19.2.2 Configuring OpenScape UC Application for IPSec-based CSTA Connections . . . 677
19.3 Configuring IPSec for MGCP Connections . . . 682
19.3.1 Configuration for Standard Duplex (small) . . . 682
19.3.1.1 Configuring OpenScape Voice for IPSec-based MGCP Connections (Standard Duplex (small)) . . . 683
19.3.1.2 Configuring OpenScape UC Application for IPSec-based MGCP Connections (Standard Duplex (small)) . . . 685
19.3.2 Configuration for Standard Duplex (large) . . . 690
19.3.2.1 Configuring OpenScape Voice for IPSec-based MGCP Connections (Standard Duplex (large)) . . . 690
19.3.2.2 Configuring OpenScape UC Application for IPSec-based MGCP Connections (Standard Duplex (large)) . . . 694
19.4 Support of IKEv2 . . . 699
19.4.1 OSV side configuration . . . 699
19.4.2 UC side configuration - CSTA . . . 701

20 Advanced Locking ID Guidelines 705
20.1 "Native" OSV Server 705
20.1.1 Overview 705
20.1.2 Displaying the Native OSV eth0 HWaddr (MAC address) 705
20.1.3 Displaying the Native OSV server License Locking ID Information 706
20.2 Virtual OSV Server 707
20.2.1 Overview 707
20.2.2 How to determine the parameters of the virtual machine Locking ID 707
20.2.3 Displaying the Virtual OSV server License Locking ID Information 712
20.2.4 Examples of License Locking Id Info and Accepted ALIs 713

21 Configuring the OSV Nodes for Shutdown. 715
21.1 Overview 715
21.2 Shutting Down the Node(s) 715

22 Building an ISO file on the OSV or Applications Server 719
22.1 Overview 719
22.2 Command Example 720
22.3 Example Session Log 721

23 Shutdown Agent Failover Model and Data Collection displays 727
23.1 Overview 727
23.2 Option 53. Failover Model - Displays the Network Configuration for Survivability 727
23.3 Option 84 System Information - Collects Survival Authority log files and data 733

24 VM Upgrade/Migration Help 735
24.1 Overview 735
24.2 Adding a CD/DVD drive to an in-service OSV cluster node (or nodes) 736
24.3 Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration 738
24.3.1 Overview 738
24.3.2 Making the OSV Image ISO file available from CD/DVD drives during a VM Upgrade/Migration . . 738
24.3.3 Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration . . . 739
24.4 Export Source System Data 740
24.5 Install the OpenScape Voice V11 Image onto the Upgrade VM Target System 741
24.5.1 Overview 741
24.5.2 Shutdown of the Native Hardware OSV Nodes 741
24.5.3 Target Release Image Install 742
24.6 Restore the Data of the Source System to the VM Target System 748

25 Upgrading ESXi 749
25.1 Upgrade VMware ESXi 5.1 to ESXi 5.5 749
25.2 Upgrade VMware ESXi 5.5 to ESXi 6 749
25.3 Upgrade VMware ESXi 6 to ESXi 6.5 749
25.4 Upgrade Example for Reference Purposes 749
25.4.1 Upgrade Steps 749
25.4.2 Screen Shots 750
25.4.3 Backing up our ESXi Host Configuration 766
25.4.4 Requirements 766
25.4.4.1 How to Enable Remote SSH 767
25.4.5 Start the Upgrade using ESXi 5.0 Hypervisor DVD 771
25.4.5.1 Upgrading the Virtual Machines VMware Tools 771

26 Modifying the /etc/hosts file. 775
26.1 Adding Additional Hosts 776

26.2 Modifying an Existing Host Entry . . . 777
26.3 Configuring the Nodes to Complete the Update Process . . . 777
26.3.1 Example Configuration Sequences . . . 778
26.3.1.1 Node 1 . . . 778
26.3.1.2 Node 2 . . . 779

27 Modifying the /etc/sysconfig/proxy-osv file . . . 781

28 Guidelines for Language and Application Package adds to Simplex Systems . . . 783
28.1 Overview . . . 783
28.1.1 Language Package Add Syntax . . . 784
28.1.2 Applications Package Add Syntax . . . 784
28.2 Supported Languages for Announcement Texts of the Media Server for PBXs . . . 785
28.3 Language Codes of the supported TTS Languages . . . 786
28.4 Media Server Autoattendant Packages Codes . . . 787
28.5 Media Server Voice Portal Language Package Codes . . . 787
28.6 Language Codes of the supported Conferencing Languages . . . 788
28.7 Language Codes of the supported ASR Languages . . . 788
28.8 Language Codes of the supported Voiceportalspeech Languages . . . 789
28.9 Procedure Example for Media Server Languages . . . 789
28.9.1 Adding Additional Packages/Languages . . . 789
28.10 Cleaning up after the Installation . . . 792

29 Guidelines for Configuring NIC Teaming on the VM Host . . . 795

30 Solution Upgrades . . . 807
30.1 Solution Overview . . . 807
30.1.1 Upgrade Paths . . . 808
30.1.1.1 Upgrades Addressed in OpenScape Voice Service Manual, Installation and Upgrades . . . 809
30.1.1.2 Upgrades Addressed in OpenScape UC Application Installation and Upgrade, Installation Guide . 809
30.1.2 General Sequence of the Solution Upgrade . . . 809
30.2 Upgrade Sequence for Solution Upgrades . . . 811

31 Change E1000 to VMXNET3 network adapters . . . 815

Index . . . 825

History of Changes

Issue	Date	Changes
01	May - June 2025	**Support for OSV virtualization with HyperV and migration to Proxmox** Added chapters: Section 4.3.8, “Create a Virtual Machine in Hyper-V” Section 4.3.9, “Migration from VMWare to Hyper-V” Section 4.3.10, “Migration from VMWare to Proxmox” **OpenScape Voice V11** Removed unsupported HW: IBM x3550 M3, IBM x3550 M4, Lenovo x3550 M5, FTS RX200 S6, FTS RX200 S7 Removed mentions of the above from accross the document Updated mentions of OSV version to V11 Removed the following chapters: 3.1.1 - 3.1.3, 3.1.6 - 3.1.7, 3.3 - 3.6 Modified chapter 4.2.2 Correction on images of 4.2.3.3 Modified table 16 at chapter 7 Updates in chapter 5 Installing the OpenScape Applications Added two notes in chapters Section 9.12.1.2, “Customize Node 1” and Section 9.12.2.2, “Customize Node 2” for limitation with OSMO - Dynamic ONS licensing Added note in chapter Section 8.3.4, “Obtain Licenses for the Target Release” for LTSS feature Added note for older/unsupported HW under chapter 3.1 Computing node
02	November 2025	Added the **Lenovo SR630 V3** platform
03	December 2025	Added SSP/SWA license information for upgrading from V11 and above. Added new Nutanix chapters: • Section 4.3.11, “Create a Virtual Machine in Nutanix and install OpenScape Voice” • Section 4.3.12, “Migration from VMWare to Nutanix”
4	January 2026	Added SUSE Base license information for upgrading from V11 and above.
5	February 2026	Added Prerequisite Package List for Standalone Media Server Installation on SLES 15

Issue	Date	Changes
6	March 2026	Updated the following sections: • Section 2.6.4.3, “DNS Configuration” • Section 4.3.2, “Checklist for Virtualization” • Section , “Survival Authority and IPMI Shutdown Agents”
7	March 2026	Improvements throughout the document (removal of obsolete content). Updated the following sections to improve the procedures for exporting and importing source system data: • Section 9.6.1, “Restore the data of the VM source” • Section 9.4, “Exporting Source System Data” • Section 24.6, “Restore the Data of the Source System to the VM Target System” • Section 24.4, “Export Source System Data”
8	March 2026	Updates for SUSE Update Subscription & SSP (Software Support Plan) / SWA (Software Assurance) License: • Section 8.3.4, “Obtain Licenses for the Target Release”
9	May 2026	Additions and Improvements regarding upgrading of OpenScape Applications • Section , “Installing the OpenScape Applications” • Section 2.6.4.3, “DNS Configuration”
10	June 2026	Updated Section 4.3.10, “Migration from VMWare to Proxmox”
11	June 2026	Updated Section , “Installing the Hardware Platform”

1 Important Notices

1.1 About this Book

This book guides installation personnel through the process of installing the hardware and software up to and including the point where provisioning can begin and the expanded network components can be installed and verified. The user must refer to the provisioning and expanded network component document (s) to support that phase of the system installation process.

1.1.1 Audience

The audience for this guide is Professional Services and Back Level Support personnel. Note that this does not preclude other company personnel, customers, or third-party service providers who have the necessary prerequisite knowledge from using the guide.

1.1.2 Prerequisite Knowledge

This guide is written to the user who has:

- Successfully completed the OpenScape Voice installation and technical training courses.
- Advanced SuSE Linux Enterprise Server (SLES) operating system and Microsoft Windows operating systems knowledge and experience.
- Basic knowledge of the third-party platforms and equipment used for OpenScape Voice including: their physical characteristics, their assembly, their documentation (installation, service, and troubleshooting), and the documentation web sites associated with the third-party platform and equipment manufacturers.
- Basic knowledge of the industry standards and specifications utilized by OpenScape Voice and associated equipment.

The procedures in this guide require an understanding of and adherence to local safety practices, the safety practices identified in this guide, and the safety practices identified in the third-party documentation.

1.1.3 Viewing the Document with Adobe Reader

When viewing the document with Adobe Reader add the “Previous View” icon to the Reader toolbar. This will ease the navigation between this procedure and associated sections of the document.

1.1.4 Special Notices

Potentially dangerous situations are noted throughout this guide. The three alert methods are defined below:

DANGER	A danger notice calls attention to conditions that, if not avoided, will result in death or serious injury.
WARNING	A warning notice calls attention to conditions that, if not avoided, could result in death or serious injury.
Caution	A caution notice calls attention to conditions that, if not avoided, may damage or destroy hardware or software.

1.2 Safety

The following information is included in this publication for the use and safety of installation and maintenance personnel.

1.2.1 General Safety

- Do not attempt to lift objects that you think are too heavy for you.
- Do not wear loose clothing; tie back your hair while working on machines.
- Wear eye protection when you are working in any conditions that might be hazardous to your eyes.
- After maintenance, reinstall all safety devices such as shields, guards, labels, and ground wires. Replace worn safety devices.
- If you feel any action is unsafe, notify your manager before proceeding.
- Do not use a telephone to report a gas leak while in the vicinity of the leak.

1.2.2 Safety with Electricity

Danger: Do not take chances with your life. Follow these safety guidelines carefully.

1.2.2.1 High Voltages

- Observe all safety regulations and read the warnings, cautions, and notes posted on the equipment.
- Find the switch to power off the cabinet. Read the posted instructions.
- Ensure that a machine cannot be powered on from another source or controlled from a different circuit breaker or disconnecting switch.
- When a procedure requires that you power off the system:
  - Lock the wall box-switch in the off position.
  - Attach a DO NOT OPERATE tag to the wall box-switch.
- ***Never assume*** that the power is turned off. Always check to ensure that a circuit does not have power.

- Do not work alone. Work with another person who knows the locations of the power-off switches, especially if you are working with *exposed* electrical circuits.
- Follow the instructions in the manual carefully, especially when working with circuits that are powered. Disconnect power when instructed to do so in the procedures.
- Disconnect all power before working near power supplies unless otherwise instructed by a maintenance procedure.
- Disconnect all power before installing changes in machine circuits unless otherwise instructed by a maintenance procedure.
- High voltages capable of causing shock are used in this equipment. Be extremely careful when measuring high voltages and when servicing cards, panels, and boards while the system is powered on.
- Do not wear jewelry or other metal objects.
- When possible, work with one hand so that a circuit is not created. Keep the other hand in your pocket or behind your back.
- Use caution when installing or modifying telephone lines. Never install telephone wiring during an electrical storm.
- Never install a telephone jack where it can get wet unless the jack is specifically designed for wet conditions.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Avoid using a telephone (other than the cordless type) during an electrical storm due to the remote risk of shock from lightning.

1.2.2.2 Equipment Room

- Look for hazards in your area and eliminate them. Examples are moist floors, ungrounded power extension cables, power surges, and missing safety grounds.
- Rubber electrostatic mats will not protect you from electrical shock. Do not use them for this purpose. Stand on suitable rubber mats to insulate you from grounds such as metal floor strips and machine frames.
- Do not use tools covered with a soft material that does not insulate you when working with powered circuits. Use only tools and testers suitable for the job. Do not use worn or broken tools or testers; inspect them regularly.
- Set controls on testers correctly and use approved probe leads and accessories intended for that tester.

- The surface of a mirror is conductive. Do not touch powered circuits with a mirror. To do so can cause personal injury and machine damage.
- Do not store combustible gases or flammable materials in cabinets near the site.

1.2.2.3 Emergencies

- Be familiar with first aid for electrical shock. This includes resuscitation methods, heartbeat restoration, and burn treatment.
- Use caution if an accident occurs. Disconnect the power before touching the victim.
- If you do not know how to disconnect the power, use a nonconductive object, such as a wooden rod, to push or pull the victim away from electrical contact.
- Administer resuscitation if the person is not breathing.
- If you are trained and certified, administer cardiac compression if the heart is not beating.
- Call a rescue group, an ambulance, or a hospital immediately.

1.2.3 Reporting Accidents

- Report to your manager all accidents, near accidents, and possible hazards to ensure their causes are resolved as soon as possible.
- Report any electric shock, no matter how small.

2 Preparing for the Installation

2.1 About OpenScape Voice

OpenScape Voice is available as a redundant or a single-node system:

- OpenScape Voice redundant is available in a standard duplex configuration:

  The nodes in an OpenScape Voice redundant system can be deployed as follows:

  – Co-located nodes

  – Geographically separated nodes in either the same subnet or in different subnets.

    The cluster interconnect links for geographically separated nodes employ a layer 3 IP connection.

    The layer 3 IP cluster interconnect connection is via an IPsec encrypted IP connection in transport mode. If the cluster interconnect traffic passes through a firewall, the firewall might block all this traffic. If this is the case, ensure that the customer has defined custom rules in the firewalls to allow ICF traffic.

    Note: The distance between geographically separated nodes is limited by a maximum round-trip delay between the nodes of 100 milliseconds. The theoretical maximum distance is 6,000 miles (10,000 kilometers), but the customer’s network must be able to keep the round-trip delay between the nodes to less than 100 milliseconds.

  – Applications associated with the Standard duplex configurations are installed on an external server or servers depending upon the Applications' deployment (i.e., a Standard Duplex Large deployment). As an example;.

    - OpenScape Voice Assistant
    - OSB Assistant
    - SBC Assistant
    - OpenScape Media Server
    - Customer License Manager (CLM)

- Common Management Platform (CMP)

Note: The OpenScape Media Server maybe installed on one or more separate external servers.

- OpenScape UC Application

Note: The OpenScape Applications Deployment Service (DLS) component might not be supported on the external applications server due to sizing limitations. A separate server running Microsoft Windows might be required for the DLS component. Please review the DLS release notes for sizing limitations when DLS is installed as a component of the external applications server.

- Integrated simplex: In this configuration, the OpenScape Applications (OpenScape Voice Assistant, OSB Assistant, SBC Assistant, OpenScape Media Server, Customer License Manager [CLM], Common Management Platform [CMP], Deployment Service [DLS], and OpenScape UC Application) are installed on the same server (the OpenScape Media Server or DLS can be optionally installed on a separate external server) that hosts OpenScape Voice.
- Low Cost systems are not supported. A Low Cost system in an older release must be migrated to a configuration supported in V11. Refer to Chapter 9, “Migrations to OpenScape Voice V11”.

2.1.1 Administration and Media Server Options

The administration and media server deployment options are as follows:

- Integrated simplex: The administration tools and OpenScape Media Server are installed on the same server (and additional external servers depending on configuration) that hosts OpenScape Voice.

- Standard duplex: The administration tools and OpenScape Media Server are installed on an external applications server (and additional external servers depending on configuration).

Attention: When servers (e.g., media server or DLS) in the same network as one of the OSV subnets need to communicate with another of the OSV subnets, then changes to the network firewall are required to allow this communication.

Attention: For Integrated Simplex deployments, the Media Server SIP endpoint shall be associated with the non-standard port numbers 5062 (SIP) and 5063 (SIP-TLS) for signaling between OSV and the Media Server. Section 5.2.3.1, “Prepare Installation of Integrated Simplex”, on page 301 for details.

2.1.2 OpenScape Branch

Available in conjunction with OpenScape Voice V11 is OpenScape Branch for remote branch offices.

OpenScape Branch provides:

- Continuance of communication services while providing a feature rich set of survivability capabilities at a remote branch location during loss of communication or service degradation between the remote branch and the main location.
- A local Media Server for tones, announcements and conferencing reducing the bandwidth needed between the locations.
- Proxy and Session Border Controller (SBC) functionality and security functions like Firewall and Virtual Private Network (VPN).
- Deployment on several hardware platforms: from one with a maximum capacity of up to 50 users to one with a maximum of up to 6000 users.
- Management via the main location’s OpenScape Voice CMP/Assistant and a localized OpenScape Branch Management Portal.

Refer to *OpenScape Branch VxRy Service Manual Volume 1, Installation and Upgrades*, for OpenScape Branch installation instructions (where VxRy indicates the released OpenScape Branch version, i.e. V1 R3).

2.2 Installing OpenScape Voice

2.2.1 Installation Media

The installation media is as follows:

- Reference Image ISO: One USB for a simplex system and two USBs for a redundant system

  The OpenScape Voice V11 Reference Image ISO provides the following components:

  – OpenScape Voice software

  – OpenScape Applications (OpenScape Voice Assistant, OpenScape Media Server, Customer License Manager [CLM], Common Management Platform [CMP], Deployment Service [DLS], and OpenScape UC Application)

  – SLES 15 operating system, and other miscellaneous and third-party software

- OpenScape Voice V11 Installation Wizard CD

  Provides several components that help you create the node.cfg file that is used during the installation to modify the Reference Image.

- Node.cfg and response file media

  One or two USB memory sticks as appropriate for the type of system (one for a single-node system and two for a redundant system).

Note: Response files no longer need to be generated for integrated systems and they should not be placed on USB sticks. If a response file is found on the USB stick that file will take precedence over the file that is automatically generated via the Image installation.

Note: An installation ISO image for each OSV node can be created and used for the installation and upgrade procedures of an OSV virtual system. This Installation ISO image of each OSV node includes the appropriate node.cfg file, license, Migration Toolkit and patch sets (including emergency patch sets).

- OpenScape Applications

  The Applications are delivered as multiple ISO files. The files required for your deployment scenario should be downloaded and installed as necessary.

For integrated systems, the OpenScape Applications are installed using the OpenScape Voice V11 Reference Image DVD. In the case of an integrated Simplex system installation or upgrade, response files are built automatically as part of the installation/upgrade process. Response files no longer need to be generated for images and are not required on USB sticks. If a response file is found on the USB stick, that file will take precedence over the file that is automatically generated via the Image installation.

Deployment Scenarios

The supported deployment scenarios are:

- Integrated Simplex
- Standard Duplex -Small deployment
- Standard Duplex - Large deployment
- Standard Duplex (Very Large)
- Media server stand alone
- Multiple Communication Server

This document contains the installation and update procedures of OpenScape UC Applications for the following deployment scenarios:

- Integrated Simplex
- Media server stand alone
- Multiple Communication Server

Note: Information for installing the OpenScape UC Application separately (apart from the normal OpenScape Voice installation) is included in the *OpenScape UC Application Vx, Installation Instructions, Installation Guide* (where *x* is the software release version). There the installation procedures for standard duplex - small, standard duplex - large and the Standard Duplex (very large) deployments are described.

2.2.2 Prerequisites and Assumptions

The building of the network infrastructure required to support OpenScape Voice and the network components associated with OpenScape Voice is outside the scope of this guide. The following is assumed:

- The design and the configuration of the network infrastructure for OpenScape Voice is complete.
- The IP addresses for OpenScape Voice and its expanded network components have been established and are available to the installation team.

- All the information necessary for creating the node.cfg file is available and has been provided to the installation team.
- All information relevant for implementing IPsec is available and has been provided to the installation team.

2.2.3 Backup License Recommendations

It is strongly recommended that backup license files, be readily available. This ensures a rapid return to service if a system restore must be performed.

Attention: OpenScape Voice may not be fully operational until these new licenses are installed.

Refer to the *OpenScape Voice Service Manual, Service Documentation* for detailed information on licensing.

2.2.4 OpenScape Voice Installation Checklist

Use the checklist as follows:

1. Make two copies of the checklist.
   - Keep one copy at the installation site in a location accessible by the installation team members.
   - Keep the other copy with you as a backup in the event something happens to the job site copy.
2. Inform the installation team members of the location of the checklist and ask them to initial the checklist item when they complete tasks for which they are responsible.
3. At the beginning and end of your shift each day, update your copy of the checklist to match the copy kept at the installation site.
4. Perform only the task indicated and then return to the checklist. As an example; if the checklist indicates Section 7.3.1 should be performed, follow the link to Section 7.3.1, perform that task, and return to the checklist.

Note: When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader toolbar. This will ease the navigation between the checklists and associated sections of the IUG.

Item	Description	Initials
Pre-installation activities: These activities should be completed prior to arriving at the customer's installation site to perform the physical installation tasks.		
1.	From SWS: • Download the OpenScape Voice V11 reference image, the Installation Wizard zip file, refer to the OpenScape Voice base software release note on G-DMS for the link to SWS, and the OpenScape Applications ISO images required for your deployment scenario. Refer to the latest version of the *OpenScape UC Application Vx Installation and Upgrade* document for details (where *x* is the software release version). **Attention:** Recommended practice for file transfer; If a checksum, md5sum or sha file is delivered with OpenScape software it is a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. **If necessary, third party software can be used to calculate these values.**	
2.	If necessary, prepare the patch sets and MOP materials. Refer to the OpenScape Voice V11 patch set release notes on G-DMS for a link to SWS and for instructions on downloading and preparing the patch sets and MOP materials.	
3.	Obtain the V11 license activation codes. **Attention:** OSV V11 upgrade/update actions from V10 with V9 licenses are not permitted, unless EMSS license extension has been purchased.	
4.	For an integrated system only, create the response file. Refer to Section 5.2.3, "Installation/Update Instructions for Integrated Simplex Systems", on page 301. Note: Integrated systems response files are built automatically as part of the installation process. Response files no longer need to be generated for images and are not required on USB sticks. If a response file is found on the USB stick, that file will take precedence over the file that is automatically generated via the Image installation.	
5.	Create a node.cfg file. • For non virtual machine server, refer to Section 2.6 on page 50. • For a virtual machine server, refer to Section 4.3.4, "Creating a Virtual Machine Node.cfg File", on page 259.	
On-site installation activities: These activities are performed at the local installation site and, as applicable, at associated remote sites.		
6.	If necessary, install the Ethernet switches into the rack. Refer to the rack and Ethernet switch documentation.	
7.	If necessary, install the servers.	

Table 1 OpenScape Voice Installation Checklist

Item	Description	Initials
8.	Install the OpenScape Voice V11 reference image. Refer to Chapter 4 for instructions. • The Virtual Machine environment installation can be found in Section 4.3, “Virtualization Environment Setup”, on page 241.	

Table 1 OpenScape Voice Installation Checklist

<table>
<tr><th>Item</th><th>Description</th><th>Initials</th></tr>
<tr><td>9.</td><td>Create a password for root and perform any other password and account management activities. Refer to the Appendix 17, “Security”. Also see Appendix 18, “OpenScape Voice Signaling Stream Security”.

Note: The active login profiles for users root and srx should not be modified. The OSV has functionality to protect the OSV login profiles for those two users from unauthorized changes. This is because alteration of these profiles typically causes issues to components that automatically login to the OSV nodes in order to perform various actions (e.g., NCPE/ EZ-IP, Assistant etc.). For details refer to Section 4.5.1, “Profiles of Users root and srx”, on page 338.

The OSV system is purged of unused non-system accounts (for security reasons). In order to address this safely and completely it is necessary to document some pre-requisites.

The customer accounts should not conflict with the "reserved" OSV accounts (and groups) listed below. If so, those customer accounts (or groups) should be removed.

Reserved OSV System Account IDs

<table>
<tr><th>Account Name</th><th>Account ID</th></tr>
<tr><td>*reserved*</td><td>501</td></tr>
<tr><td>sym</td><td>502</td></tr>
<tr><td>cdr</td><td>1001</td></tr>
<tr><td>srx</td><td>1522</td></tr>
<tr><td>solid</td><td>5000</td></tr>
<tr><td>superad</td><td>10000</td></tr>
<tr><td>sysad</td><td>10001</td></tr>
<tr><td>secad</td><td>10010</td></tr>
<tr><td>dbad</td><td>10011</td></tr>
<tr><td>*reserved*</td><td>10012</td></tr>
<tr><td>webad</td><td>10013</td></tr>
</table>

Reserved OSV Group IDs

<table>
<tr><th>Group Name</th><th>Group ID</th></tr>
<tr><td>rtpgrp</td><td>911</td></tr>
<tr><td>*reserved*</td><td>912</td></tr>
<tr><td>sym</td><td>913</td></tr>
<tr><td>dba</td><td>3020</td></tr>
<tr><td>cdrusers</td><td>3021</td></tr>
<tr><td>seclog</td><td>10001</td></tr>
<tr><td>*reserved*</td><td>10002</td></tr>
</table>
</td><td></td></tr>
</table>

Table 1 OpenScape Voice Installation Checklist

Item	Description	Initials
10.	Execute RapidStat to ensure the health of the OpenScape Voice system. Any Error or Warning messages should be addressed before proceeding. **Note:** During the server installation, IF you chose to configure the IMM/iRMC IP address, Netmask and Gateway data while configuring the BIOS settings, THEN the Remote Maintenance Controller **MAY NOT** have been updated with the OSV default sa_ipmi shutdown agent credentials during the OSV installation process. This may cause sa_ipmi test failures. Refer to step 11 of this task list to resolve this issue.	
11.	If needed, change the default user ID and password for the Intel Management Module account or Integrated Remote Management Controller (iRMC) account. Refer to Section 4.5.3 on page 341.	
12.	For duplex systems, verify the Survival Authority and IPMI shutdown agents. A description and functional overview of the shutdown agents can be found in Section , “Survival Authority and IPMI Shutdown Agents”. To verify the shutdown agents reference Section 6.8, “Verifying the Shutdown Agents Configuration”, on page 409. VMs are not configured with the IPMI shutdown agent.	
13.	If applicable, change the Ethernet NICs to a fixed operation mode (the default is auto-negotiation operation). Refer to Section 4.5.4 on page 347.	
14.	Check the Ethernet port assignments, refer to Section 4.5.5 on page 349.	
15.	If applicable, test the KVM/mouse combination. Refer to Section 4.5.6 on page 354.	
16.	If applicable, create and install Transport Layer Security (TLS) certificates. Refer to the Appendix 17, “Security”.	
17.	If necessary, apply MOPs. Refer to the MOPs for instructions.	
18.	If the customer is providing hardware for an external applications server, ensure that the server is installed and meets the requirements described in Section 5.1.2, “External (Offboard) Applications Server Hardware Requirements”, on page 298.	
19.	If the OpenScape UC Application is going to be deployed, refer to the OpenScape UC Application Installation and Planning guides for pre-installation requirements.	
20.	If applicable, verify remote access for the srx user account in a Standard Duplex configuration. Refer to Section 4.5.2, “Verify Remote Access for srx Account in a Standard Duplex”, on page 339.	
21.	For standard duplex only: Install OpenScape Applications onto the external applications server. Refer to Section 5.2, “Installation Instructions for Applications Servers”, on page 299.	
22.	If applicable, change the SNMP Community Names on the OpenScape Voice server. Refer to Section 4.5.7, “SNMP Community Names on OpenScape Voice”, on page 354.	

Table 1 OpenScape Voice Installation Checklist

Item	Description	Initials

23.	If the OSV licenses were not included on the Installation USB (Non VM) or the Installation ISO (VM) download the licenses to the OpenScape Voice nodes.
	• Simplex systems perform the activity of Section 9.12.1.2, “Customize Node 1”, on page 567 and then return to Checklist Item 24.
	• Duplex systems must perform both the Section 9.12.1.2, “Customize Node 1”, on page 567 and Section 9.12.2.2, “Customize Node 2”, on page 570 activities. Return to Checklist Item 24.
	--- 	
	Hint: Verify the license data has been updated to the OpenScape voice server. After the license files (or file in the case of a simplex system) are downloaded; wait at least 7 minutes and then display the License Usage Indicator info via Cli.
	
	Perform this exercise on both nodes of a duplex OpenScape Voice system.
	
	To access the RTP Cli interface enter ‘startCli’ from the OpenScape Voice server prompt (the OpenScape Voice server must be in state 4);
	`sysad@nodename:[/home/sysad] #183`
	`$ startCli`
	From the ‘Cli’ Main Menu select:
	6 (Application-level Management)
	1 (Softswitch Management)
	1 (Softswitch Information)
	10 (Software License Management)
	1 (Display Usage Indicator Info)
	
	The Usage Indicator display should reflect the values of the downloaded license files (or file in the case of a simplex system).
	
	Or, to enter the ‘expert’ form of RTP Cli enter ‘startCli –x’ from the OpenScape Voice server prompt (the OpenScape Voice server must be in state 4);
	`sysad@ nodename:[/home/sysad] #184`
	`$ startCli -x`
	`>licendpointdisplay`
	
	The Usage Indicator display should reflect the values of the downloaded license files (or file in the case of an simplex system).
	--- 		

24.	Import the subscriber database file using the Common Management Platform. Refer to the *OpenScape Voice Vx, Service Manual, Service Documentation* (where *x* is the software release version) or CMP online help for instructions.	
25.	For geo-separated deployments, refer to *OpenScape Voice, Administrator Documentation*, Section "How to Configure parameters for SIP FQDN (Fully Qualified Domain Name) Support" for instructions on how to enable FQDN support on the OpenScape Voice Server.	
26.	If applicable, ensure that OpenScape Voice is configured for OpenScape 4000 interoperability. Refer to the appropriate OpenScape Voice configuration documentation and OpenScape 4000 documentation for instructions.	
27.	If applicable, ensure that the OSB and SBC Assistants are installed and operational. For instructions, refer to the OSB and SBC documentation.	

Table 1 OpenScape Voice Installation Checklist

Item	Description	Initials
28.	If applicable, ensure that OpenScape Voice is configured for the gateway that provides E911 functionality.	
29.	Ensure that the billing servers or billing clients are installed. Refer to Section 5.2.9, “Configuring Billing Servers and Billing Clients”, on page 339.	
30.	For integrated systems, install any additional Media Server language(s). Reference Appendix 28, “Guidelines for Language and Application Package adds to Simplex Systems”, on page 783 for more details.	
31.	If applicable, ensure that the third-party media server, or servers, are installed and operational.	
32.	If applicable, ensure that the CAP server, or servers, are installed.	
33.	If applicable, ensure that the ComAssistant server/application is installed and operational.	
34.	If applicable, ensure that the OpenScape Xpressions server/application is installed and operational.	
35.	If applicable, ensure that the OpenScape Contact Center server/application is installed and operational.	
36.	Ensure that optiPoint soft clients are deployed and operational.	
37.	Ensure that OpenStage telephones are deployed and operational.	
38.	If applicable, verify OpenScape Voice interoperability with the OpenScape 4000.	
39.	If applicable, verify OpenScape Voice interoperability with the OSB and SBC Assistants.	
40.	Verify E911 functionality through the gateway that provides E911 functionality.	
41.	Ensure that the basic traffic tool is installed and configured. Refer to Chapter 10.	
42.	If applicable, ensure that branch survivability equipment is installed, configured, and functioning properly. For OpenScape Branch, refer to *OpenScape Branch V*/R* Service Manual Volume 1, Installation and Upgrades*, part number *A31003-H8113-J100-*-7631* for more information. If branch survivability solutions other than OpenScape Branch are employed, refer to the appropriate documentation for the survivability solution.	
43.	If applicable, ensure that IPsec-based connections are created for secure endpoints, SIP endpoints, media servers, and media gateways. Refer to Appendix 17, “Security”. (Section 17.2.6, “Turn on IPsec (Internet Protocol Security) Between Servers”, on page 629 contains a doc-link to return you to this step.)	
44.	At this time, it should be verified the system has been hardened as recommended by the *OpenScape Voice* V*x* Security Checklist Planning Guide (where *x i*s the software release version) . The Security Checklist Planning Guide contains the official signoff forms.	
45.	After system and feature verification is complete, perform a file system backup. Refer to the *OpenScape Voice* V*x*, Service Manual, Service Documentation (where *x i*s the software release version) or CMP online help for instructions.	

Table 1 OpenScape Voice Installation Checklist

2.3 Guidelines for Geographically Separated Nodes

2.3.1 Guidelines for Configuration Parameters of Geographically Separated Nodes

If the two OSV nodes are installed at different locations it is recommended to configure the nodes as follows (using the NCPE tool).

Note: References to OSV communication partner(s) are devices external to the OSV server (e.g. a SIP phone).

2.3.1.1 Node Separation = <none, separate>

Set '**Node Separatio**n' to '**none**' if the two nodes share the same IP networks (L2 geo separation). In case of a node failure the OSV communication partner only needs to know one OSV IP address as it switches over to the surviving node. It is recommended, although not required, to configure the communication partner with 2 OSV IPs (e.g. with DNS SRV) so that they can connect to the other OSV node in case of partial network failures.

Set '**Node Separation**' to '**separate**' to disable virtual IP failure and to allow for node 2 to be connected to different IP subnets than node 1 (L3 geo separation). In this case all OSV communication partners have to know the IP addresses of both OSV nodes.

2.3.1.2 StandAloneServiceEnabled = <yes, no>

The '**StandAloneServiceEnabled**' parameter determines how the nodes of the OSV cluster will react when they cannot communicate with each other via the x-channel. This action will avoid a 'split brain' situation.

When '**StandAloneServiceEnabled** 'is set to '**no**' the split brain situation is avoided by deactivation of one of the nodes.

If 'S**tandAloneServiceEnabled**' is set to '**yes**' both nodes will continue service in a limited capacity.

In **StandAloneService** one node is Primary and the other is Secondary. When an x-channel failure occurs;

- IP addresses of the partner are not activated (to avoid having the same IP at two locations)

- The secondary node does not allow any provisioning (to avoid two databases with conflicting data). The secondary node does not allow any provisioning (to avoid two databases with conflicting data).

Attention:

- The default configuration for OSV systems with '**Node Separation**' set to '**separate**' is '**StandAloneServiceEnabled**' = '**yes**'.

- **Setting StandAloneService** to '**yes**' **IS NOT** recommended for L2 geo separation (because of the restriction on IP address failover).

2.3.1.3 Survival Authority = <IP address>

In case the two OSV nodes cannot communicate with each other neither via x-channel nor the admin network, their connectivity to the Survival Authority decides which node Survives (if '**StandAloneServiceEnabled**' is set to '**no**') or which node transitions to StandAlonePrimary (if '**StandAloneServiceEnabled**' is set to '**yes**').

For the Survival Authority to be useful, it should not be placed within a failure unit that is common to either node of the cluster. If the Survival Authority fails along with a node this may trigger the surviving node to shutdown, resulting in a total outage; or in case of StandAloneService, go to StandAloneSecondary mode.

More Survival Authority information can be found in Chapter 6, “Survival Authority and IPMI Shutdown Agents”.

2.3.1.4 PreferredNodeToTakeOver = <node1, node2>

In case the two OSV nodes cannot communicate with each other via the x-channel; the node marked as '**PreferredNodeToTakeOver**' is the first node to invoke the shutdown agent(s) to deactivate its partner node (in order to avoid the split brain scenario). This should be the node that should survive a network failure, e.g. because it is co-located with OpenScape UC and other OpenScape applications.

Attention: Please note that if the '**PreferredNodeToTakeOver**' experiences a real HW failure (server crash) it will take approximately 30 seconds longer for the partner node to take over. The reason is that the partner node waits to be killed by the '**PreferredNodeToTakeOver**' before triggering its switchover procedure. The wait time is defined by shutdown agent timers.

2.3.1.5 Timezone is the always the same for both nodes

2.3.1.6 Cluster Timeout = 15 seconds

The default of 15 seconds should be kept. This is the time the x-channel needs to be down before one of the OSV nodes is deactivated or the nodes enter a standalone operation mode.

2.3.1.7 MTU X-Channel

The default is 1500. It should only be reduced in the rare cases where the network connection between the nodes does not support 1500 byte packets.

2.3.2 Guidelines for Static Routes of Geographically Separated Nodes

The following guidelines apply to static routes of geographically separated nodes.

The general rules for creating the static routes in the node.cfg file are:

- The “default router” in the node.cfg must be on the SIGNALING network (nafo1 [bond1] subnet) of OpenScape Voice.
- In general, all static routes should be created for the Admin network for both subnets (nafo0 [bond0]), except of the broadcast routes and the x-channel static routes that are automatically created for the Cluster network (nafo3 [bond3]).
- Create static routes for the SurvivalAuthority IP for both nodes.
- The '239.255.255.253 255.255.255.255 0.0.0.0 nafo0' route is no longer necessary. These routes were used for OpenScape Voice network broadcast and multicast messages.

For example, assume that the SIGNALING network IP addresses on the nafo1 (bond1) subnet and that the ADMIN network IP addresses on the nafo0 (bond0) subnet are as follows:

Parameter	SIGNALING NETWORK (bond1)	ADMIN NETWORK (bond0)
id	nafo1	nafo0
nafo group	nafo_udp	nafo_alias
itf1	bond1	bond0
itf2	bond1	bond0
node 1	10.5.11.10	10.5.12.10

Parameter	SIGNALING NETWORK (bond1)	ADMIN NETWORK (bond0)
node 2	10.5.131.20	10.5.132.20
netmask	255.255.255.0	255.255.255.0
subnet	10.5.11.0	10.5.12.0
gateway	10.5.11.1	10.5.12.1
broadcast	10.5.11.255	10.5.12.255
netmask_2	255.255.255.0	255.255.255.0
subnet_2	10.5.131.0	10.5.132.0
gateway_2	10.5.131.1	10.5.132.1
broadcast_2	10.5.131.255	10.5.132.255

Using the general rules and these network IP addresses, an example of the static routes created using the NCPE for the node.cfg file would be as follows:

```
default_router: 10.5.11.1
default_router_2: 10.5.131.1
domain_name: h8k.sec
survival_authority: 10.0.242.250
first_node_r1:   10.5.132.20  255.255.255.255  10.5.12.1  nafo0
first_node_bc1:   239.255.255.253  255.255.255.255  nafo3
second_node_bc1:   239.255.255.253  255.255.255.255  nafo3
second_node_r1:   10.5.12.10  255.255.255.255  10.5.132.1  nafo0
```

Consider the following regarding static routes:

- During the installation of OpenScape Voice geographically separated nodes, you will see error messages such as "network unreachable" on your console for the NTP server IP addresses and for all the "static route" IP addresses.

  These are expected errors because the bonding devices on the OpenScape Voice nodes are not set up at that time.

  After the bonding devices are created, these error messages will no longer be displayed, the cluster should go to state 4 4, and the L2/L3 interconnection test should pass successfully.

- The IFgui in update mode can be used to add static routes without causing an OpenScape Voice server outage. For details refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. Alternatively, the ManageRoutes.pl (/etc/hiq8000/ManageRoutes.pl) script can be employed to Update (Add or Delete) static routes in the OpenScape Voice systems while the system is in state 2, 3 or 4. The script is node specific, meaning only updates to the OpenScape Voice configuration data and O/S route data on the current node will take place. On a cluster system the command should be repeated on the other node. As user *root*, enter this command from the OpenScape Voice server command line (the resulting output is quite extensive and can be copied for future reference);

  # /etc/hiq8000/ManageRoutes.pl -info

- The default filter rules of OpenScape Voice block “pinging” through the SIGNALING network. To use “ping” through the ADMIN network, do the following:

  1. Get the bond0 IP addresses of the nodes with the command:

     ```
     # grep bond0 /etc/hiq8000/node.cfg
     ```

  2. Then use “ping” from Node1 with the command:

     ```
     # ping -I <bond0_IP_node1> <ping_IP>
     ```

     For example, assume bond0 is 10.5.12.10 for node1 and bond0 is 10.5.132.20 for Node2, issue the following command from Node1:

     ```
     # ping -I 10.5.12.10 10.5.132.20
     ```

     Or to “ping” with tracing, issue the command:

     ```
     # ping -R -I 10.5.12.10 10.5.132.20
     ```

2.4 Source Based Routes

Source based routing is supported; where OSV sends IP packets to an IP gateway/router based on which subnet the source IP of the packet belongs to. For this, default gateways should be specified for the OSV IP subnets admin, signaling and billing. If, for example, a billing gateway is specified, the OSV sends billing files via this gateway and there is no need for the creation of static routes to each billing server.

Another advantage of source base routing is that responses to admin requests from a remote IP network to the OSV admin IP address are sent back via the default admin gateway. Without this admin gateway, the response would be sent via the default router, which is usually on the signaling network.

Even with source based routing, there is a need for static routes because not all OSV Software specifies a source IP to an outgoing packet to give source based routing the necessary information. Some static routes are automatically created by the NCPE tool at installation, but others have to be created by the installer/craft. Generally a route is needed if the IP address of the destination is not in one of the local subnets.

Attention: Add a route on the NCPE tool in order to route traffic from the UC IP to the external application IP

(It is assumed that the global default router is in the Signaling subnet)

– DNS

  - If the DNS is on the customer OAM&P network, the static route should employ the admin gateway as the destination.

- If the DNS is on the customer signaling network, there is no need for a static route as the DNS traffic can route via the default router (without a static route applied).

– NTP

- If the NTP server is on the customer OAM&P network, the static route should employ the admin gateway as the destination.
- If the NTP server is on the customer signaling network, there is no need for a static route as the NTP traffic can route via the default router (without a static route applied).

– Billing server (unless there is a default billing gateway - in this case, the default route of the Billing subnet will be used)

– Partner x-channel (unless there is a default x-channel gateway - in this case the NCPE creates the static route automatically)

– SNMP Trap destination. In the Installation (and update modes) the NCPE tool will automatically generate a static route when a SNMP server IP address is added to the SNMP Servers table, but only if a default admin gateway is defined.

– Backup server (unless there is a default admin gateway - in this case the default route of the Admin subnet will be used)

– Trace Manager (unless there is a default admin gateway - in this case the default route of the Admin subnet will be used)

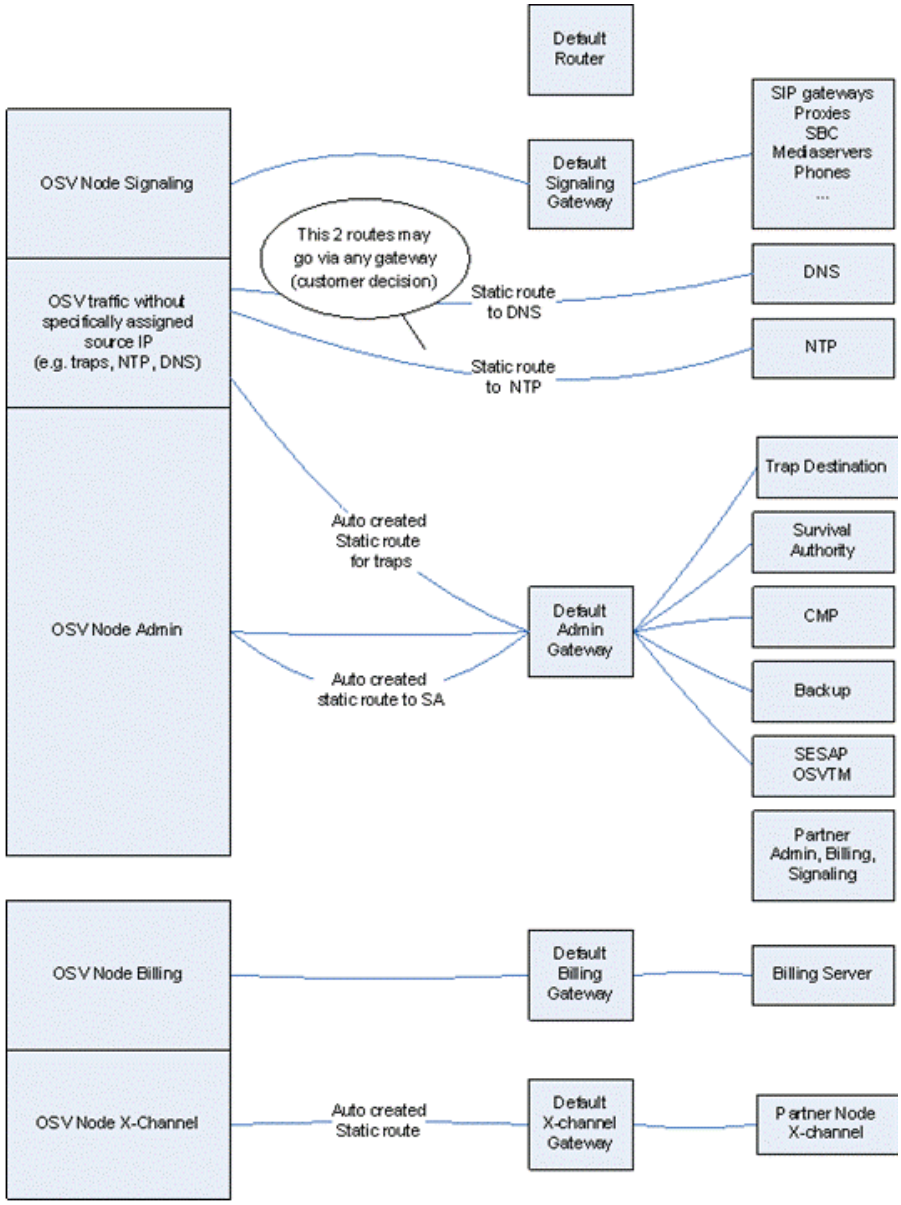
– Super User (CMP) (unless there is a default admin gateway - in this case NCPE creates the static route automatically)

– Survival Authority (unless there is a default admin gateway - in this case the NCPE creates the static route automatically)

Note: Partner billing node (previously employed during a Split Mode Upgrade) and partner admin are no longer required because all node to node communication is now via the x-channel.

The following diagram represents possible static routes for an OpenScape Voice server. The following assumptions are made for this system;

- The Admin, Signaling, Billing, and x-channel subnets have default gateways assigned
- The global default router is in the Signaling subnet



It is therefore highly recommended to specify default gateways via NCPE, when preparing the node.cfg for the new release.

Notes:

- There is no source based routing for the OSV x-channel subnet. But an x-channel default gateway is still required if the x-channel subnets of the two nodes are different. It is used by the OSV to automatically create a static route to the partner node x-channel IP address.

- Even with source based routing, static routes are still required for OSV trap destinations, NTP and DNS (the reason is that OSV software does not control the source IP of packets sent to these devices).
- OSV automatically replicates each static route to the source based routing table of the subnet that the router belongs to. For example, if the admin network is 1.2.3.0 to 1.2.3.255 and if a static route to IP 4.4.4.4 is specified via router 1.2.3.1, there will be two static routes, one in the admin source based routing table and one in the global routing table. So even if the OSV sends out a packet to 4.4.4.4 with source IP 2.2.2.2, it will still go via 1.2.3.1.

Note: If you arrived here from Section 2.6, “Creating a Node.cfg File”, on page 50, this link will take you back.

2.5 Flexible Ethernet circuit and IP Address Configuration

2.5.1 Overview

This feature allows for a flexible configuration of Ethernet circuits and IP addresses.

In the extreme configuration case, an OSC Voice Server can now be installed with one used Ethernet circuit (pair in case of redundancy) and one single IP address, not counting the IP address of the maintenance controller (IMM, iRMC).

The remote maintenance controller IP address has to be different than any other OSV IP (because the remote maintenance controller is on a separate Ethernet port).

The OSV feature of flexible Ethernet circuits and IP addresses applies only to new installations. Outage Free toolkit upgrade and toolkit migration will not support the reduction or combination of IP addresses or Ethernet circuits of existing installations. However, after systems are successfully upgraded, the feature can be introduced using the IFgui Update feature. Refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”.

2.5.2 Merging of IP subnets to common Ethernet ports

Some or all of the 4 OSV IP subnets can be merged. Each subnet is assigned to ports as defined in Chapter 3, of this document, (in the "Connecting the Cables" section of each platform). Chapter 3 port assignments are based on the "default" configuration (which is described below). The following combinations are supported:

For Duplex:

- All 4 subnets different (this is the default configuration): Either all 8 Ethernet ports are used or all 4 Ethernet port pairs are used.
- Mgmt and Billing shared - Signaling and Cluster separate: Billing Ethernet ports are not used.
- Mgmt, Billing and Signaling shared - Cluster separate: Billing and Signaling ports are not used.
- Mgmt, Billing, Signaling and Cluster (X-channel) shared: The Billing, Signaling and Cluster ports are not used.
- Mgmt and Cluster (X-channel) are shared - Signaling and Billing are separate: The Cluster ports are not used.
- Mgmt, Billing and Cluster (X-channel) are shared - Signaling separate: The Billing and Cluster ports are not used.

For Simplex:

- All 3 subnets different (the default): eth0, eth1, eth2 are used.
- Mgmt and Billing shared - Signaling separate: The Billing port is not used.
- Mgmt, Billing and Signaling shared: The Billing and Signaling ports are not used. Only Mgmt port is used.

In the case of a flat network (NoOfInterfaces = 1 where Mgmt, Billing and Signaling are shared (with or without a cluster configuration), the OSV routing defaults to the Default Router listed in the NCPE. There are no default static routes because there are no defined gateways for the Management, Signaling, and Billing subnets but this does not mean that the craft cannot create static routes.

For more details refer to Appendix 16, “Flexible Ethernet circuit and IP Address Configuration Examples”.

2.5.3 Sharing of IP addresses

In addition to combining subnets, OSV IP addresses can be shared too with the following restrictions:

- Shared IP addresses have to be on the same subnet.

  Examples given;

  - Mgmt shared with Billing: In this case, the Mgmt and Billing subnets may use the Mgmt subnet Node IP.
  - Mgmt, Billing and Signaling shared: In this case, the Mgmt, Billing and Signaling subnets can use the Mgmt subnet Node IP.
  - For Duplex systems, IF the Cluster (X-Channel) is shared with the Mgmt subnet, THEN the Cluster (X-Channel) IP is automatically the same as the Mgmt subnet Node IP.
  - In a co-located or L2-geo-separated cluster Signaling subnet (node.cfg parameter Node Separation = none), a virtual IP cannot be the same as a static IP. Reference Appendix 16.4, “Co-located Cluster Signaling Subnet” for an example of this static and virtual IP configuration. The reason is that a virtual IP moves to the partner node if the node is out of service while a static IP does not move.
  - On a network separated cluster Signaling subnet (node.cfg parameter Node Separation = separate), a virtual IP can be the same as a static IP. Reference Appendix 16, “Flexible Ethernet circuit and IP Address Configuration Examples” for an example of this static and virtual IP configuration.
- The remote maintenance controller IP address has to be different than any other OSV IP (because the remote maintenance controller is on a separate Ethernet port).
- The OSV can be configured with a local port for SIP signaling using UDP, TCP, TLS or MTLS. The default port for UDP and TCP is 5060, and for TLS or MTLS is 5061.
  - When the OpenScape Voice IP addresses for TLS and MTLS are the same, then port 5161 must be used for MTLS.
    - For Integrated Simplex deployments, the Media Server SIP endpoint shall be associated with the non-standard port numbers 5062 (SIP) and 5063 (SIP-TLS) for signaling between OSV and the Media Server.

      Change the Integrated Media Server SIP listening ports via CMP from

5060/5061 to 5062/5063. If you need to create a SIP endpoint for the MS, use ports 5062/5063 as well. Update the corresponding packet filter rules with the new port numbers.

Note: Combining/sharing subnets does not mean IP addresses have to be combined/shared; it is an option. Defaults for new installations will share IP addresses if the user chooses to combine/share subnets.

If the billing subnet is shared with the Mgmt subnet, the default billing IP address is the Mgmt IP address.

For more details refer to Appendix 16, “Flexible Ethernet circuit and IP Address Configuration Examples”.

Note: Follow this link to return to: Section 7.1.2, “Flexible Ethernet circuit and IP Address Configuration”, on page 421.

2.5.4 Default IPs for the 4 OSV Configuration Variants

Node	Same Subnets Node 1	Same Subnets Node 2	Separated subnets Node 1	Separated Subnets Node 2	Simplex	OSVE
Admin Subnet	1.2.3.0	1.2.3.0	1.2.3.0	1.2.4.0	1.2.3.0	1.2.3.0
XCh Subnet	10.1.3.0	10.1.3.0	1.2.3.16	1.2.4.16		
Billing Subnet	1.2.3.32	1.2.3.32	1.2.3.32	1.2.4.32	1.2.3.32	
Signaling Subnet	1.2.3.48	1.2.3.48	1.2.3.48	1.2.4.48	1.2.3.48	
Node	6	7	6	7	6	6
LSM	14	14 (if node 1 down)	14	14	14	14
IMM/iRMC	10	11	10	11	10	10 not for X3250M2
X-Channel	10.1.3.1	10.1.3.2	22	23		
Billing	38	39	38	39	38	6
Signaling (static)	52	53	54	55	54	12
SIP	54, 55 if node 2 down	55, 54 if node 1 down	54	55	54 and 55	12
MTLS	56, 57 if node 2 down	57, 56 if node 1 down	56	57	56 and 57	8
MGCP	58, 59 if node 2 down	59, 58 if node 1 down	58	59	58 and 59	12
CSTA	60, 61 if node 2 down	61, 60 if node 1 down	60	61	60 and 61	12

2.5.5 Default IPs for the 4 OSV configuration variants - Case Merged Admin, Billing and Signaling Subnet

Node	Same Subnets Node 1	Same Subnets Node 2	Separated subnets Node 1	Separated Subnets Node 2	Simplex	OSVE
Admin Subnet	1.2.3.0	1.2.3.0	1.2.3.0	1.2.4.0	1.2.3.0	1.2.3.0
XCh Subnet	10.1.3.0	10.1.3.0	1.2.3.16	1.2.4.16		
Node	6	7	6	7	6	6
LSM	14	14 (if node 1 down)	14	14	14	14
IMM/iRMC	10	11	10	11	10	10 not for X3250M2
X-Channel	10.1.3.1	10.1.3.2	22	23		
Billing	6	7	6	7	6	6
Signaling (static)	6	7	12	13	12	12
SIP	12, 13 if node 2 down	13, 12 if node 1 down	12	13	12 and 13	12
MTLS	8, 9 if node 2 down	9, 8 if node 1 down	8	9	8 and 9	8
MGCP	12, 13 if node 2 down	13, 12 if node 1 down	12	13	12 and 13	12
CSTA	12, 13 if node 2 down	13, 12 if node 1 down	12	13	12 and 13	12

2.5.6 Example of a 1 IP subnet configuration with a minimized set of IP addresses

Node	Same Subnets Node 1	Same Subnets Node 2	Separated subnets Node 1	Separated Subnets Node 2	Simplex	OSVE
Admin Subnet	1.2.3.0	1.2.3.0	1.2.3.0	1.2.4.0	1.2.3.0	1.2.3.0
Node	6	7	6	7	6	6
LSM	12	12 (if node 1 down)	6	7	6	6
IMM/iRMC	10	11	10	11	10	10 not for X3250M2
X-Channel	6	7	6	7		
Billing	6	7	6	7	6	6
Signaling (static)	6	7	6	7	6	6
SIP	12, 13 if node 2 down	13, 12 if node 1 down	6	7	6	6
MTLS need to use non-standard port number	12, 13 if node 2 down	13, 12 if node 1 down	6	7	6	6
MGCP	12, 13 if node 2 down	13, 12 if node 1 down	6	7	6	6
CSTA	12, 13 if node 2 down	13, 12 if node 1 down	6	7	6	6

2.6 Creating a Node.cfg File

Note: Because the network design and IP address allocations should already be known, it is strongly recommended that you prepare the node.cfg file prior to arriving at the customer's installation site to perform the physical hardware and software installation tasks.

Refer to the *OpenScape Voice, Network Planning Guide* for information on subnetting scheme network assignments and for the recommended cluster addressing scheme.

Note: Source-Based IP Routing is implemented. If 'route operations' message windows are presented during the Node.cfg creation, the "OK" button should be selected. For more information regarding the Source-Based IP Routing feature as it applies to installations, refer to Section 2.4, "Source Based Routes".

The Flexible Ethernet circuit and IP Address Configuration feature is introduced. This feature allows for a flexible configuration of Ethernet circuits and IP addresses. For more details refer to Appendix 16, "Flexible Ethernet circuit and IP Address Configuration Examples".

You create the node.cfg file by editing a node.cfg file template using the Installation Wizard. The Installation Wizard helps to eliminate errors in the node.cfg file that can result in problematic or failed installations.

Attention: Ensure that you enter only IPs in the respective fields of NCPE upon fresh installation and not FQDNs, as FQDNs are not officially supported by OpenScape Voice IDS service.

The OSV configuration parameters which end up in the OSV IDS configuration file (/etc/rules/osv.rules) are modified by startCli menu, and in particular are under the Denial of Service Management sub-menu, where user can modify trusted hosts configuration and service rate limits.

This sub-menu is retrievable from startCli by choosing 6 > 1 > 1 > 6 > 2 options.

The modifications from the user end up to the `/etc/rules/osv.rules`

```
Denial of Service Management:
Denial of Service Config Mgmt.................1
Denial of Service Trusted Hosts Mgmt..........2
Denial of Service Rate Limiting Mgmt..........3
```

The below parameter values should be defined as **IPs** and not FQDNs, as FQDN definition is not supported by OSV IDS service.

Forbidden from being FQDNs startCli fields
$cluster_partner_alias
$cluster_node_alias

Table 2 startCli fields that must be forbidden from being FQDNs

Forbidden from being FQDNs startCli fields
$sip_alias_1
$sip_alias_2
$sip_alias_3
$sip_alias_4
$ncs_alias_1
$ncs_alias_2
$csta_alias_1
$csta_alias_2
$bond_node_alias
$bond_bms_alias
$bond_udp_alias
$bond_partner_alias
$bond_partner_bms
$bond_partner_udp
$ntp_server_1
$lsm_alias_1
$lsm_alias_2
$dns_server_1
$link_local_v6_1
$link_local_v6_2
$link_local_v6_3
$link_local_v6_4
$link_remote_v6_1
$link_remote_v6_2
$link_remote_v6_3
$link_remote_v6_4
$sis_server

Table 2 startCli fields that must be forbidden from being FQDNs

See also in Appendix 13.2.1, “EZIP Method Using the CMP” and Appendix 13.2.2, “EZIP Method Using the NCPE Tool in Update Mode” for CMP and NCPE fields respectively, that must be forbidden from being FQDNs.

The Installation Wizard consists of several components: an Installation Framework (IF), Node Configuration Parameters Editor (NCPE), hardware definition files, IP address definition files, and other data definition files. The Installation Wizard automatically populates fields in the NCPE (and the node.cfg file) based on your selection in the Installation Framework screen and selections in subsequent NCPE screens.

The NCPE provides two modes: Wizard and Expert. The Installation Framework component launches the NCPE in Wizard Mode after you select whether you are doing an Install or an Update. A button at the bottom right corner of the NCPE screens allows you to switch to Expert Mode.

Attention: Use WinZIP to extract the ncpe zip file, as other tools will not work.

Attention: In the Expert mode of the NCPE, page IP Configuration (1/5); Updating the Management subnets or netmasks will impact the Signaling, Billing, Cluster, and Remote Administration IP settings. If the Management subnet or netmask IP addresses are changed please review/verify the Signaling, Billing, Cluster, and Remote Administration settings before proceeding to another page of the NCPE.

Attention: Input to the IP Configuration and IP Security sections of the node.cfg will create packet filter rules that secure access to the OpenScape Voice server.

Create the node.cfg file:

Attention: The following procedure is for an initial installation of OpenScape Voice V11. If you are upgrading to V11, refer to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11” for upgrade information and procedures.

If you were directed to this section by a Upgrade or Migration procedure, execute the steps as indicated in that procedure instruction. When the last step is complete, a doclink back to your Upgrade/Migration procedure will be provided.

2.6.1 Download the "OpenScape Voice Installation Wizard"

Download (from SWS) the latest "OpenScape Voice Installation Wizard" zip file that corresponds to the OSV software version you are installing.

Note: If necessary, refer to the OpenScape Voice base software release note on G-DMS for the link to SWS to download the Installation Wizard zip file.

Recommended practices for file transfer and burning of CD/DVD media;
1. If a checksum, md5sum or sha file is delivered with OpenScape software it is

a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. **If necessary, third party software can be used to calculate these values.**
2. When burning a file to a CD/DVD media use a lower burning speed (i.e.; 4x).
3. Use the 'verify' option of the burning application to ensure data integrity after the DVD burning is complete.

Unzip the downloaded file. Now there should be a parent directory named 'ncpe-OfflineWizard-<version_number>'. Change to the bin path located one level below 'ncpe-OfflineWizard-<version_number>'.

For Windows systems; open (double click) the file named ifgui.cmd.

For Linux systems; open the file named ifgui.

Note: For Linux users, if needed, export the DISPLAY of the output to your PC by entering "export DISPLAY=<IP address>:0", where the IP address of the destination of the DISPLAY is to be sent is used. This step is done as the root user.

The Installation Framework options screen appears.

On the **Installation Framework** options screen, select **Install** and click **Next**.

The Node Configuration Parameters Editor (NCPE) opens in Wizard Mode and displays the **Section 1: Configuration and Hardware (1/1) screen**.

Note: X-channel and CIGroup references apply to virtual duplex deployments.

2.6.2 Section 1: Configuration and Hardware (1/1) screen

On the Section 1: Configuration and Hardware (1/1) screen, select the values for the following fields.

2.6.2.1 Hardware Platform

Select the appropriate HW platform.

2.6.2.2 Configuration

Select **Integrated Simplex, Standard Duplex** or **Standard Duplex Large,** as appropriate. If you select Integrated Simplex, **Node Separation, Survival Authority, Preferred Node to Takeover and Stand Alone Service Enabled and X-Channel compression,** parameters are removed. An **OpenScape Enterprise Express** option is also presented also (this option will be read only - not selectable).

Note: For more information see chapter "OpenScape Voice Deployment Models" in *OpenScape Voice Administrator Documentation*.

2.6.2.3 Node Separation

This field appears only if you selected the duplex option.

Select the option **none** for co-located duplex systems or for duplex systems where the nodes are geographically separated but still on the same IP subnets (L2 geographically-separated systems).

Select the **separate** option for duplex systems where the nodes are geographically separated and require different subnet schemes for the management, signaling, and billing networks of each node (L3 geographically-separated systems).

If you selected **none** for the Node Separation parameter, the NCPE automatically creates static routes for Survival Authority, SNMP server and Super User IP addresses that are outside the Management subnet address range.

If you selected **separate** for the Node Separation parameter, the NCPE automatically creates static routes for Survival Authority, SNMP server and Super User in addition to static routes for each node like admin, x-channel and RSA. To review the static routes switch to Expert Mode and click the IP Configuration (4/5) tab for the IPV4 routes. The IP Configuration (5/5) tab contains the IPV6 static routes. Section 2.3, “Guidelines for Geographically Separated Nodes”, on page 37 can be used as a reference.

Even with source based routing, there is a need for static routes because not all OSV Software specifies a source IP to an outgoing packet to give source based routing the necessary information. Some static routes are automatically created by the NCPE tool at installation, but others have to be created by the installer/craft. Generally a route is needed if the IP address of the destination is not in one of the local subnets. For more details refer to Section 2.4, “Source Based Routes”, on page 41.

To add **static routes**, switch to Expert Mode and select the IP Configuration (4/5) tab and add the static routes in the according field. **NO duplicate routes should exist**. Duplicate routes will result in Image installation failures.

The following info would be required to add this static route:

- The destination server IP address
- The destination IP address netmask (typically 255.255.255.255)
- For the subnet gateway IP address, refer to the IP Configuration (1/5) tab.

Note: Instead of typing the gateway IP address, you can type in nafo0, nafo1, or nafo2. The NCPE will automatically select the default gateway for the respective subnet (mgmt, signaling, billing).

- For the SNMP server example the Administration subnet gateway IP address would be employed.
- For the Billing server example the Billing subnet gateway IP address would be employed.
- The Nafo ID is automatically populated based on the subnet gateway.

Note: Instead of typing the gateway IP address, you can type in nafo0, nafo1, or nafo2. The NCPE will automatically select the default gateway for the respective subnet (mgmt, signaling, billing).

In a Virtual or non-Virtual environment, the Stand Alone Service feature is enabled by default when the node.cfg parameter Node Separation = separate is selected. More info on the Stand Alone Service feature follows in step Section 2.6.2.9, “Stand Alone Service Enabled”, on page 57.

Note: When the separate option is selected, virtual IP migration is not possible.

To return to the Wizard Mode, select from the menu bar **File**, then **Wizard**. There is also a **Wizard** icon in the Expert mode tool bar that will switch you back to the Wizard Mode.

2.6.2.4 Software Build ID

Select appropriate software build for your installation.

2.6.2.5 Survival Authority

This field appears only if you selected the duplex option. Enter the Survival Authority IP address. Reference Chapter 6, “Survival Authority and IPMI Shutdown Agents” for further details of the shutdown agents operation.

2.6.2.6 Preferred Node to Takeover

This parameter indicates which node reacts first to an x-channel failure.

The value defaults to node 2. If the x-channel fails, node 2 will be the first to call the shutdown agents in order to "kill" node 1. Reference Chapter 6, “Survival Authority and IPMI Shutdown Agents” for further details of the shutdown agents operation.

2.6.2.7 Timezone

Select the appropriate time zone from the drop-down list.

2.6.2.8 Keyboard

Select the appropriate keyboard language from the drop-down list.

2.6.2.9 Stand Alone Service Enabled

The Standalone Service option is available for duplex configurations. If it is enabled, a node that does not receive permission to take over from the Survival Authority stays active (in Standalone Secondary mode). For more information regarding the Standalone Service feature, refer to the *OpenScape Voice Vx, Feature Description* documentation, section "*Survival Authority*" (where *x is the software release version*). Information is also available in Chapter 6, “Survival Authority and IPMI Shutdown Agents” of this document.

This box is present only if you selected the duplex option. Stand Alone Service is enabled by default for all L3 geographically separated deployments (node.cfg parameter Node Separation = **separate** is selected in this case). Stand Alone Service is recommended to be enabled for L2 geographically separated deployments as well, where the nodes are in different geographic locations but still on the same IP subnet.

If this flag is disabled (not recommended) one node will perform a reboot immediately upon detection of a complete interconnection failure and will stop the reboot action at cross-connect-check step; waiting for the craft input or for the repair of the interconnection failure.

Stand Alone Service is recommended to be disabled for co-located duplex systems, so leave this box unchecked if you are configuring such a deployment.

Note: There is one exception for the case of Virtual geographically separated deployments with the two nodes belonging to the same IP subnets (indicated by node separation = none); the Stand Alone Service will not be enabled.

2.6.2.10 X-Channel Compression

This checkbox will turn on/off X-Channel Compression. The default configuration is X-Channel Compression on. By 'checking' the box X-Channel Compression is on. Removing the check configures X-Channel Compression off.

2.6.2.11 Cluster Timeout

The ‘Cluster Timeout’ parameter indicates how long the cluster cross channel (AKA x-channel and cluster interconnect) can be down before the Cluster Manager declares “Changed cross channel state to DOWN” and initiates shutdown agent activity to prevent a split brain condition. The default value is 15 seconds for all OpenScape voice deployments. If a node to node connection failure is less likely than a server failure (e.g.; in a co-located configuration), the timeout should be set to 10 seconds. If the likelihood of short term connection failures is higher, values of up to 15 seconds are recommended.

2.6.2.12 Cluster Name, Node 1 Name and Node 2 Name

Enter the Cluster Name, Node 1 Name and Node 2 Name (if applicable).

Attention: Do not make changes to the node names. Refer to the required upgrade or migration procedure for the specific node.cfg changes.

The convention in this guide for referring to the nodes is as follows:

- **Node1** refers to the node identified by the **Node 1 Name** parameter value.
- **Node2** refers to the node identified by the **Node 2 Name** parameter value in the node.cfg file.

Observe the following guidelines when naming the nodes:

- The node name should not contain the underscore (_) character (for example, node1_name). The Installation Wizard will reject a node name that contains an underscore character.

- Do not use the following as node names:
  Single characters (for example; a, b, c, 1, 2, 3), dots (...), pri, sec, dev, alias, bond, priv, prim, cluster, node0, node1, node2, clusternode1, clusternode2, or localhost.
- Use only lowercase alphabet and numeric characters (for example; pchprod1, pchprod2). Do not use any symbols. Node names cannot begin with a numeric character (for example; 1pchprod), but can use numeric characters inside or at the end of the name (for example; pch1prod or pchprod1).
- Node names should consist of at least four characters (more than six is recommended) and can include up to 20 characters.

2.6.2.13 Assistant, Cluster Name

The **Assistant** parameter is auto populated with the **Cluster Name**, **Node 1 Name** and **Node 2 Name** values.

Click **Next**. The NCPE displays the **Section 2: IP Configuration (1/4)** screen.

2.6.3 Section 2: IP Configuration (1/4) screen

On the **Section 2: IP Configuration (1/4)** screen, select the values for the following fields.

Note: The **Flexible Ethernet circuit and IP Address Configuration** feature allows for a flexible configuration of Ethernet circuits and IP addresses. For more details refer to Appendix 15, “Example data collection session with the OSV Tools”.

2.6.3.1 Share Cluster with Mgmt button

Select the associated box if the X-channel (Cluster Interconnect Group-CIGroup) is to share the same subnet (and Ethernet ports) as the Management Network.

This parameter was introduced with the Flexible Ethernet circuit and IP Address Configuration feature. For more details refer to Appendix 16, “Flexible Ethernet circuit and IP Address Configuration Examples”.

When this box is selected, the CIGroup parameters will be grayed out and the CIGroup is placed in the Management Network subnet address scheme. In this scenario the CIGroup (X-channel) ports are not used.

2.6.3.2 Subnet Sharing

This parameter will dictate the number of Ethernet ports used and the IP addressing schema for the subnets.

This parameter was introduced with the **Flexible Ethernet circuit and IP Address Configuration** feature. For more details refer to Appendix 16, “Flexible Ethernet circuit and IP Address Configuration Examples”.

- **Mgmt-Billing-Signaling-Separated:** Default configuration. All 8 Ethernet port pairs are used. Each subnet is assigned to ports as defined in Chapter 3 of this document (in the "Connecting the Cables" section of each platform).
- **Mgmt-Billing-Shared:** The Mgmt and Billing subnets are merged. The Billing ports are not used.
- **Mgmt-Billing-Signaling-Shared:** Mgmt, Billing and Signaling subnets are merged. Billing and Signaling ports are not used.

Note: IF 'Share Mgmt with X-channel' was selected THEN the CIGroup is merged with the Mgmt subnet also. In this scenario the CIGroup (X-channel) ports are not used.

2.6.3.3 Default Router Node 1

Enter IP address for the Default Router if required.

Note: If you selected **separate** for the **Node Separation** parameter in step 2 on page 54, there is a **Default Router Node 2** field. Ensure that the IP address for the second subnet in the **Default Router Node 2** field is correct.

2.6.3.4 Management, Signaling, Billing Networks, and CI Group

Type the IP addresses in the **Subnet** and **Netmask** fields for the **Management, Signaling Network, Billing Network** and **Cluster Interconnect Group** (CIGroup).

There is an option for the user to set the **Maximum Transmission Unit (MTU)** for each subnet interface. The feature is partially implemented and there are MTU sizes that should be avoided on a duplex interface. Please refer to OSV Release Notes for further instructions.

Note: If you selected **Separate** for the **Node Separation** parameter there are 2 additional fields (**Subnet Node 2** and **Netmask Node 2**) for each network. The IP addresses for the second subnet are indicated in these fields. For example, if the management interface on Node1 is on subnet 1.2.3.0, and the second subnet is 4, then Subnet Node 2 is 1.2.4.0.

Click **Next**. The NCPE displays the Section 2: IP Configuration screen (2/4).

2.6.4 Section 2: IP Configuration (2/4) screen

On the **Section 2: IP Configuration (2/4)** screen of the Wizard Mode, enter the values for the following fields:

2.6.4.1 Assistant Cluster Name

The name to be given to the cluster

2.6.4.2 Assistant/CMP

For the **Assistant/CMP** value enter the IP address of the SOAP Server Interface. This will trigger the installation scripts to add the IP address to the /etc/security/access.conf file. The **Assistant/CMP** parameter is intended for the IP address of an external (offboard) Applications server. It is recommended the CMP FQDN be included in the access.conf file access list. Refer to Section 4.5.2, “Verify Remote Access for srx Account in a Standard Duplex”, on page 339 for more details on this configuration.

No **Assistant/CMP** IP address is required for Simplex systems because the Applications server is integrated into the OpenScape Voice system.

2.6.4.3 DNS Configuration

Enter Timeout, Attempts, Name Server IP 1, 2 and 3, Domain Name, Search Domain 1 - 6 data as required.

Note: DNS server(s) configuration in **node.cfg** is mandatory and the specified DNS server(s) must be able to respond to DNS requests at all times; that is, during installation, upgrade and regular operation of the system.

2.6.4.4 NTP Configuration

Enter the NTP server FQDNs (or IP addresses) as required.

Note: To change the NTP server or DNS configuration after the system is placed into service, refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. Changing the NTP server or DNS configuration is done by using the Update option of the EZIP tool as described in Appendix 13. The changes to NTP and DNS parameters will not cause a system outage.
When opening the EZIP GUI in the Update option, the fields that are related to NTP and DNS have a green background color. The green colored background indicates that modification to these fields will not cause a system outage.

The EZIP tool updates all the files and packet filter rules that relate to the NTP and DNS parameters and IP addresses.

Click **Next**. The NCPE displays the **Section 2: IP Configuration (3/4) screen**.

2.6.5 Section 2: IP Configuration (3/4) screen

2.6.5.1 Source/Static Routes

Static routes are added here. There is no limit but they must be in a sequence. The first missing number will terminate processing.

2.6.5.2 Broadcast Routes

Broadcast routes are added here. There is no limit but they must be in a sequence. The first missing number will terminate processing.

Note: There are different tables for node 1 and node 2. The user must enter routes for each node to the corresponding table.

2.6.6 Section 3: IP Configuration (4/4) screen

2.6.6.1 Source/Static Routes IPv6

Static routes are added here. There is no limit but they must be in a sequence. The first missing number will terminate processing.

Note: There are different tables for node 1 and node 2. The user must enter routes for each node to the corresponding table.

2.6.7 Section 3: IP Security (1/2) screen

Enter IP Security parameters in **Section 3: IP Security (1/2)** of the Wizard Mode as required:

2.6.7.1 SNMP Servers

Enter the FDNs or IP addresses and ports for the OpenScape Voice Assistant and any other SNMP server(s). Click the appropriate icon below the table to enter more values or to remove values.

Attention: For Integrated system enter the local loopback IP address 127.0.0.1 and port 162 as an SNMP server.

2.6.7.2 License Servers

Enter the FQDNs or IP addresses for the License Servers. Click the appropriate icon below the table to enter more values or to remove values.

2.6.7.3 LicenseAgentPort

The default value for the License Agent Port should already be populated.

Click **Next.** The NCPE displays the **Section 3: IP Security (2/2)** screen.

2.6.8 Section 3: IP Security (2/2) screen

On the **Section 3: IP Security (2/2)** screen of the Wizard Mode, select the desired SSH Algorithms from the list.

Proceed to Section 2.6.9, “Finishing the Node.cfg” to finish and save the node.cfg file.

2.6.9 Finishing the Node.cfg

1. On the **Section 3: IP Security (2/2)** screen of the Wizard Mode, click the **Finish** button (located on the lower right side of the NCPE).
2. The NCPE opens a Node.cfg Preview window and displays the node.cfg file you just created for you to review.
3. After the node.cfg review is complete, click **OK**.

   The NCPE opens a Node.cfg Save dialog box.
4. In the Node.cfg Save dialog box, specify where to save the file and click **Save**.

   The NCPE displays a message box stating that the node.cfg was saved successfully.
5. In the message box indicating the node.cfg was saved successfully, click **OK** and when prompted, “`Do you want to exit?`,” click **Yes**.
6. After the Installation Framework screen appears, click **Finish**.

Note: If you have arrived at this step from Section 4.3.4.1, “Preparation of the node.cfg files using a Linux or Windows Environment”; copy the completed node.cfg file to safe location. Rename the node.cfg file as **node.cfg.primary**. If this is a duplex OSV, make another copy of the node.cfg named

node.cfg.secondary. Click here to return to step e on page 260, of Section 4.3.4.1, “Preparation of the node.cfg files using a Linux or Windows Environment”.

Note: For the "Low Cost Native Hardware to Virtual Integrated Simplex Migration"; copy the completed node.cfg file to safe location. Rename the node.cfg file as **node.cfg.primary**. This file will used during the OSV Image install on the virtual machine.

---

7. Copy the completed node.cfg file to the USB memory stick as **node.cfg.primary**, disconnect the stick from the USB port, and label it **node.cfg.primary**. For a redundant system, connect another memory stick, copy the node.cfg to the second memory stick as **node.cfg.secondary**, and label the stick **node.cfg.secondary**. Ensure the file was not saved with a name that has a .cfg extension (for example: node.cfg.primary.cfg). The file name should be without the second .cfg extension (in fact: node.cfg.primary)

Attention: If you are performing a "Low Cost to Standard Duplex Migration" and arrived at this section from Section 9.9, “Create the Node.cfg for the Target System (Source system = Low Cost)”, follow this link back to Section 9.2, “Create the Node.cfg for the Target System”.

Note: Patch sets can be loaded onto the memory sticks for automatic installation during the image installation. This can be done now or at any time before you begin the image installation. Refer to Section 2.7, “Including Patch Sets and License files on the USB Memory Stick(s)”, on page 66 for instructions.

---

8. For an integrated simplex only: Rename the response file that you created for the simplex system to **response.cfg.primary** and copy it to the USB stick.

Attention: Integrated systems response files are built automatically as part of the installation process. Response files no longer need to be generated for images and are not required on USB sticks. If a response file is found on the USB stick that file will take precedence over the file that is automatically generated via the Image installation.

---

9. On the OpenScape Voice Installation Checklist, initial step 5. After you arrive at the customer site and are ready to begin the physical installation tasks, proceed to step 6 of the OpenScape Voice Installation Checklist.

2.7 Including Patch Sets and License files on the USB Memory Stick(s)

2.7.1 Loading Patch Sets onto the USB Memory Sticks

Note: Recommended practices for file transfer and burning of CD/DVD media;
1. If a checksum, md5sum or sha file is delivered with OpenScape software it is a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. **If necessary, third party software can be used to calculate these values.**
2. When burning a file to a CD/DVD media use a lower burning speed (i.e.; 4x).
3. Use the 'verify' option of the burning application to ensure data integrity after the DVD burning is complete.

Patch sets and emergency patch sets may be loaded onto the USB memory stick for automatic installation during the image installation as follows:

Note: A Windows PC or Linux server can be used for performing this procedure.

---

1. Create a */patch* directory on the memory stick for node 1. This memory stick also contains the *node.cfg.primary* file.
2. Create an empty file, *dev.8kps*, under the /*patch* directory.
3. Put the patch sets and the emergency patch sets, including the SPA files, into the *patch* directory. Generally, **this means the needed tar files from the latest cumulative patch set and all the tar files of the latest cumulative emergency patch set.**

   For example, if the latest image is delivered with PS07.E02 and PS12.E05 is required as part of the image installation;

   – Download cumulative PS12 including the associated SPA file.

   – Download cumulative emergency PS12.E05 including the associated SPA file.

   – Place the downloaded patch sets and SPA files in the patch directory of the USB memory stick.

   Note: Including the SPA file in this step will trigger an md5sum check of the patch sets before they are installed. A patch set md5sum check failure will be reported to the console and the installation will abort.

   If cumulative patch sets are not available, tar files of the regular patch sets

can be placed in the patch directory as well as the related tar files of the emergency patch sets. The standard naming convention of the patch sets **must** be maintained. **Remember to include the patch set SPA files in order to trigger the md5sum check during the installation.**

4. For a duplex configuration, repeat this procedure to load the patch sets onto the memory stick for node 2. This memory stick also contains the *node.cfg.secondary* file.

2.7.2 Including the License file on the Installation USB

The voice server license files can be copied onto the installation USB for automatic installation during the image installation process. This requires the keyword **OpenScape_Voice** be used in the license file name.

For Integrated Simplex only, the UC server license files can be copied onto the installation USB for automatic installation during the image installation process. This requires the keyword **OpenScape** be used in the license file name.

Note: The following are examples for naming OpenScape Voice License files and UC license file:

00-0E-0C-E9-83-F8_**OpenScape_Voice**_Vx.lic (for OSV node 1)
00-0E-0C-E9-83-F8_**OpenScape_Voice**_Vx_STANDBY.lic (for OSV node 2)

ACP00_5CF3FCE8E0B8_**OpenScape_**Vx.lic (for UC in Simplex)

where Vx represents the release version (e.g., V10 for Release 10).

Attention: It is good practice to verify the OSV license locking_id before copying the license file to the USB. Refer to Appendix 20, “Advanced Locking ID Guidelines”, for instructions. If this is a duplex system, verify node 2 also.

1. Copy node 1's OSV license file to node 1's installation USB at the same level as the installation file node.cfg.primary.
2. For a duplex configuration, copy node 2's OSV license file to node 2's installation USB at the same level as the installation file node.cfg.secondary.

3. For an integrated simplex configuration, copy node 1's UC license file to node 2's to node 1's installation USB at the same level as the installation file node.cfg.primary.

Note:
Click this link to return to Section 4.2.2, “Installation”, on page 232.
Click this link to return to Section 4.3.4.2, “Saving the node.cfg, license and Patchsets to a Installation ISO Image”, on page 261.

2.8 Fix Subscriber with Global Numbering Plan (E164NANP)

There are some OSV systems that have subscribers with the Global Numbering Plan (E164NANP) assigned to their profiles. This configuration is not allowed for enterprise solutions and must be fixed in order to prevent other issues.

The purpose of the current procedure is:

1. to check if any OSV system in any version is affected by the wrong configuration
2. to repair the wrong configuration (available for any OSV versions)

Prerequisites

It can be applied in the following patch set levels:

- **PS10E13** or greater e-patch
- **PS21E02** or greater e-patch
- **PS23** or greater patch set

Customers with patch set level lower than the required, must upgrade to one of the required patch sets before starting executing the next steps. The required file is the `repairNANP.tar`

2.8.1 Step 1: Check procedure

Check whether there are subscribers with the default NP (E164NANP) assigned. All steps described below must be executed as user root:

1. Copy file `repairNANP.tar` to srx home directory

   `/unisphere/srx3000/srx`

2. Change directory to srx home directory:

   `cd/unisphere/srx3000/srx`

3. Extract file `repairNANP.tar`

   ```
   tar -xf repairNANP.tar
   ```

4. Change directory:

   ```
   cd repairNANP
   ```

5. Execute the fixNANP.sh script using the –check option

   ```
   ./fixNANP -check
   ```

2.8.1.1 Output 1

If there are no subscribers with the Global Numbering Plan assigned the output will be the following:

Checking if there are subscribers with E164NANP assigned to them...

More details will be logged in /log/
P_FIX_E164NANP_SUBS_ALL_05172013_154828.log

All subscribers have correct Numbering Plan.

In this case the system works properly and there is no need for further actions. You can proceed to step 5 of Step 2: Repair procedure.

2.8.1.2 Output 2

When there are subscribers with the Global Numbering Plan assigned, the script will inform about:

1. the Subscriber Directory Number
2. the name of the Business Group to which the subscriber belongs
3. the Numbering Plan that is assigned to this Business Group, if it can be determined

---

Checking if there are subscribers with E164NANP assigned to them...

More details will be logged in /log/
P_FIX_E164NANP_SUBS_ALL_05172013_154828.log

Error: There are subscribers with the Global Numbering Plan (E164NANP) assigned

*Subscriber: **433164115289** - BG Name: **IPC_EMEA_1_01 - NP** cannot be determined for BG*

*Subscriber: **302108189100** - BG Name: **BG_GVS_Common - NP** assigned to BG: **NP_GVS_Common***

There is at least one subscriber with the default NP assigned. Proceed to Step 2: Repair procedure

2.8.1.3 Output 3

There is a possibility, especially for systems that have been upgraded from a very old version of OSV, that the following condition may exist:

1. There are subscribers without HomeDn / OfficeCode
2. There are Business Groups without any valid Numbering Plan assigned

If any of these conditions exists, the script will provide information regarding these invalid configurations.

Checking if there are subscribers with E164NANP assigned to them...

More details will be logged in /log/ P_FIX_E164NANP_SUBS_ALL_05172013_154828.log

---

Error: There are subscribers without HomeDn / OfficeCode.

Please create the HomeDn / OfficeCodes for these subscribers before proceeding to any repair action.

Subscriber 302104980000 has no HomeDN

Error: There are Business Groups without any valid Numbering Plan assigned.

Please assign a valid Numbering Plan to these Business Groups before proceeding to any repair action.

Business Group: bg-inf-2 has no valid Numbering Plan assigned

- If there are subscriber(s) without HomeDn / OfficeCode then create the HomeDn / OfficeCodes for these subscribers and execute Step 1: Check procedure again.

- If there are Business Groups without any valid Numbering Plan assigned, then create, or assign, a valid Numbering Plan to these Business Groups and execute Step 1: Check procedure again.

2.8.2 Step 2: Repair procedure

Attention: This step should be executed only if the output of Step 1: Check procedure is equal to Output 2 or Output 3.

Attention: Before proceeding with the next steps, ensure that you have taken a database backup. The existence of the database backup is crucial, as it can be used to restore the database to a working state, in case unexpected issues arise from the next steps.

The purpose of this step is to repair the configuration for subscribers that have the default NP (E164NANP) assigned.

All steps described below must be executed as user root. In case of a cluster the following steps should be executed only once, at Node 1 or Node 2.

1. This process has to be executed with the system in state 3 3

   Bring system down to state 3 3 with the following command:

   ```
   /unisphere/srx3000/srx/startup/srxctrl 3 3
   ```

2. Execute the fixNANP.sh script using the `-repair` option

   ```
   ./fixNANP -repair
   ```

   1. *Important: Please be aware that you must have a backup of the database. Do you have a backup of the database [Y/N]:*

   – If a database backup has not been taken before the execution of the script then type **N**, take a database backup and execute **Step 2 2** again.

   – If a database backup has been taken prior to the execution of the scrip then type **Y**

   2. You will be prompted to enter a valid Numbering Plan for all Business Groups that have at least one Subscriber with the Global Numbering Plan (E164NANP) assigned. The script will print the Global Numbering Plan assigned to the Business Group as well as the list of all available Numbering Plans assigned to this Business Group.

      Please enter a valid Numbering Plan Name for BG: bg-inf-1 ID: 27

      Global Numbering Plan Name assigned to BG bg-inf-1 is:

NP_bg-inf-1

Available Numbering Plan Name(s) for BG bg-inf-1 are:

NP_bg-inf-1

NP_bg-inf-2

Selected Numbering Plan Name: <print the NP here>

If everything finishes successfully, the following message will appear on the screen:

Numbering Plan corrected for selected subscribers. Update completed successfully!

Please check routing for the Numbering Plan that you have specified, especially when you have assigned a Numbering Plan which you have created before you executed the script.

3. Bring the system up to state 4 4 with the following command:

   ```
   /unisphere/srx3000/srx/startup/srxctrl 4 4
   ```

4. Check routing for all the Numbering Plans that you have specified, especially if you have assigned a Numbering Plan that was created for the needs of this procedure.

5. Remove unnecessary files

   cd /unisphere/srx3000/srx

   rm -rf repairNANP

3 Installing the Hardware Platform

OpenScape Voice software has passed operability testing on the equipment described in Section 3.1, “Computing Node”.

If you are installing a OpenScape Voice redundant system in a geographically separated node configuration, note that the distance between the nodes is limited by a maximum round-trip delay between the nodes of 100 milliseconds. The theoretical maximum distance is 6,000 miles (10,000 kilometers), but the customer’s network must be able to keep the round-trip delay between the nodes to less than 100 milliseconds.

The **Flexible Ethernet circuit and IP Address Configuration** feature allows for a flexible configuration of Ethernet circuits and IP addresses. This feature has a direct impact on the Ethernet port configuration of and OpenScape Voice server. In the extreme configuration case, an OpenScape Voice Server can now be installed with one used Ethernet circuit (pair in case of redundancy) and one single IP address. For more details, refer to Appendix 16, “Flexible Ethernet circuit and IP Address Configuration Examples”.

The following node.cfg parameters will impact the Ethernet port and IP address configuration of the OpenScape Voice server.

a) Share Cluster (i.e., X-channel) with Mgmt check box: Select this check box if the X-channel (Cluster Interconnect Group- CIGroup) is to share the same subnet (and Ethernet ports) as the Management Network. When this box is selected the CIGroup parameters will be grayed out and the CIGroup is placed in the Management Network subnet address scheme; the default last octet of the CIGroup IPs are ‘4’ for node 1 and ‘5’ for node 2.

   - The CIGroup IPs are set to the same IP as the Node 1 (or 2) IP of the Management network.

b) Subnet Sharing: This parameter dictates the number of Ethernet ports used and the IP addressing schema for the Mgmt, Billing and Signaling subnets. The following is an overview of the Subnet Sharing choices available and how they impact the Ethernet port and IP address configuration of the OpenScape Voice server;

   - **Mgmt-Billing-Signaling-Separated:** Default configuration. Each subnet is assigned to ports as defined in Chapter 3 of this document (in the “Connecting the Cables” section of each platform).
   - **Mgmt-Billing-Shared:** The Mgmt and Billing subnets are merged - the Signaling and Cluster ports are separate. The Billing ports are not used.

- **Mgmt-Billing-Signaling-Shared:** Mgmt, Billing and Signaling subnets are merged - Cluster ports are separate. Billing and Signaling ports are not used.

Attention: When you select "Share Mgmt with X-channel", the CIGroup is also merged with the Mgmt subnet. In this scenario, the CIGroup (X-channel) ports are not used.

3.1 Computing Node

Historically the OpenScape Voice (OSV) system was installed on a variety of hardware servers. Many of these servers have reached end-of-sale and are no longer supported. Please refer to Table on page 417 for the currently supported hardware servers for new installation, Upgrade or Migration.

Note: In case of older / unsupported hardware, migration to a supported hardware or to a virtualized environment is needed.

3.1.1 Lenovo SR530 Server

The Lenovo SR530 server is deployed for two node OSV cluster (co-located and network separated) and integrated simplex.

Housed within a 19" rack-mountable enclosure, the Lenovo SR530 server is equipped for OpenScape Voice as follows:

- Processor: 2 x Intel® Xeon® Silver 4110 Processor 8-core @ 2.10GHz
- Memory: 32 GB (2x16) of Double Data Rate 4 (DDR4) memory
- Hard disk drive: Two 300GB 15K 12 Gbps SAS 2.5" HDD
- Disk controller: ThinkSystem RAID 530-8i PCIe 12Gb Adapter
- Ethernet interfaces
  - 2 on motherboard standard, 2 via the 2-port Intel X722 LOM. Supported link modes 1GbE/10GbE, but not 10Mb or 100Mb
  - 4-port Intel Ethernet Server Adapter I350-T4
- Remote supervision: One Integrated Management Module with optional Virtual Media Key (VMK)
- Universal Serial Bus (USB) ports: Four (two at the front, two at the back)

- Power Supply: 2 x 550 W

3.1.2 Lenovo SR630 V2 Server

The Lenovo SR630 V2 can be used as the computing node in both the redundant configurations and the simplex configuration. The SR 630 is housed in a rack-mountable enclosure.

Lenovo SR 630 Product Attributes

- Processor: One 2.40 GHz 16-Core Intel Xeon Silver 4314 CPU
- Memory: 32 GB. 1 x 32GB DDR4-3200 2666 MHz (1Rx4 1.2V) RDIMM memory
- Hard Disk Drives: 2 x 300GB, 2.5", 15K SAS 12Gb Hot Swap 512n HDD
  - Disk controller: RAID 5350-8i PCIe 12Gb Adapter
- Optical drive: None, support for an external USB DVD RW Optical Disk Drive
- Disk controller: Internal on-board RAID controller
- Ethernet interfaces (8 ports):
  - 2X BCM5719-4P - 4 x 1GbE PCIe NIC (10/100/1000BASE-T and 10/100/1000BASE-X support)
- Remote Supervision: One Intel Management Module with optional Virtual Media Key (VMK)
- Universal Serial Bus (USB) ports (6 ports):
  - Front: 1x USB 3.2 G1 (5 Gb/s) port, 1x USB 2.0 port (also for XCC local management), External diagnostics port, optional VGA port.
  - Rear: 3x USB 3.2 G1 (5 Gb/s) ports, 1x VGA video port, 1x RJ-45 1GbE systems management port for XCC remote management. Optional DB-9 COM serial port (installs in slot 3).
  - Internal: 1x USB 3.2 G1 connector for operating system or license key purposes

Power supply: 2 x 500W(230Vac/115Vac) AC Hot-Swap Power Supply

This server meets the Energy Star guideline for energy efficiency

3.1.3 OpenScape Voice Hardware - Lenovo SR630 V3 Server

The Lenovo SR630 V3 can be used as the computing node in both the redundant configurations and the simplex configuration. The SR 630 V3 is housed in a rack-mountable enclosure.

Lenovo SR 630V3 Product Attributes:

- Processor: One 2.40 GHz 12-Core INTEL(R) XEON(R) SILVER 4510
- "Memory: 32 GB. 1 x 32GB Samsung DDR5 4400 MHz DIMM_7memory
- "Hard Disk Drives: 2 x 300GB 15K 12Gbps SAS 2.5" HDD
  - oDisk controller: ThinkSystem RAID 5350-8i PCIe 12Gb Adapter
- "Optical drive: None, support for an external USB DVD RW Optical Disk Drive
- "Disk controller: Internal on-board RAID controller
- "Ethernet interfaces (8 ports):
  - Intel Ethernet Server Adapter I350-T4 & Intel I350 1GbE RJ45 4-port OCP Ethernet Adapter v2
- Remote Supervision: One Intel Management Module with optional Virtual Media Key (VMK)
- Universal Serial Bus (USB) ports: Six:
  - Front: 1x USB 3.2 G1 (5 Gb/s) port, 1x USB 2.0 port (also for XCC local management), External diagnostics port, optional VGA port.
  - Rear: 3x USB 3.2 G1 (5 Gb/s) ports, 1x VGA video port, 1x RJ-45 1GbE systems management port for XCC remote management. Optional DB-9 COM serial port (installs in slot 3). Optional second RJ-45 1GbE systems management port for XCC remote management (installed in OCP adapter slot).
  - oInternal: 1x USB 3.2 G1 connector for operating system or license key purposes.
- "Power supply: 2 x 750W (ACBE) AC Hot-Swap Power Supply.
- "This server meets the Energy Star guideline for energy Efficiency.

3.2 Ethernet Switch

An Ethernet switch, or switches, are required. The Ethernet switch requirements are as follows:

- For a single-node OpenScape Voice system: One VLAN capable switch with at least four ports on the OpenScape Voice side, gratuitous ARP support.
- For a redundant OpenScape Voice with co-located nodes: Two VLAN capable switches in duplex configuration with two high-speed links and at least seven ports on the OpenScape Voice side, gratuitous ARP support.
- For a redundant OpenScape Voice with geographically separated nodes: Two VLAN capable switches **for each node (i.e., total of 4)**.

The Ethernet switch provides 24 RJ-45 copper 100/1000 FastEthernet paths for system management, control, transfer of call detail record files, and database maintenance and mirroring. Two Gigabit copper ports and two fiber ports deliver two active uplinks for greater throughput and two redundant uplinks.

3.3 Installing the Lenovo SR630 V2 Server into the Rack

This section describes the equipment needed on the Lenovo SR630 V2. All necessary hardware comes pre installed. You can find the appropriate steps necessary to assemble the hardware, connect the cables and load the needed firmware so that OpenScape Voice can be loaded with the applicable OpenScape Voice software load.

3.3.1 KVM Notes

The following section applies more to older KVM / Software combinations and should not be relevant for newer hardware/software technologies. However, It remains listed in this document for completeness.

The interaction between the KVM switch and devices attached, is not very simple. When the KVM is not switched to a server/node, it must simulate the connection. If a different signature is generated on the simulation, the server/node will request clarification of the type of mouse in use. Some combinations of KVM switches and mouse are not 100% compatible. Failure to have a correctly working KVM/mouse combination may cause your server to hang during a reboot, waiting for operator input.

The following test is suggested to determine, whether problems can be expected. This test must be performed after an installation from scratch (unfortunately this test can't be performed before the installation):

1. Select the test machine with your KVM and login as root.
2. Run hwbootscan; it should produce no output.
3. Switch the KVM to another position.
4. Remotely login, as root, to the test machine.
5. Run hwbootscan; it should produce no output.

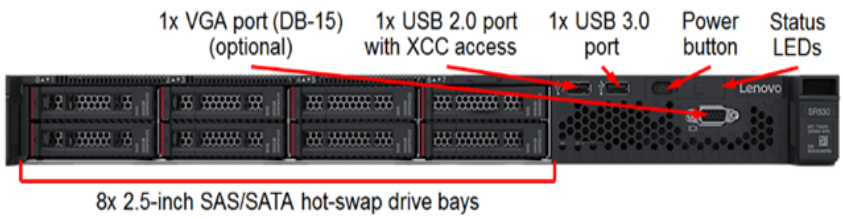
If you see a menu to select a mouse, you have a problem because your KVM does not simulate the mouse the same in both positions. You will either need to change the KVM/mouse combination or perform the following steps each time, the system is installed from scratch.

6. When prompted, select your mouse type, and ACCEPT.
7. Switch back to the test machine.
8. Run hwbootscan; it should produce no output.

Repeat this process on the other node.

3.3.2 Installing the Disk Drive

The image below shows the location of the two drives. The system comes with a total of 8 2.5-inch drive bays.

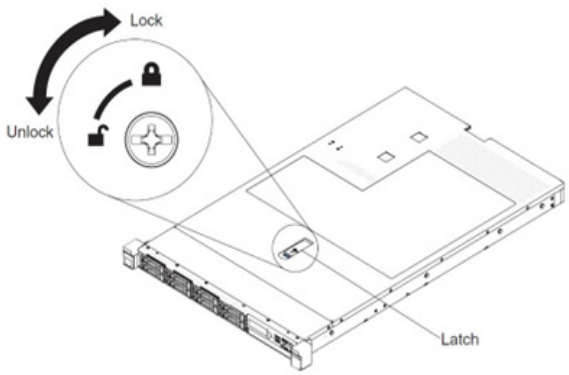


The image below is a close-up of the drives, with the two leftmost bays populated with hard disks.

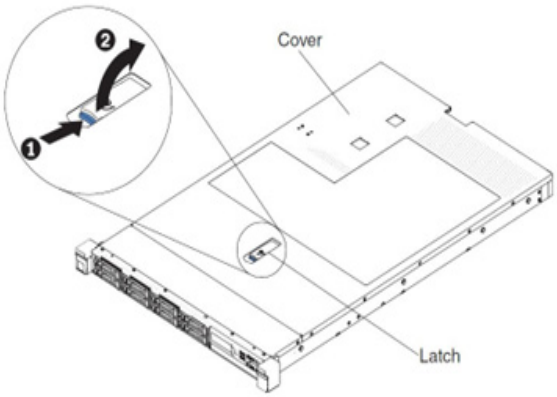
To remove a drive, slide the blue release latch to the right with one finger while using another finger to grasp the black drive handle and pull the hard disk drive out of the drive bay.

3.3.3 Removing the Top Cover

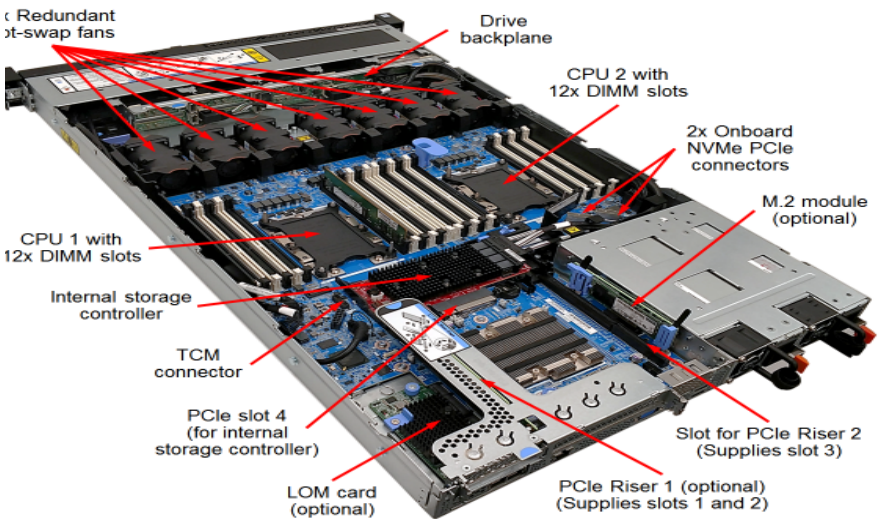
Always check whether the cover is locked. If it is locked, use a screwdriver to turn the cover lock to the open position.



Press in on the blue tab on the cover-release latch and lift the cover release latch up (the cover slides to the rear). Lift the server cover off the server and set it aside.



The image below shows the top view of the Lenovo SR630 V2 with its cover removed.



3.3.4 Installing Memory and CPU for the Lenovo SR630 V2

Memory and CPUs come pre installed. However, make sure that the memory is installed in the correct slots according to Lenovo for optimal heat dissipation. This can be done in multiple ways, the easiest being from the IMM interface (see Section 3.7.12, "Memory Verification via the IMM Interface for the Lenovo SR630 V2 server"). The physical method to verify the memory is the following:

Your server has 16 channels, 32 memory slots, and supports:

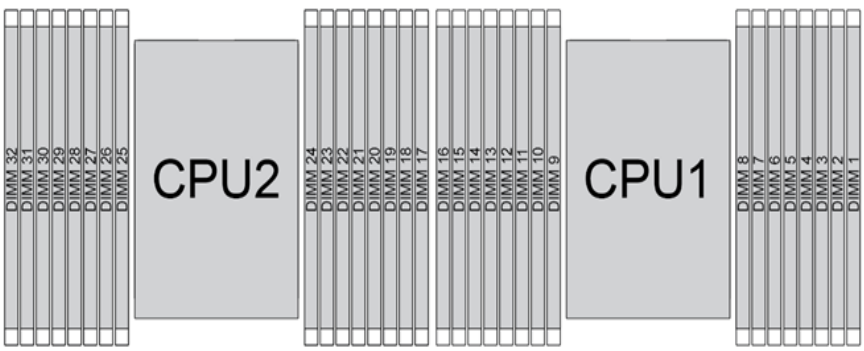
Minimum memory:

- 16 GB

Maximum memory:

- Without PMEMs:
  - 2 TB using 32 x 64 GB RDIMMs
  - 8 TB using 32 x 256 GB RDIMMs
- With PMEMs:
  - 10 TB: 16 x 128 GB 3DS RDIMMs + 16 x 512 GB PMEMs (Memory Mode)
  - Total 10 TB installed memory capacity, of which 8 TB (PMEMs) is used as system memory and 2 TB (3DS RDIMMs) is used as cache.
  - 12 TB: 16 x 256 GB 3DS RDIMMs + 16 x 512 GB PMEMs (App Direct Mode)
  - Total 12 TB installed memory capacity, of which 4 TB (3DS RDIMMs) is used as system memory and 8 TB (PMEMs) is used as persistent memory for storage.

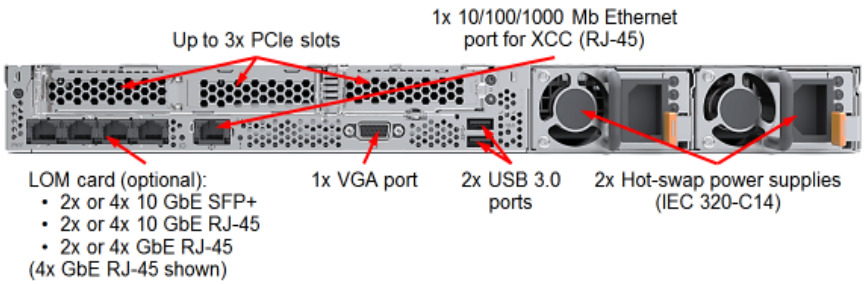
As shown below:



Note: The CPUs come pre installed, so no manual intervention/ installation is necessary.

3.3.5 Connection Panel in the rear of the Lenovo SR630 V2 server

The image below gives a general overview of the connection panel in the rear of the Lenovo SR630 V2 server.



3.3.6 Installing the PCI

The system comes pre installed with four onboard ports (two Integrated one GbE and 2x1/10/100 GbE LOM - LAN on Motherboard), and an Intel 4 port PCI Express card.

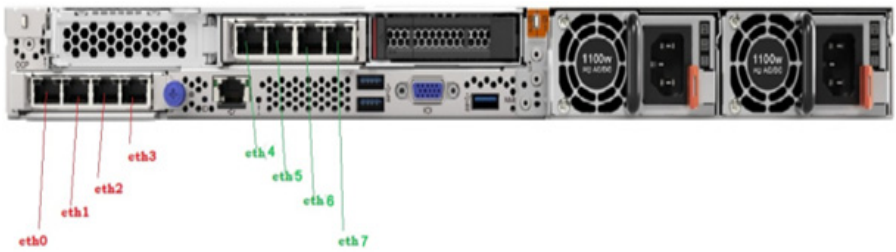
These are identified as follows:

PCI express card (Intel)	Integrated-LOM (Broadcom)
eth4 - eth7	eth0 - eth3

Table 3

Note: The four onboard ports provide only gigabit support.

Note: To avoid installation failure, the Intel PCIe card should be installed in PCIe slot as shown in the picture below.



3.3.7 Installing the Power Module

Dual power supplies come pre installed and are visible from the back of the machine, see Section 3.7.5, "Connection Panel in the rear of the Lenovo SR630 V2 server".

3.3.8 Wiring the Cluster

The following diagrams show the Ethernet port assignments for the Lenovo SR630 V2, for a duplex and a simplex setup.

Note: For a simplex setup, only ports eth0, eth1 and eth2 are used.

Ethernet	Number of ports	Duplex			Simplex			
Ethernet card	4 ports	4	5	6	7			
LOM	4 ports	0	1	2	3	0	1	2
		Bond 0 (admin)	Bond 1 (signaling)	Bond 2 (billing)	Bond 3 (X-channel)	admin	signaling	billing

Table 4 Ethernet Port Assignment

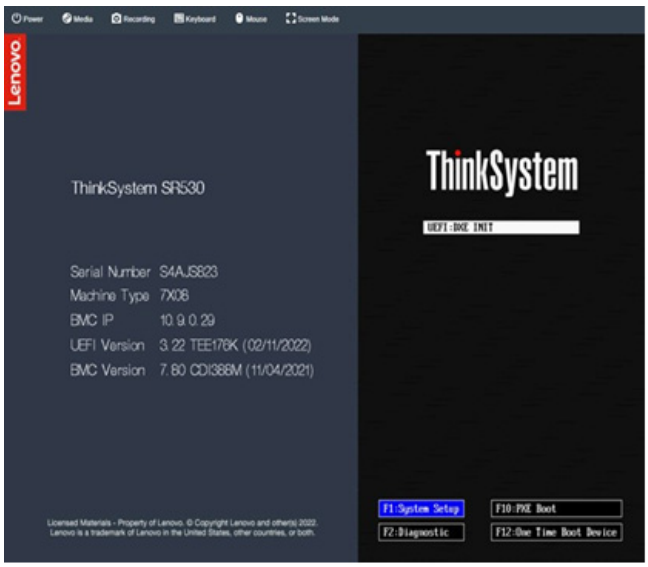
After adding and wiring all hardware to the machine, continue with the UEFI configuration, RAID creation and firmware updates. Connect the KVM devices to the server prior to initial boot.

Note: SR630 V2 requires a USB keyboard and mouse. Use a PS/2 to USB adaptor in most cases. See previous section on KVM issues for more details.

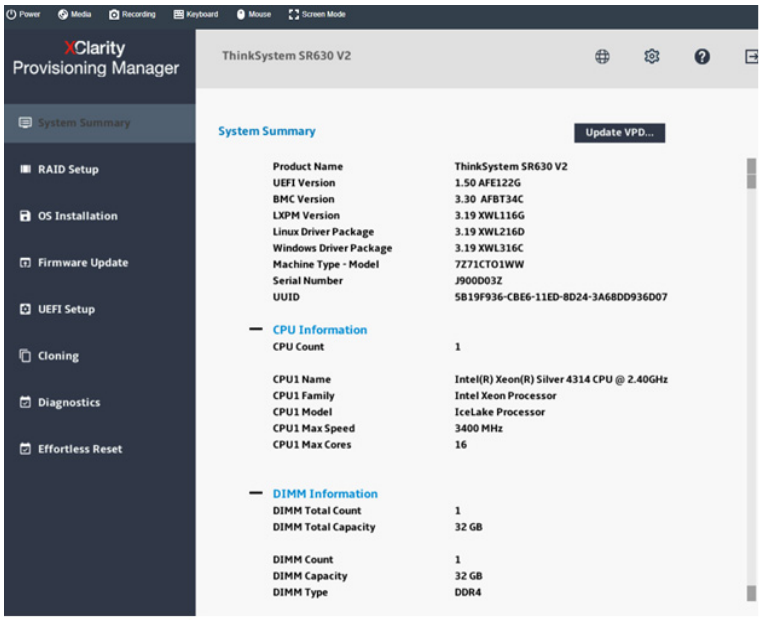
3.3.9 Setting up the UEFI for the Lenovo SR630 V2 server

Follow the instructions below to setup the UEFI.

1. Reboot the system to enter the Setup Utility. At the initial screen prompt of <F1> **System Setup**, press **F1** to enter “System Setup".

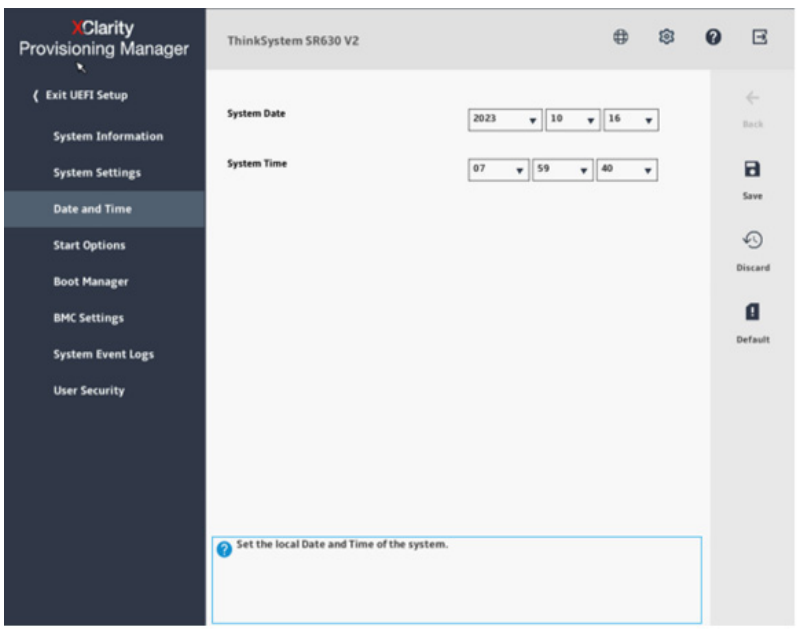


2. The System Configuration utility page opens:



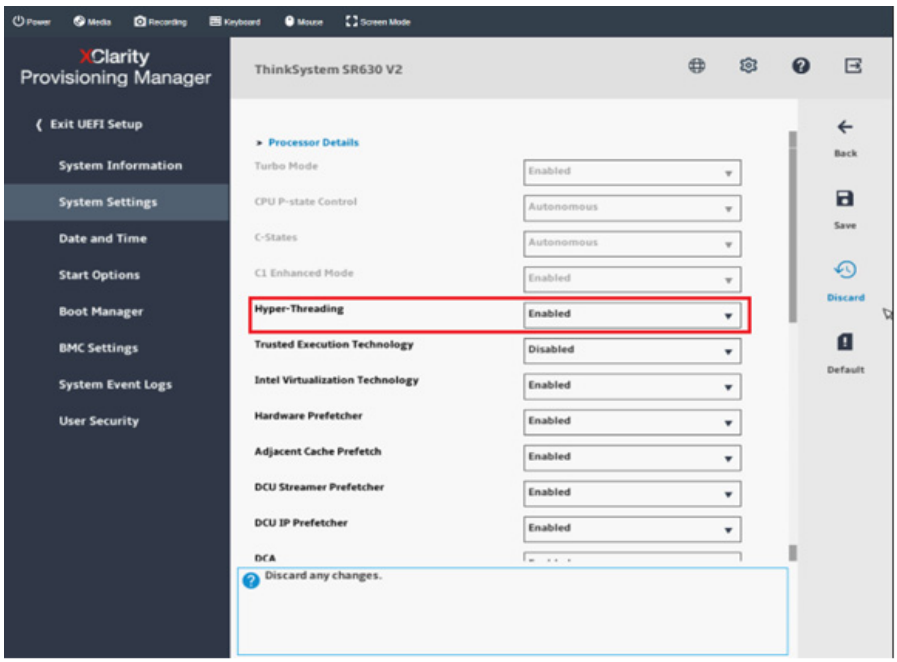
3. Under **UEFI Setup** select **Date and Time** to verify the System time and date. Configure the **System Date** and **System Time** parameters, click **Save** and return to the UEFI Setup menu.

Note: To display the System Configuration utility page, you can also click on the help icon at the top right of your screen and select Getting Started.



4. Navigate to **System Settings > Processors**.

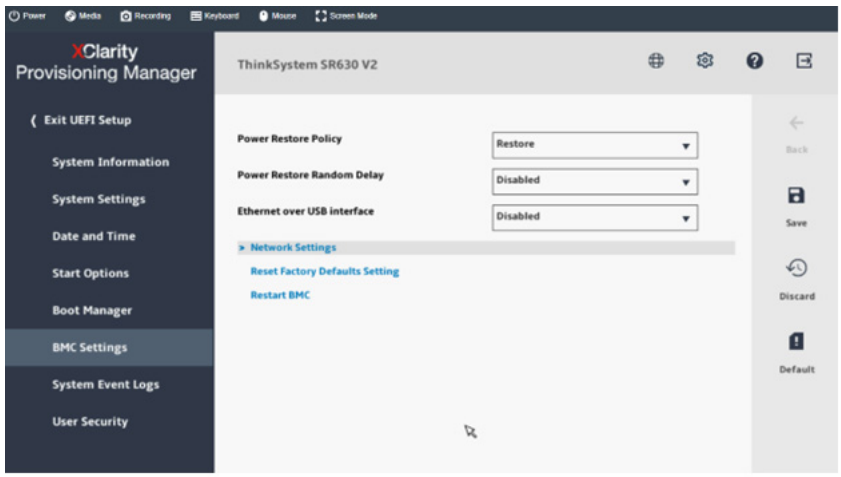
5. In the **Processor Details** page, configure the parameter **Hyper - Threading** with the value "Disable". Click **Save** and return to the **System Settings** menu.

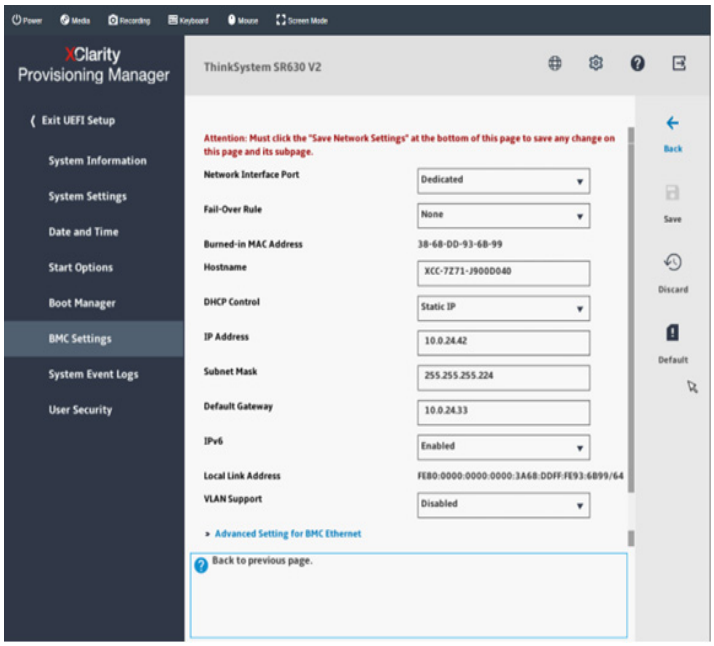


Note: After disabling the Hyper - Threading, perform a power-cycle before the system boots up again.

---

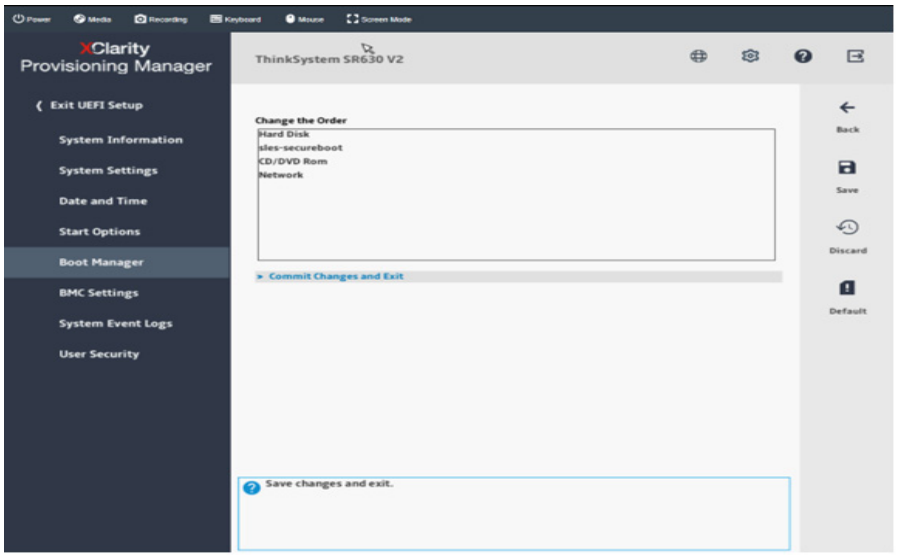
6. Select **BMC Settings** and navigate to **Network Settings** to change the network configuration for the IMM.





7. In the Network Configuration window, configure the following parameters:
   - DHCP Control: Static IP
   - IP Address: Value from for the given network
   - Subnet Mask: Value from for the given network
   - Default Gateway: Value from for the given network

8. Click Save Network Settings
9. Navigate back to the UEFI Setup menu and select Boot Manager



10. In the Boot Manager page, select Change the Order

11. Place the boot devices in the following order:

    – <USB Storage>

    – <Hard Disk>

Note: Reorder the selected devices with the use of -/+ keys in the Change the Order box, when needed.

---

12. Click Commit Changes and Exit

13. Return to the Boot Manager menu and select Boot Modes

14. For the bootable USB sticks to be identified as bootable devices, configure the following parameter:

    – System Boot Mode: Legacy Mode

15. Save your changes and return to the Boot Manager menu. The system is ready for RAID 1 setup.

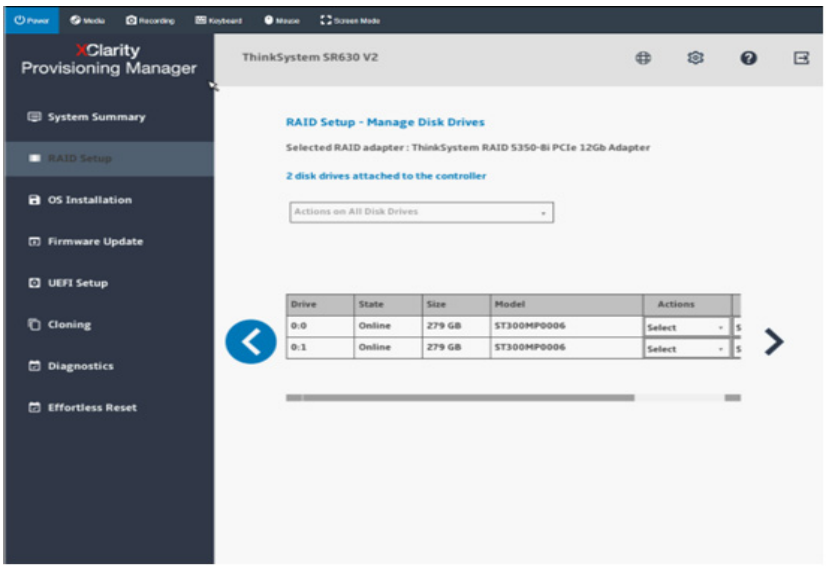
Note: You don't need to reset the IMM for Network changes to take effect.

3.3.10 Creating the LSI RAID for the Lenovo SR630 V2

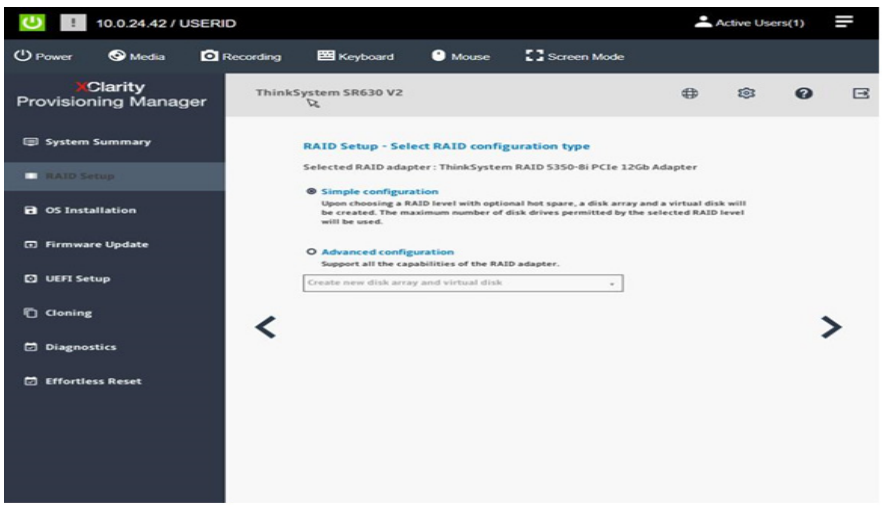
Follow the steps below to setup the internal LSI controller and disks into a mirrored pair (RAID1). The LSI RAID Creation is done via the UEFI RAID Setup.

1. In the main menu of the UEFI select **RAID Setup**.

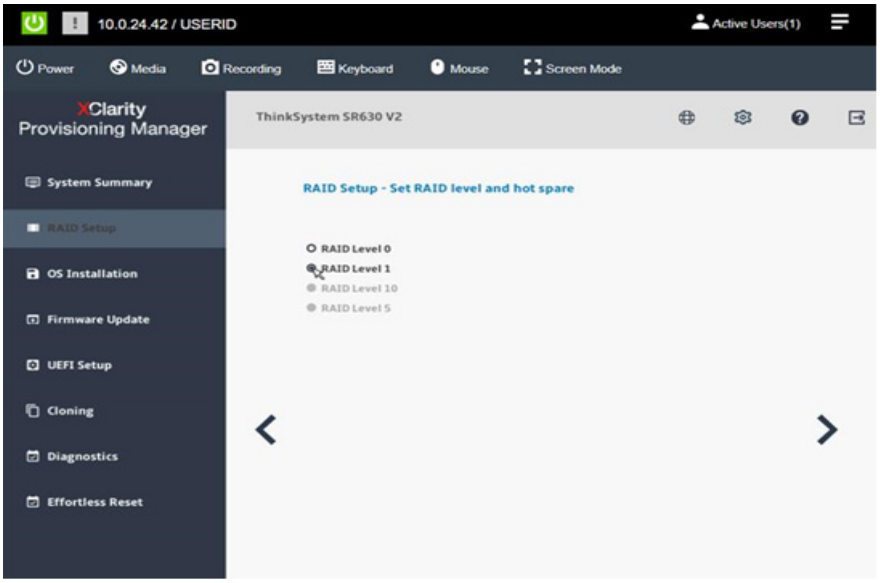
2. Navigate to **Manage Disk Drives**, select **Actions on All Disk Drives** and click **Next**



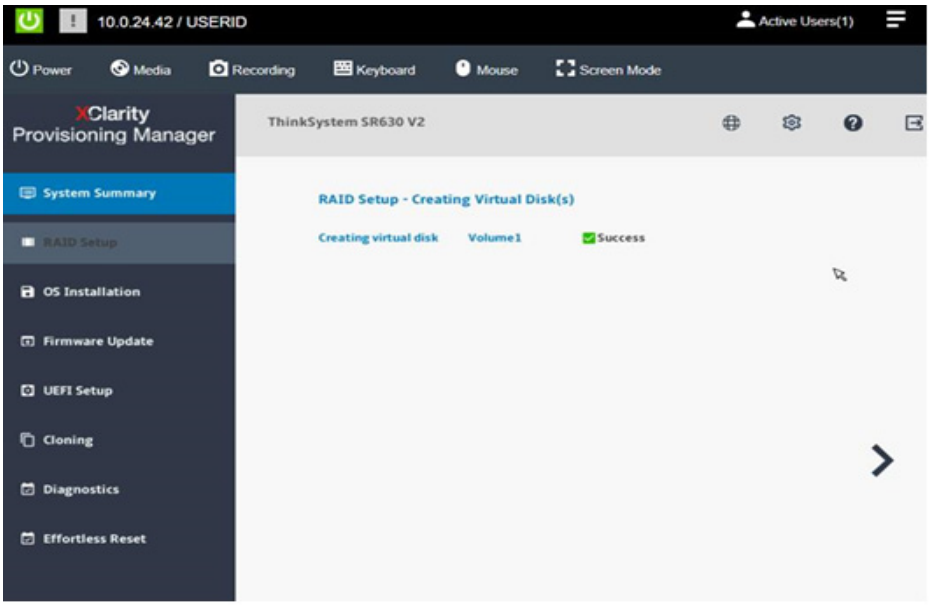
3. Select **Simple configuration** in the **Select RAID configuration type** page and click **Next**



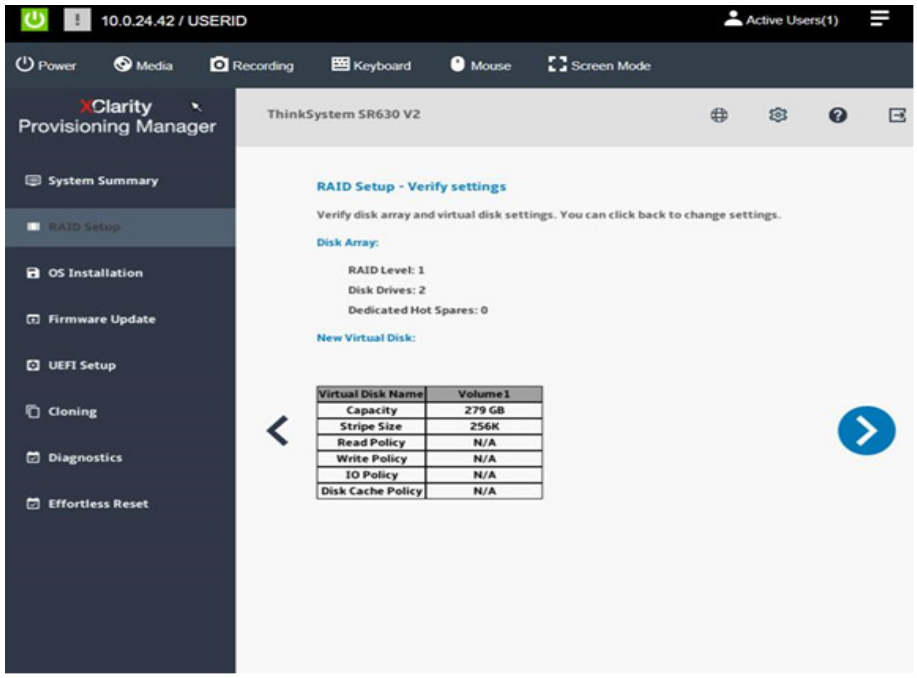
4. Select **RAID Level 1** in the **Set RAID level and hot spare** page and click **Next**.



5. Verify that **Virtual Disk** was created successfully and click **Next**.



6. In the **Verify Settings** page, check that everything is properly set.



The LSI configuration has been completed.

7. Return to the main menu, click **Exit** and then click **OK**.

Verify the IMM interface and then reboot the server. It is now ready for OSV software installation.

3.3.11 Activation of IPMI Over LAN for the Lenovo SR630 V2 server

The IPMI Over LAN capability needs to be activated, as it is required by the IPMI shut down agent. For the activation, you need to login to the IMM interface.

1. Open a Web browser.
2. In the address or URL field, type the IP address or hostname of the IMM server to which you want to connect. Use https for a secure connection.

This brings up the web page for the IMM.

Note: Click on **Supported Browsers** to see a list of web browser versions which are supported by the IMM firmware.

---

3. Provide your user id and password.

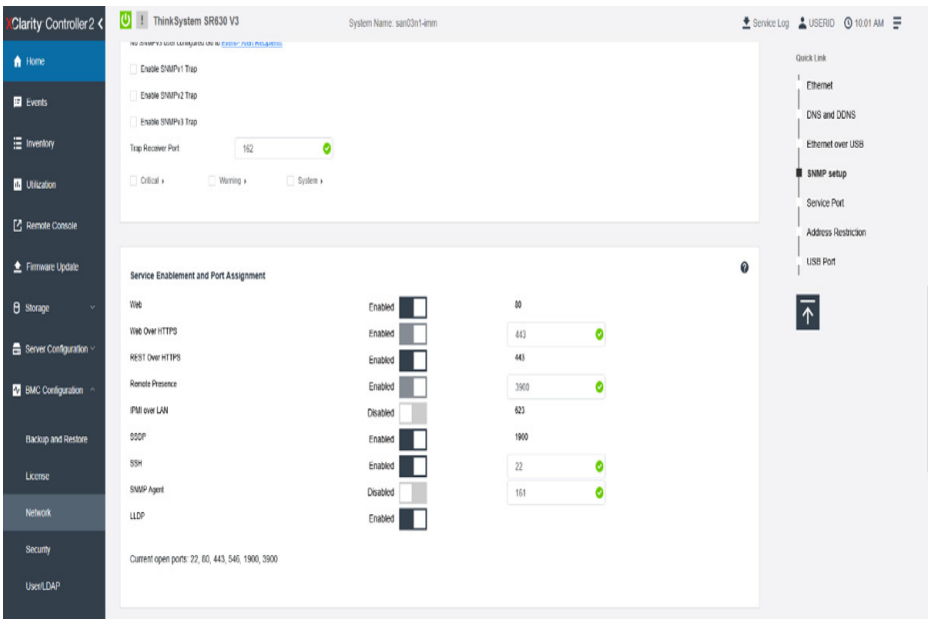
The default values are:

- User name: USERID
- Password: PASSW0RD

Note: The 0 in PASSW0RD is the digit 'zero'.

After the user id and password are entered, the main page appears.

4. Navigate to **BMC Configuration > Network** tab.
5. Enable the **IPMI over LAN** slider, if not already enabled.



3.3.12 Remote Console Startup for the Lenovo SR630 V2 server

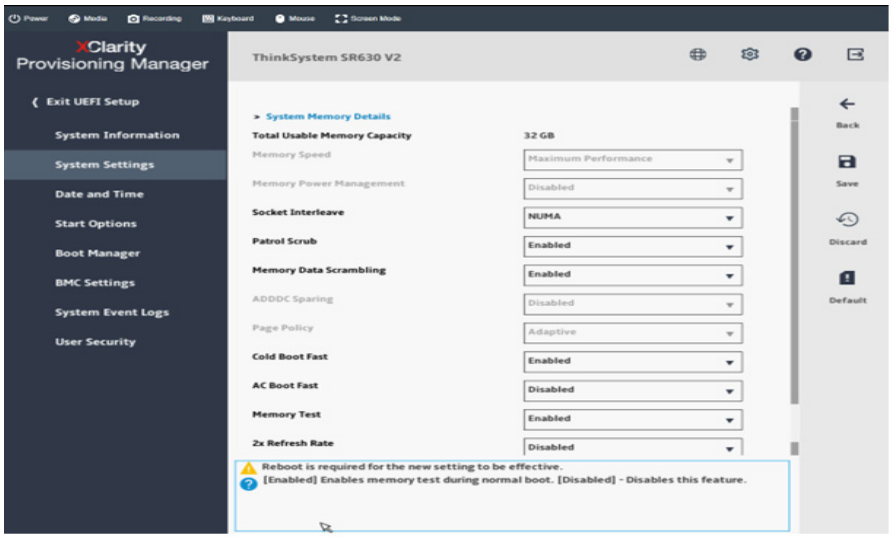
1. Log into the IMM interface of the server as described in the previous Section 3.3.11, “Activation of IPMI Over LAN for the Lenovo SR630 V2 server”.
2. In the **Remote Control Preview** field, click on **Launch Remote Control**.

A new tab opens, giving you full access to the server console.

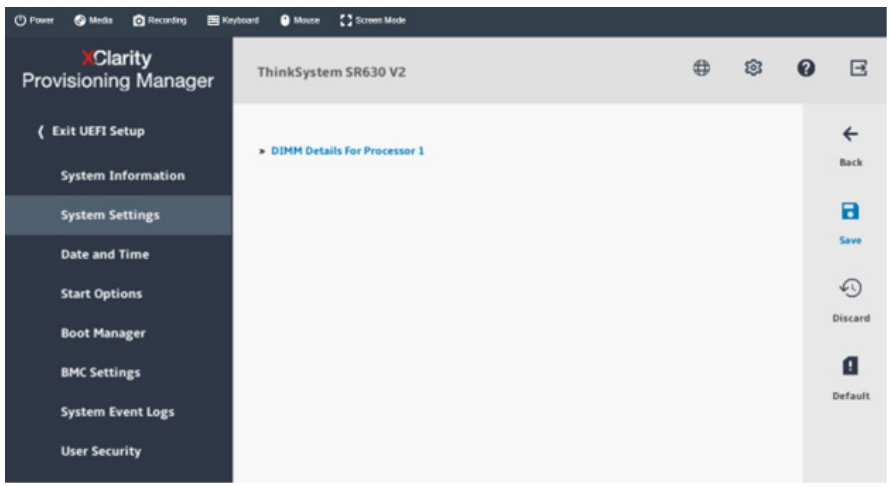
3.3.13 Memory Verification via the IMM Interface for the Lenovo SR630 V2 server

Instead of removing the cover of the server to verify the memory, you can use the IMM Web interface to verify the DIMM positioning.

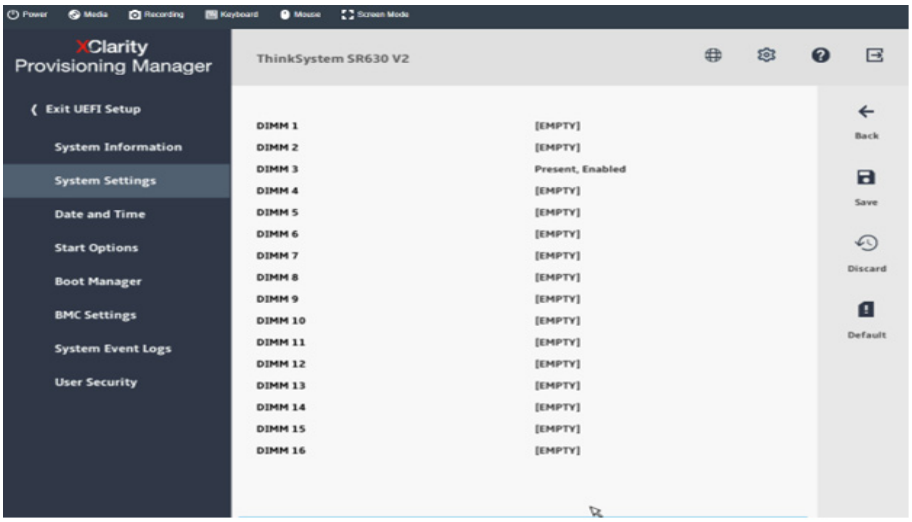
1. In the UEFI Setup (imm) main menu, navigate to **System Settings > Memory > System Memory Details > Cold Boot Fast > Enable**.



2. A list with all installed processors appears.



3. Click on each Processor to get details on the installed DIMMs.



The above figures show how the memories are positioned:

– Processor 1 has one DIMM that occupies slot No.3

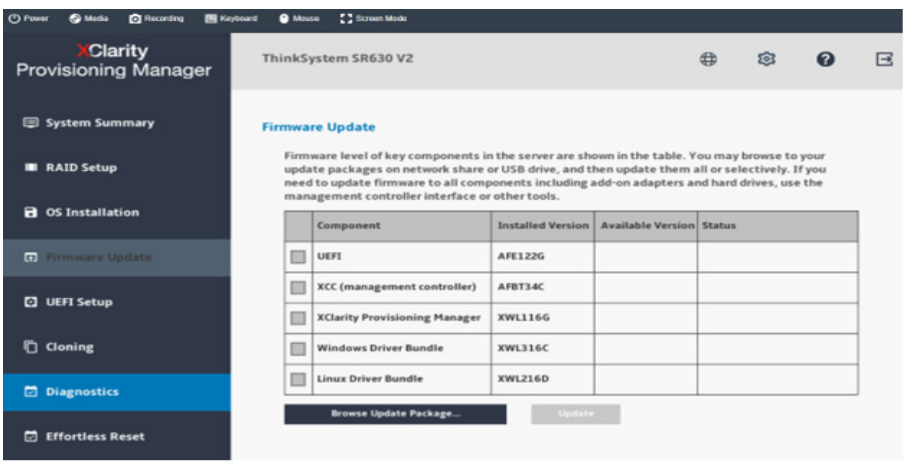
3.3.14 Firmware Updates for Lenovo SR630 V2

1. In the main menu, navigate to **UEFI Setup > System Information**.

2. Verify that the UEFI version is at version 1.30 or higher.

3. The UEFI version comes preloaded from Lenovo. When it is not at the level indicated previously, log in to the Lenovo website, download and install the latest version for this platform.

4. To provide version update, select **Firmware Update** from initial screen.



5. Click **Browse Update Package** and **Update**.

3.3.15 Entering USB menu

1. When booting press F12 to access the BIOS
2. Check **Legacy mode**
3. Finally, select **USB**

3.4 Installing the Lenovo SR630 V3 Server into the Rack

This section describes the equipment needed on the Lenovo SR630 V3. All necessary hardware comes pre-installed. You can find the steps necessary to assemble the hardware, connect the cables and load the necessary firmware so that OpenScape Voice can be loaded with the applicable OpenScape Voice software load.

3.4.1 KVM Notes

The following section applies more to older KVM / Software combinations and should not be relevant for newer hardware/software technologies. However, It remains listed in this document for completeness.

The interaction between the KVM switch and devices attached, is not very simple. When the KVM is not switched to a server/node, it must simulate the connection. If a different signature is generated on the simulation, the server/node will request clarification of the type of mouse in use. Some combinations of KVM switches and mice are not 100% compatible. Failure to have a correctly working KVM/mouse combination may cause your server to hang during a reboot, waiting for operator input.

The following test is suggested to determine, whether problems can be expected. This test must be performed after an installation from scratch (unfortunately this test cannot be performed before the installation):

1. Select the test machine with your KVM and login as **root**.
2. Run: **hwbootscan**; it should produce no output.
3. Switch the KVM to another position.
4. Remotely login, as root, to the test machine.

5. Run: **hwbootscan**; it should produce no output.

Note: If a mouse-selection menu appears, it indicates that the KVM does not simulate the mouse consistently in both positions. In that case, you will either need to change the KVM/mouse combination or perform the steps below each time the system is installed from scratch.

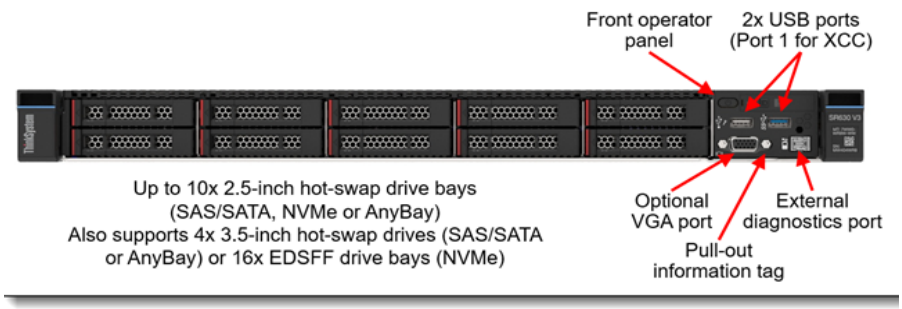
---

6. When prompted, select your mouse type, and **ACCEPT**.
7. Switch back to the test machine.
8. Run: **hwbootscan**; it should produce no output.

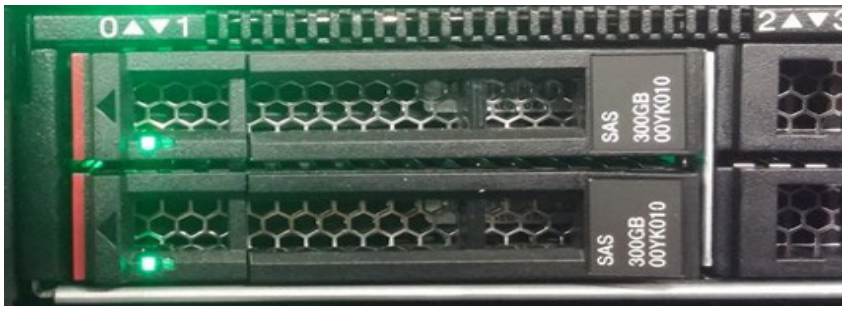
Note: Repeat this process on the other node.

3.4.2 Installing the Disk Drive

The image below shows the location of the two drives. The system comes with a total of 8 2.5-inch drive bays.



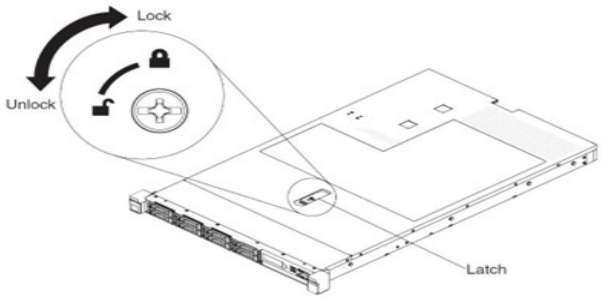
The image below is a close-up of the drives. The two left-most bays are populated with hard disks.



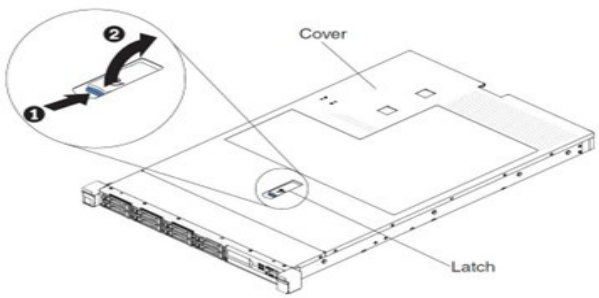
To remove a drive, slide the blue release latch to the right with one finger, while using another finger to grasp the black drive handle and pull the hard disk out of the drive bay.

3.4.3 Removing the Top Cover

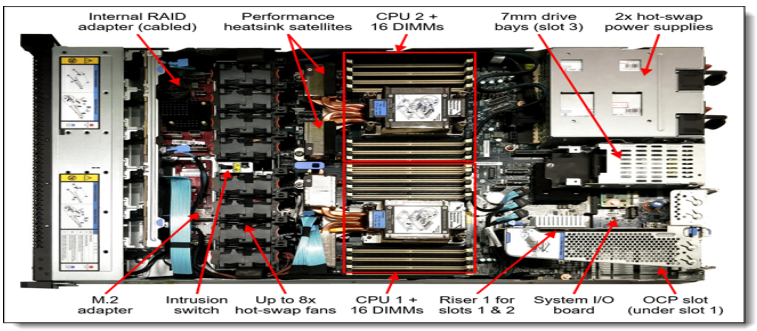
Always check whether the cover is locked. If it is locked, use a screwdriver to turn the cover lock to the open position.



Press the blue tab on the cover-release latch and lift the latch up (the cover will slide toward the rear). Then lift the server cover off and set it aside.



The image below shows the top view of the Lenovo SR630 V3 with its cover removed:



3.4.4 Installing Memory and CPU for the Lenovo SR630 V3

Memory and CPUs come pre-installed. However, ensure that the memory is installed in the correct slots according to Lenovo for optimal heat dissipation.

This can be done in multiple ways, with the easiest method being through the IMM interface (see Remote Console Startup for the Lenovo SR630 V3 server).

The physical method to verify the memory is as follows.

Your server has 16 channels, 32 memory slots, and supports:

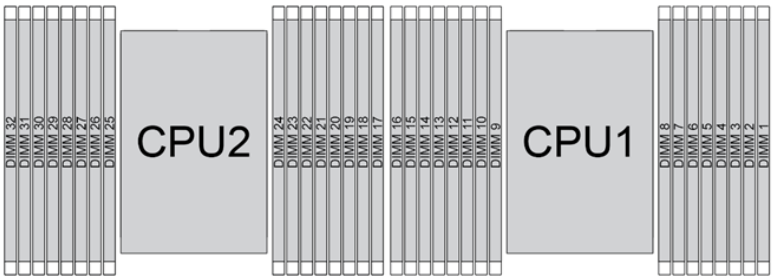
Minimum memory:

- 16 GB

Maximum memory:

- Without PMEMs:
  - 2 TB using 32 x 64 GB RDIMMs.
  - 8 TB using 32 x 256 GB RDIMMs.
- With PMEMs:
  - 10 TB: 16 x 128 GB 3DS RDIMMs + 16 x 512 GB PMEMs (Memory Mode).
  - Total 10 TB installed memory capacity, of which 8 TB (PMEMs) is used as system memory and 2 TB (3DS RDIMMs) is used as cache.
  - 12 TB: 16 x 256 GB 3DS RDIMMs + 16 x 512 GB PMEMs (App Direct Mode).

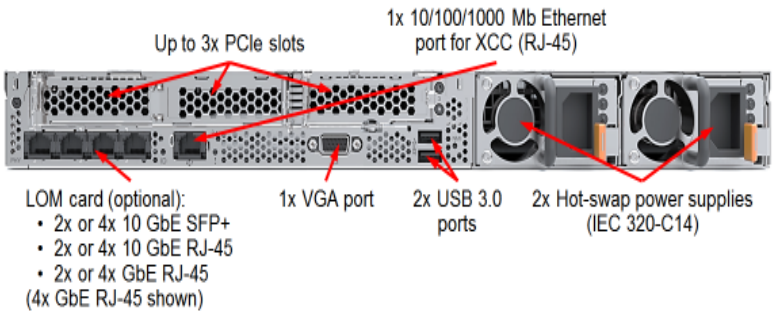
- Total 12 TB installed memory capacity, of which 4 TB (3DS RDIMMs) is used as system memory and 8 TB (PMEMs) is used as persistent memory for storage.



Note: The CPUs come pre-installed, so no manual intervention/ installation is required.

3.4.5 Connection Panel in the rear of the Lenovo SR630 V3 server

The image below gives a general overview of the connection panel in the rear of the Lenovo SR630 V3 server:



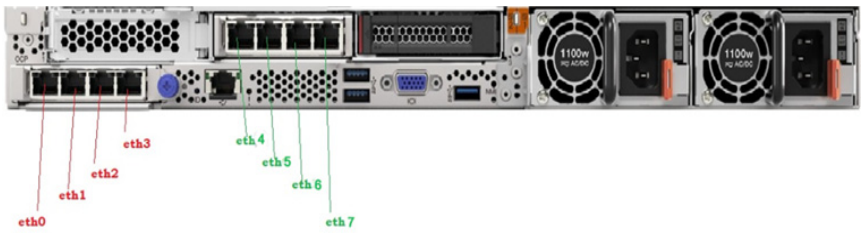
3.4.6 Installing the PCI

The system comes pre-installed with four onboard ports (two integrated, one GbE, and 2 × 1/10/100 GbE LOM – LAN on Motherboard), as well as an Intel 4-port PCI Express card. These are identified in the table below:

PCI express card (Intel)	Integrated-LOM (Broadcom)
eth4 - eth7	eth0 - eth3

Table 5 Onboard Ports

Note: The four onboard ports provide only gigabit support.



3.4.7 Installing the Power Module

Dual power supplies come pre installed and are visible from the back of the machine, see Chapter 3.8.5 Connection Panel in the rear of the Lenovo SR630 V3 server.

3.4.8 Wiring the Cluster

The following diagrams show the Ethernet port assignments for the Lenovo SR630 V3, for a duplex and a simplex setup.

Note: For a simplex setup, only ports eth0, eth1 and eth2 are used.

Ethernet	Number of ports	Duplex			Simplex			
Ethernet card	4 ports	4	5	6	7			
LOM	4 ports	0	1	2	3	0	1	2
		Bond 0 (admin)	Bond 1 (signaling)	Bond 2 (billing)	Bond 3 (X-channel)	admin	signaling	billing

Table 6 Ethernet Port Assignment

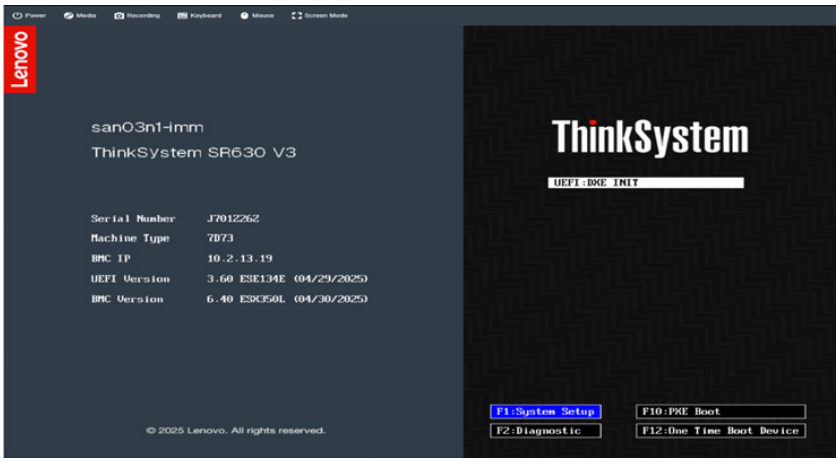
After adding and wiring all hardware to the machine, continue with the UEFI configuration, RAID creation and firmware updates. Connect the KVM devices to the server prior to initial boot.

Note: SR630 V3 requires a USB keyboard and mouse. Use a PS/2 to USB adaptor in most cases. See previous section on KVM issues for more details.

3.4.9 Setting up the UEFI for the Lenovo SR630 V3 server

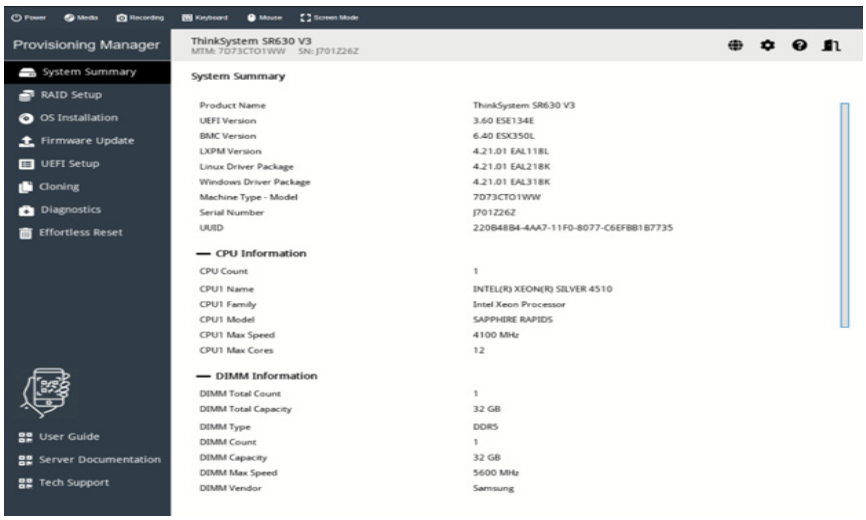
Follow the instructions below to setup the UEFI.

1. Reboot the system to enter the **Setup Utility**. At the initial screen prompt of **<F1> System Setup**, press **F1** to enter "System Setup".



2. The **System Configuration utility** page opens:

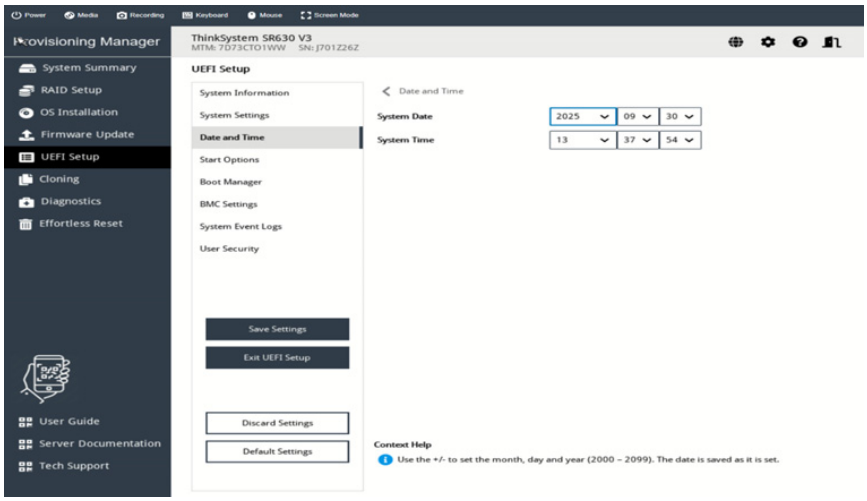
Note: You can also display the **System Configuration utility** page by clicking the help icon at the top right of your screen and selecting Getting Started.



3. Under **UEFI Setup,** select **Date and Time** to configure the System time and date.

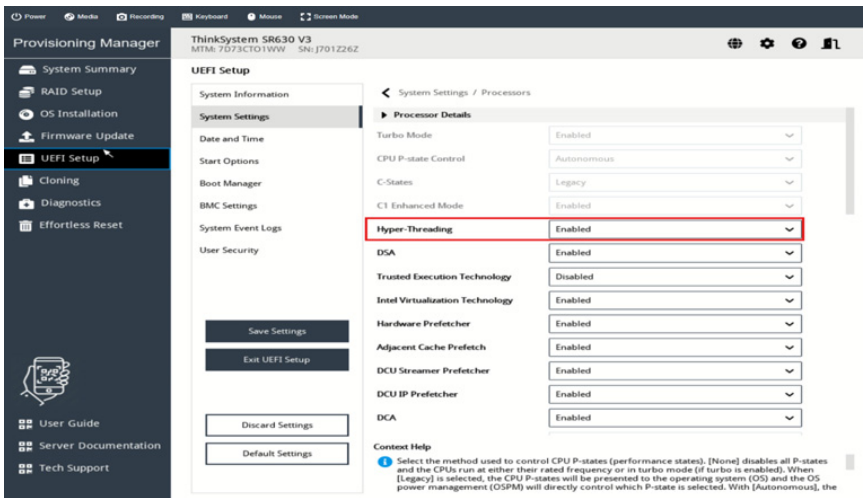
4. Click **Save Settings.**

You are directed back to the **UEFI Setup** menu.



5. Navigate to **System Settings** > **Processors**.
6. In the **Processor Details** page, from the **Hyper- Threading** drop-down menu, select "Disable".
7. Click **Save**.

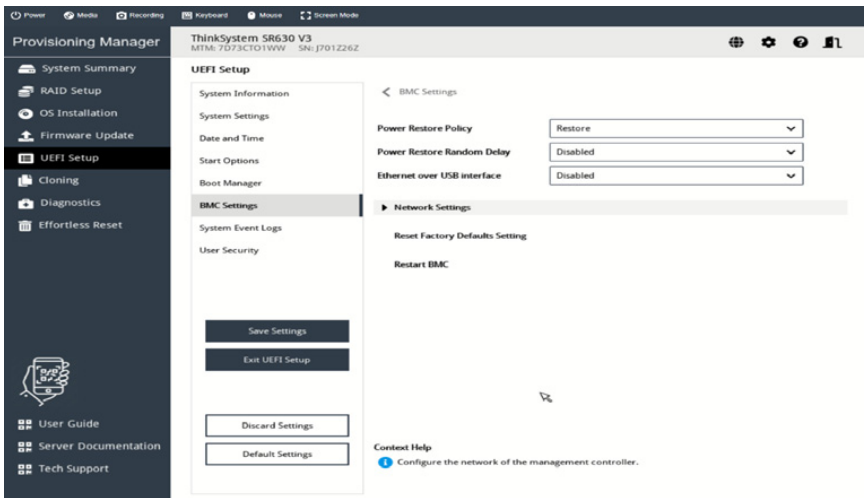
You are directed back to the **System Settings** menu.

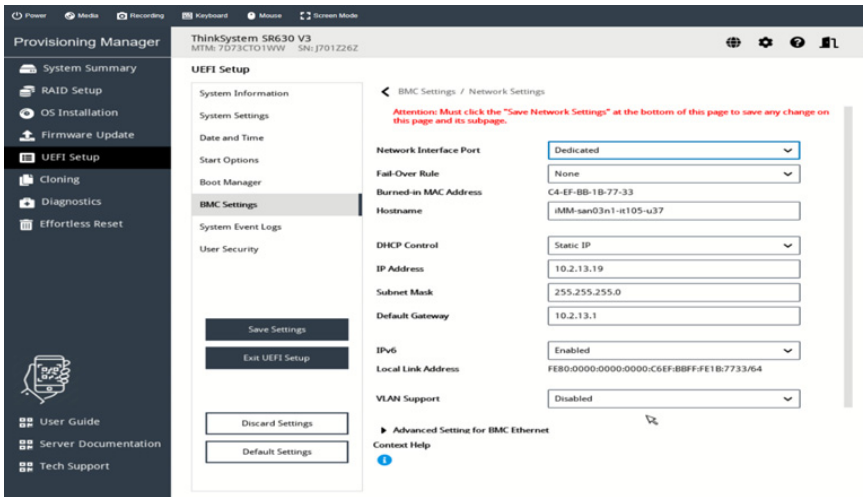


Note: After disabling Hyper-Threading, perform a power-cycle before restarting the system.

---

8. Select **BMC Settings** and navigate to **Network Settings** to change the network configuration for the IMM.

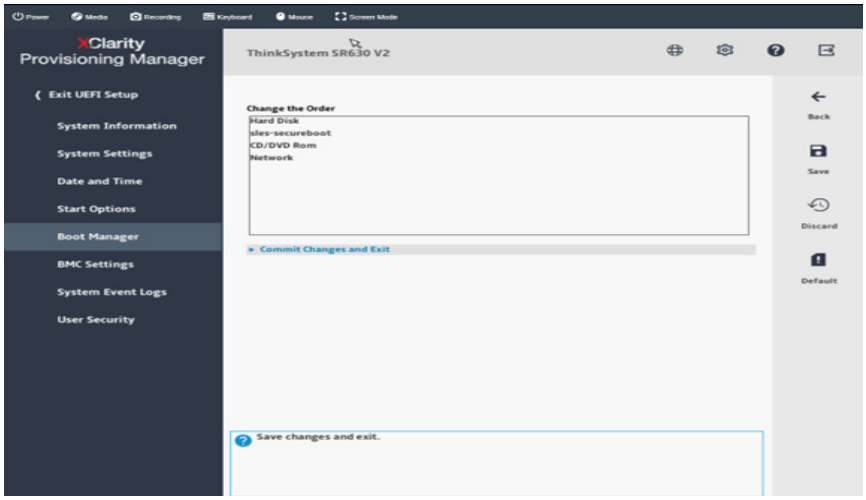




9. In the **Network Configuration** window, configure the following parameters:
   - **DHCP Control**: Static IP
   - **IP Address**: Value from for the given network
   - **Subnet Mask**: Value from for the given network
   - **Default Gateway**: Value from for the given network
10. Click **Save Settings**.

You are directed back to the UEFI Setup menu.

11. Select **Boot Manager** -> **Change Boot Order**.



12. In the **Boot Manager** page, select **Change the Order**.
13. Place the boot devices in the following order:
    - <CD/DVD Rom>
    - <Hard Disk>
    - <Network>S

Note: If needed, reorder the selected devices with the use of -/+ keys in the **Change the Order** box.

---

14. Click **Commit Changes** and **Exit**.
15. Return to the Boot Manager menu and select **Boot Modes** under the System section.
16. To have the bootable USB sticks recognized as bootable devices, configure the following parameter::
    - System Boot Mode: Legacy Mode
17. **Save** your changes.

You are directed back to the Boot Manager menu.

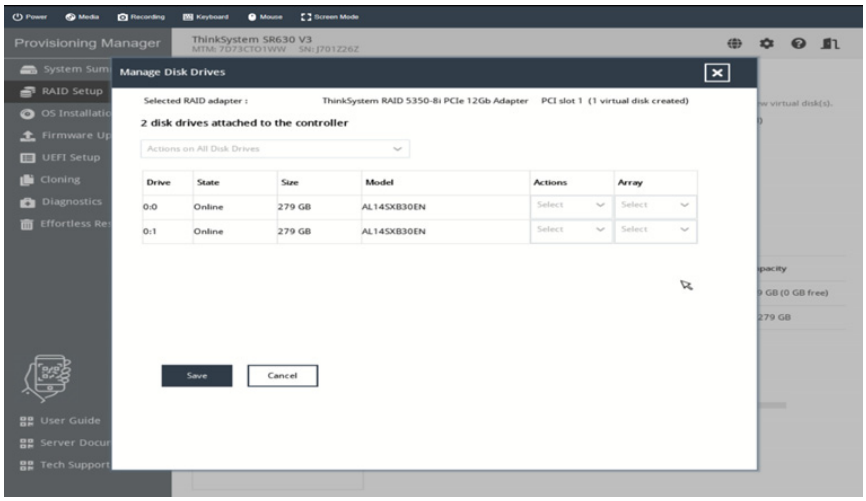
The system is ready for RAID 1 setup.

Note: You don't need to reset the IMM for Network changes to take effect.

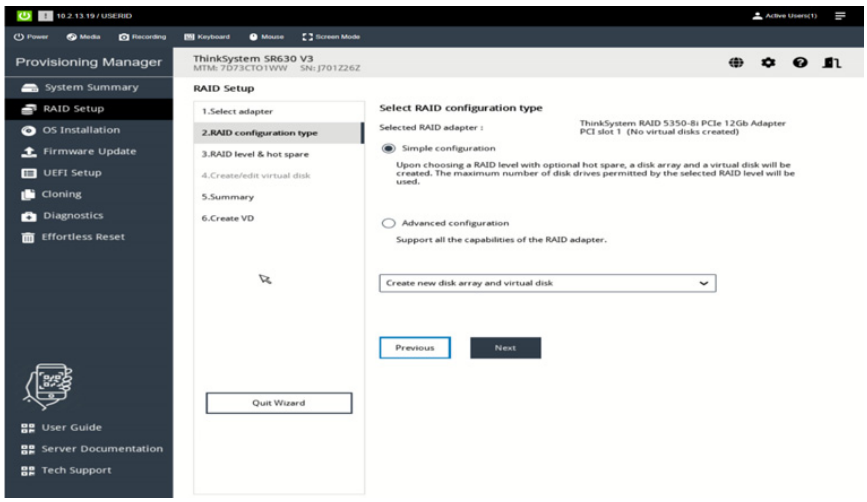
3.4.10 Creating the LSI RAID for the Lenovo SR630 V3

Follow the steps below to setup the internal LSI controller and disks into a mirrored pair (RAID1). The LSI RAID Creation is done via the UEFI RAID Setup.

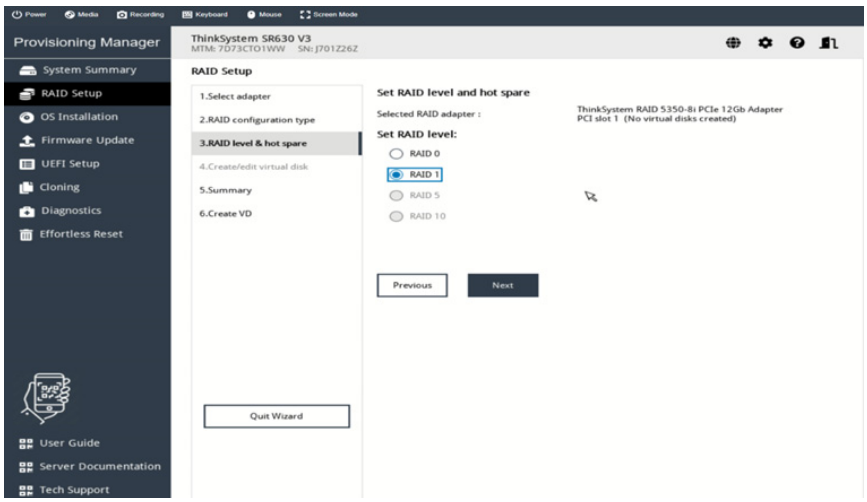
1. In the UEFI main menu, select **RAID Setup**.
2. Navigate to **Manage Disk Drives**, select **Actions on All Disk Drives** and click **Next.**



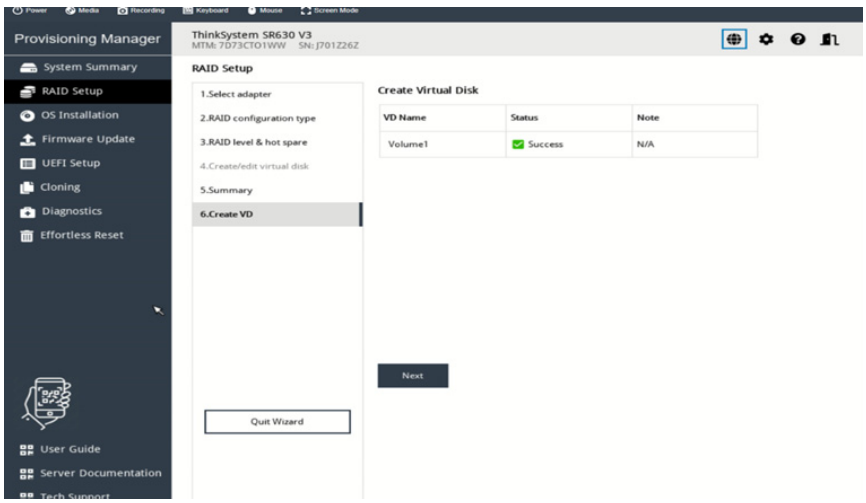
3. In the **Select RAID configuration type** page, select **Simple configuration** and click **Next**.



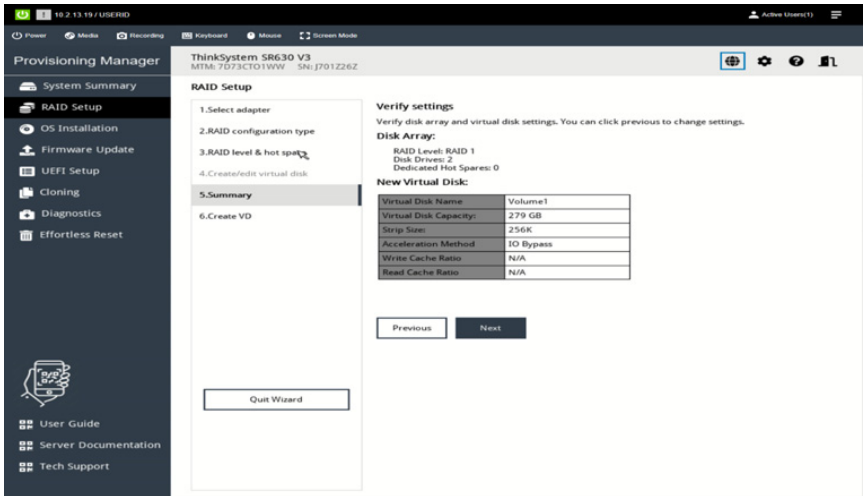
4. In the **Set RAID level and hot spare** page, select **RAID Level 1** and click **Next**.



5. Verify that **Virtual Disk** was created successfully and click **Next**.



6. In the **Verify Settings** page, ensure that everything is properly set.



The LSI configuration has been completed.

7. Return to the main menu, click **Exit** and then click **OK**.

Verify the IMM interface and then reboot the server. It is now ready for OSV software installation.

3.4.11 Activation of IPMI Over LAN for the Lenovo SR630 V3 server

The IPMI Over LAN capability needs to be activated, as it is required by the IPMI shut down agent. For the activation, you need to login to the IMM interface.

1. Open a Web browser.
2. In the address or URL field, type the IP address or hostname of the IMM server to which you want to connect.

Note: Use **https** for a secure connection. This brings up the web page for the IMM.

---

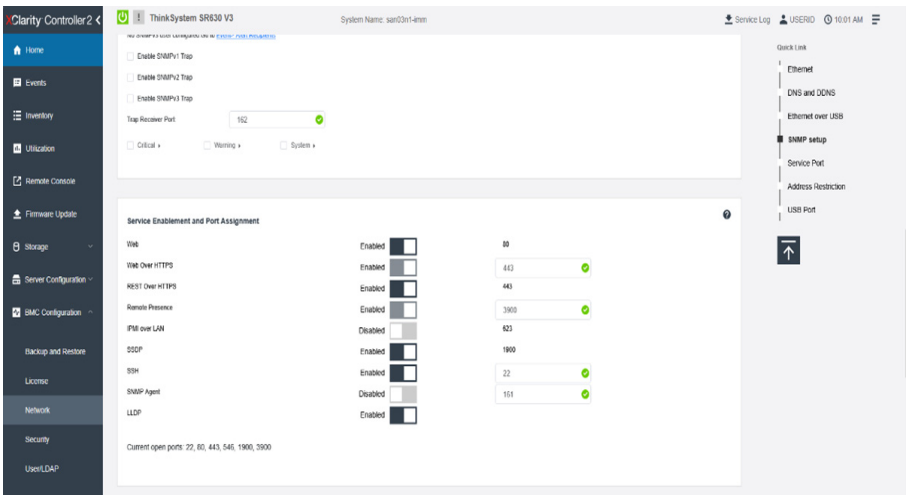
3. To view a list of web browser versions which are supported by the IMM firmware, click on **Supported Browsers**.
4. Enter your user id and password. The default values are:
   - Username: USERID

- Password: PASSW0RD

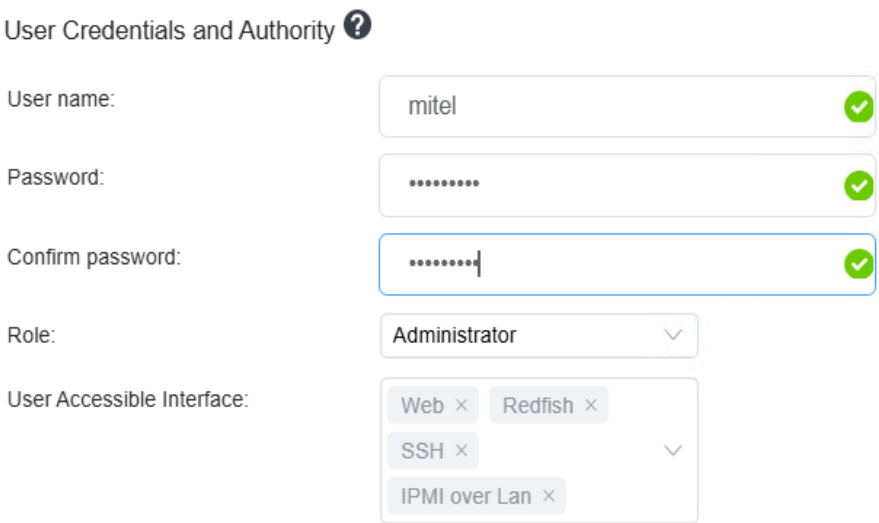
Note: The 0 in PASSW0RD is the digit 'zero'.

After you enter the user id and password, the main page appears.

5. Navigate to the **BMC Configuration** > **Network** tab.
6. Enable the **IPMI over LAN** slider, if not already enabled.



7. Next, navigate to the **BMC Configuration > User/LDAP** tab.
8. Edit each user and add option **IPMI over LAN** in the **User Accessible Interface** box.



3.4.12 Remote Console Startup for the Lenovo SR630 V3 server

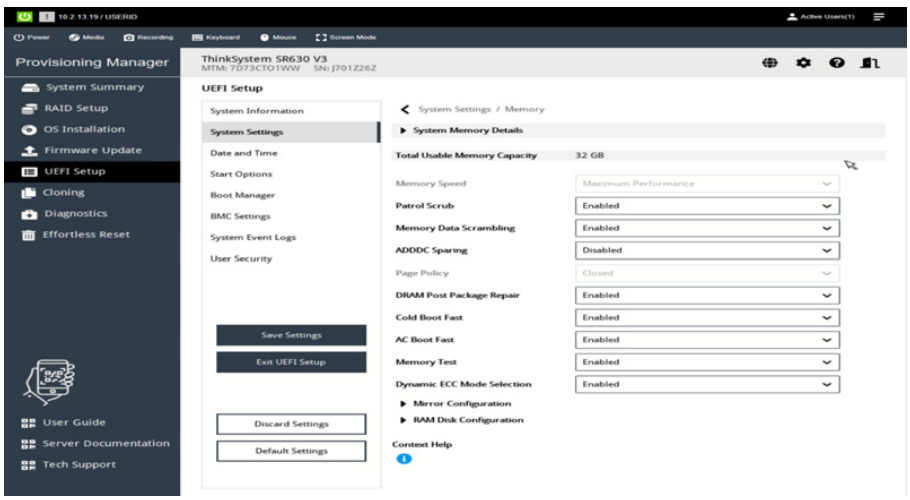
1. Log into the IMM interface of the server as described in the previous Section 3.4.11, “Activation of IPMI Over LAN for the Lenovo SR630 V3 server”.
2. In the **Remote Control Preview** field, click on **Launch Remote Control**.

A new tab opens, giving you full access to the server console.

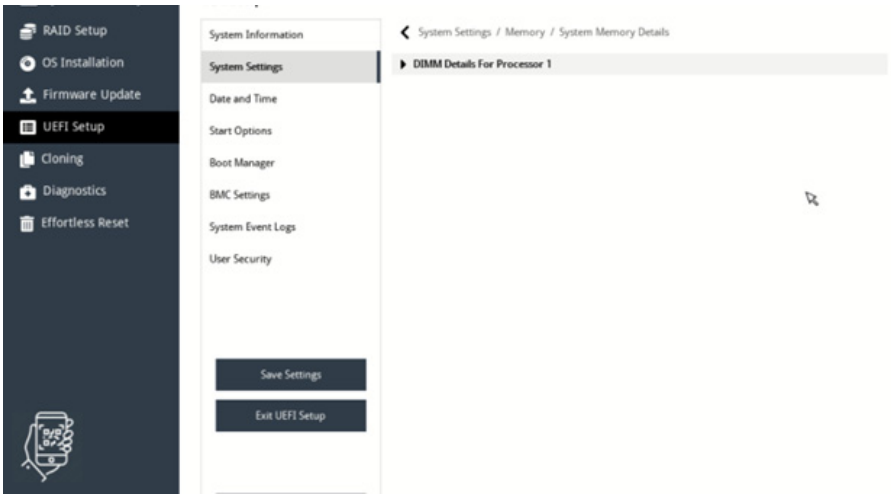
3.4.13 Memory Verification via the IMM Interface for the Lenovo SR630 V3 server

Instead of removing the cover of the server to verify the memory, you can use the IMM Web interface to verify the DIMM positioning.

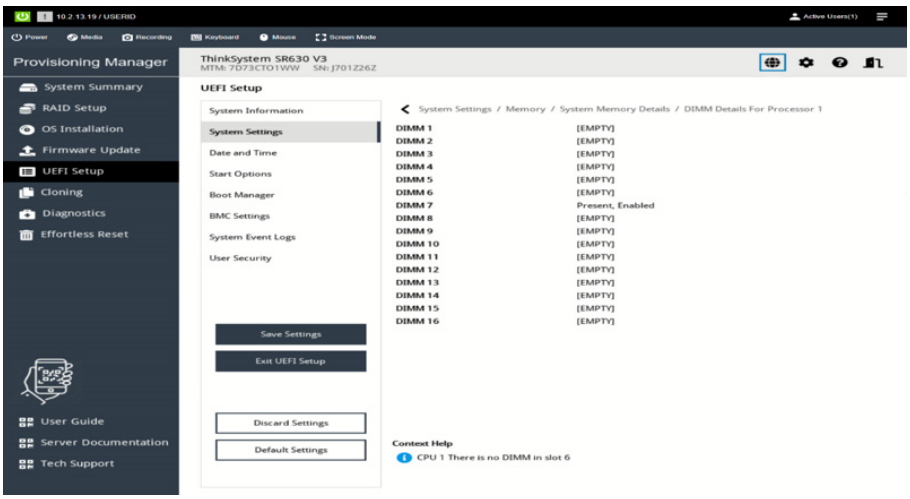
1. In the UEFI Setup (imm) main menu, navigate to **System Settings** > **Memory** > **System Memory Details** > **Cold Boot Fast** > **Enable**.



A list with all installed processors appears.



2. Click on each Processor to get details on the installed DIMMs.



The above figures show how the memories are positioned:

- Processor 1 has one DIMM that occupies slot No. 7

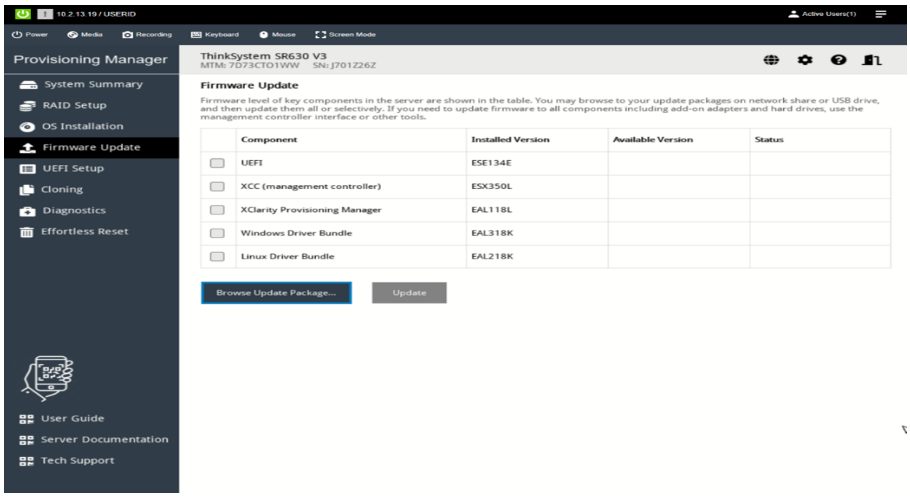
3.4.14 Firmware Updates for Lenovo SR630 V3

1. In the main menu, navigate to **UEFI Setup** > **System Information.**
2. Verify that the UEFI version is at version 1.30 or higher.

Note: The UEFI version comes preloaded from Lenovo. If it is not at the version indicated above, log in to the Lenovo website to download and install the latest version for this platform.

---

3. To provide version update, select **Firmware Update** from the initial screen.



4. Click **Browse Update Package** and **Update**.

3.4.15 Entering USB menu

1. When booting, press F12 to enter the BIOS.
2. Check the **Legacy mode** checkbox**.**
3. Select **USB**.

3.5 Remote Video Redirection and Java 7, Update 51

Beginning with Java 7 update 51 (scheduled for January 14, 2014), all applets that do not comply with the new security model will be blocked when using the default security settings within the Java Control Panel.

This behavior will block the Java based access to the maintenance controller "Remote Video Redirection" feature. The "Remote Video Redirection" feature allows users access to the OSV node console from a workstation/PC. The "Remote Video Redirection" feature negates the need for on-site console access and is the recommended access method for the OSV "Remote Software Upgrade" procedure.

The maintenance controller in an IBM server is commonly referred to as the IMM. In a Fujitsu server the maintenance controller is commonly referred to as the iRMC.

A solution and workaround provided by Java can be found at this URL:

http://www.java.com/en/download/help/java_blocked.xml

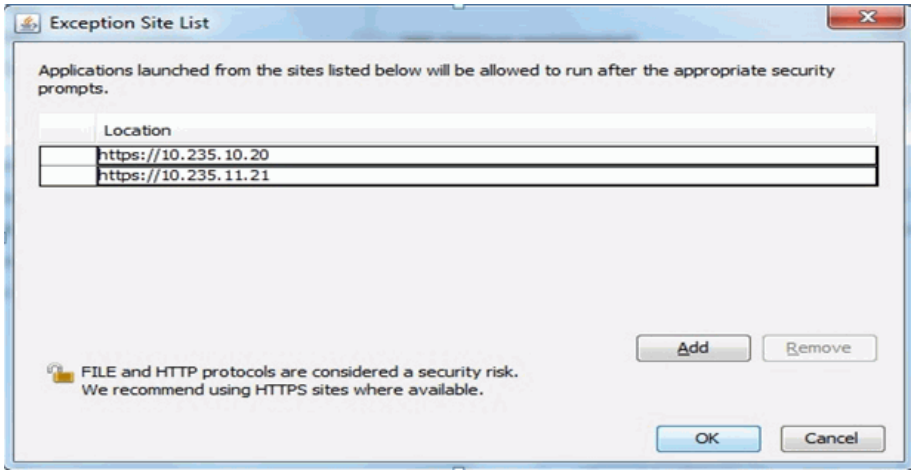
Workaround Overview

The workaround edits the Java 'Exception Site List' in the Java Control Panel.

To access the Java Control Panel from a Windows PC:

- Select **Start** > **Control Panel** > **Java (32/64-bit)**.
- In the Java Control Panel, click on the **Security** Tab and then click the **Edit Site List** button.

When executing the workaround, the Maintenance Controller IP(s) can be substituted for a URL in the "Exception Site List". An example "Exception Site List" update follows. The example is for a workstation that accesses the maintenance controllers of a network separated OpenScape Voice deployment. In a co-located OpenScape Voice deployment the first three octets of the IP addresses would be the same;


Exception Site List
Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.
Location
https://10.235.10.20
https://10.235.11.21
Add
Remove
FILE and HTTP protocols are considered a security risk.
We recommend using HTTPS sites where available.
OK
Cancel

.

4 Installing the OpenScape Voice Reference Image

Before starting the installation, ensure that the servers to be used are supported for the new installation. For details, refer to Table on page 417.

4.1 Prerequisites

- Hardware installation: Before the OpenScape Voice reference image can be loaded, the hardware must be installed and cabled. Refer to the checklists in Chapter 2, “Preparing for the Installation” and Chapter 3, “Installing the Hardware Platform”.
- Reference image ISO: Copy the Reference image to USB stick(s) for Physical Server refer to Section 4.2.3.1, “Physical systems via USB” or upload to Datastore for Virtual Server, refer to Section 4.2.3.3, “Virtual systems via Virtual CD/DVD”.
- Node.cfg file: Because the network design and IP address allocations are already known, the node.cfg configuration file can and should be prepared in advance of the installation process. Refer to Section 2.6 on page 50 to prepare the node.cfg file.
- Before starting Symphonia services, make sure that you are logged in as a `root` user or if you are a srx user, change to root user with the following command: `su - root`

4.2 Installation via USB

4.2.1 Overview

The L3 interconnection link must be up and running during the entire procedure in order for the installation to complete successfully.

For a redundant (duplex) system, the installation of both nodes should be performed in parallel because the installation process requires both nodes to communicate over the cluster interconnect.

The first node will stop at "RtpInstall step 0" and wait for the second node to reach "RtpInstall step 0".

At that point, the two nodes will get in sync, pass the interconnection test, and complete the installation.

During an installation or an upgrade process, the hard disk drives for each node are divided into two partitions of equal size. These HDD partitions are referred to as the ‘Primary’ partition and the ‘Secondary’ partition.

The partition on which the running software resides is called the ‘Active’ partition (this could be either the ‘Primary’ or ‘Secondary’) and the other partition is called the ‘Fallback’ partition (also referred to as the ‘standby’ partition).

Patching procedures always apply to the ‘Active’ partition only.

Note: This Note does not pertain to Upgrade or Migration procedures. Upgrades and migrations should follow the steps of their respective Upgrade/Migration scenario.

This note only applies to lab environments installing an OpenScape Voice server image without updating the existing External Application Server (OffBoard) server. This will prevent a lockout of the OpenScape Voice ‘srx’ user during the image installation.

In lab environments with an already existing External Application Server (OffBoard);

If the external Applications server is a Multiple Communication Server Admin deployment, remove the Voice server system from the external Applications server List of Switches. Do not ‘Add’ the Voice Server to the external Applications server until the image install is complete.
If the external Applications server is monitoring this system only, i.e., Applications servers deployed in a “Standard Duplex - Small Deployment”, stop symphoniad. The symphoniad process can be ‘stopped’ before the image is installed and ‘started’ after the image install completes.

Removing an OpenScape Voice server from a Standard Duplex (Large or Small) UC Applications deployment will result in the loss of UC application data (e.g., OpenScape Users/Resources).

4.2.2 Prerequisites

Installation and Restore functionality are supported for the following:

- Virtual ESXi VMware platform
- Lenovo SR630 V2

For fresh installation choose the latest image from the software repository (for example V11_RX_X.X_IMG.iso).

USB memory stick requirements:

- Minimum size of 16 GB
- Standard Type-a USB connection
- USB 2 or USB 3

Note: The USB stick will be formatted and all data will be deleted.

The OSV USB stick must contain:

- OSV DVD image ISO in root of USB drive (for example E:\V11_RX_X.X_IMG.iso)
- Any applicable OSV patch sets in folder patch of USB drive (for example E:\patch\)
- Node configuration file in root of USB drive (E:\node.cfg.primary or E:\node.cfg.secondary)
- License files in folder patch (for example E:\patch\ Eula-01-End_User_License_Agreement) (optional)
- OpenScape_Voice license

Note: The voice server license files can be copied onto the installation USB for automatic installation during the image installation process. This requires the keyword OpenScape_Voice be used in the license file name.

A diagram of the USB files is the following:

- USB root folder (e.g. E:\)
  - <OSV DVD image ISO>
  - <NCPE or CDC node.cfg.{primary,secondary}>
  - OpenScape_Voice license
  - patch
    - <License files>(End_User_License_Agreement) (optional)
    - <patch sets>
    - An empty file, dev.8kps

Note: You can only edit the content of the USB stick. For example, reformatting the drive to FAT32 will break the disk's functionality.

4.2.3 Installation Procedure

4.2.3.1 Physical systems via USB

OpenScape Voice can be installed via a USB bootable device.

The **OpenScape Voice USB Service System (OSV_USB_Service_System)** is a minimal live Linux system booted from USB drive in order to launch service operations:

- Image Installation
- System Restore
- Service System Image Write

The main workflow of the USB image installation is the following:

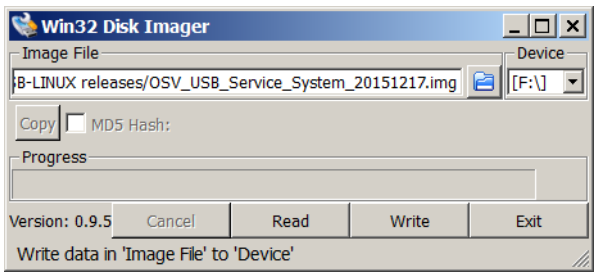
1. Download the **OpenScape Voice USB Service System (OSV_USB_Service_System)** from SWS repository.
   Extract the **OSV_USB_Service_System_<VERSION>.zip** archive to obtain the raw image of the live system, **OSV_USB_Service_System_<VERSION>.img**. The space needed for the uncompressed file is approximately 16GB.

   To write it on a USB flash drive, use the "Service System Image Write" operation, as described at Section 4.2.3.2, “Image installation/System Restore USB/Service System Image Write”.

   Alternatively, a low level copy tool, may be used. For Microsoft Windows use Win32 Disk Imager, please download it from here:

   http://sourceforge.net/projects/win32diskimager/

2. Choose the image and the target USB device and click write:



   The writing process may take several minutes (more than 50 minutes) depending on the combined speed of the USB port and drive.
   For Linux use the dd data dump program. Detect the USB drive device with the help of 'blkid' and 'lsblk' commands. If, for example your USB drive is

block device /dev/sdb, you can write the image with command: "dd if=/path/to/OSV_USB_Service_System_<VERSION>.img of=/dev/sdb && sync"

Caution: This dd command should be run on the whole device, not in one of its partitions (e.g. /dev/sdb1, /dev/sdb2 etc.). The image contains the partition table of the live system and this should be dumped on the USB drive as it is

---

After the successful writing process close the programs and check that the flash drive label is 'OSV-USB-LINUX', which means everything went OK. The first partition is in NTFS format in every case and is the only partition present in Microsoft Windows or Mac OSX. The live bootable system is transparent on all OSes and is only used during the installation. You can use this USB drive for any use BUT if you reformat it to something other than NTFS, the Openscape Voice image ISO won't fit (for example, FAT32 limits) and also the installation program will complain and abort.

3. The data and configuration files are generated from their respective tools (NCPE or CDC tool for node.cfg) or acquired from shared locations (OSV ISO images, license files).

Note: For the automated procedure, ignore steps 4 and 5 below and follow the instructions described in Section 4.2.3.2, “Image installation/System Restore USB/Service System Image Write”

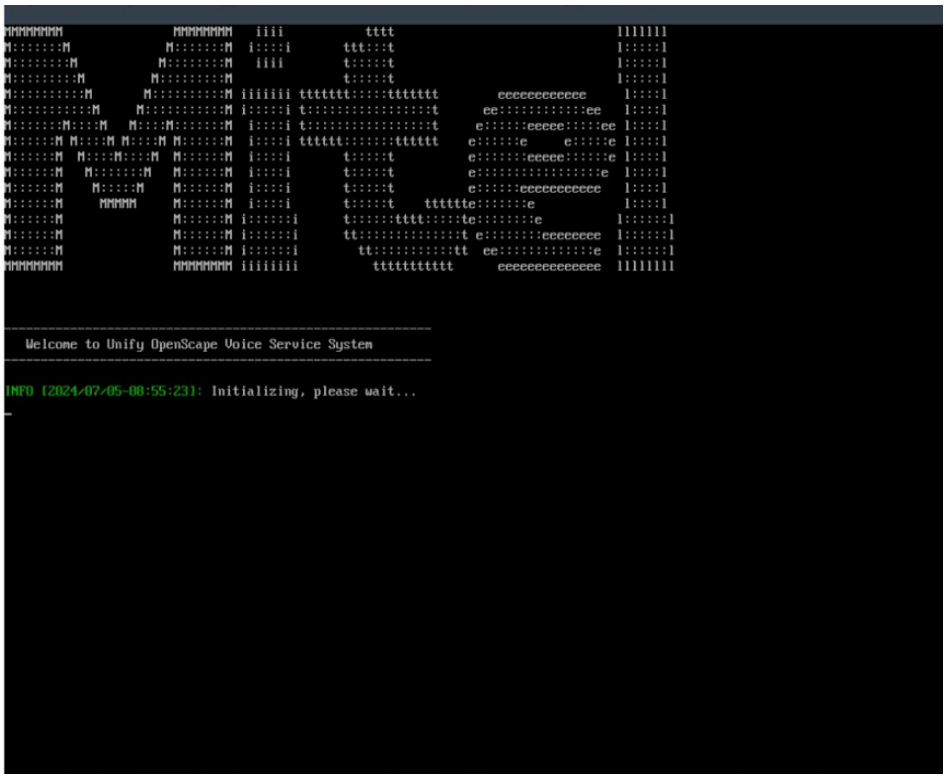
---

4. Copy the completed node.cfg file to the USB memory stick as node.cfg.primary. Click here to return to step e, of Section 4.3.4.1, “Preparation of the node.cfg files using a Linux or Windows Environment”.
5. Make another copy of the node.cfg named node.cfg.secondary. Return to step e, of Section 4.3.4.1, “Preparation of the node.cfg files using a Linux or Windows Environment”
6. The USB drive(s) are ready for booting and starting the image installation. In case of a cluster, both nodes are started with their respective USB drives attached.
7. Click F12 to start the boot drive choice menu and choose the USB drive.

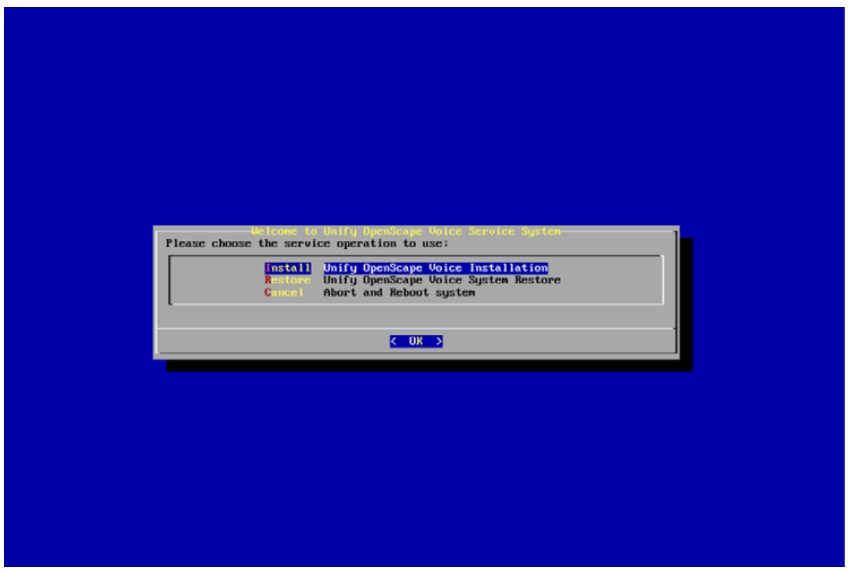
   Note: For detailed information on how to select the USB drive, consult your server’s manual.

   ---

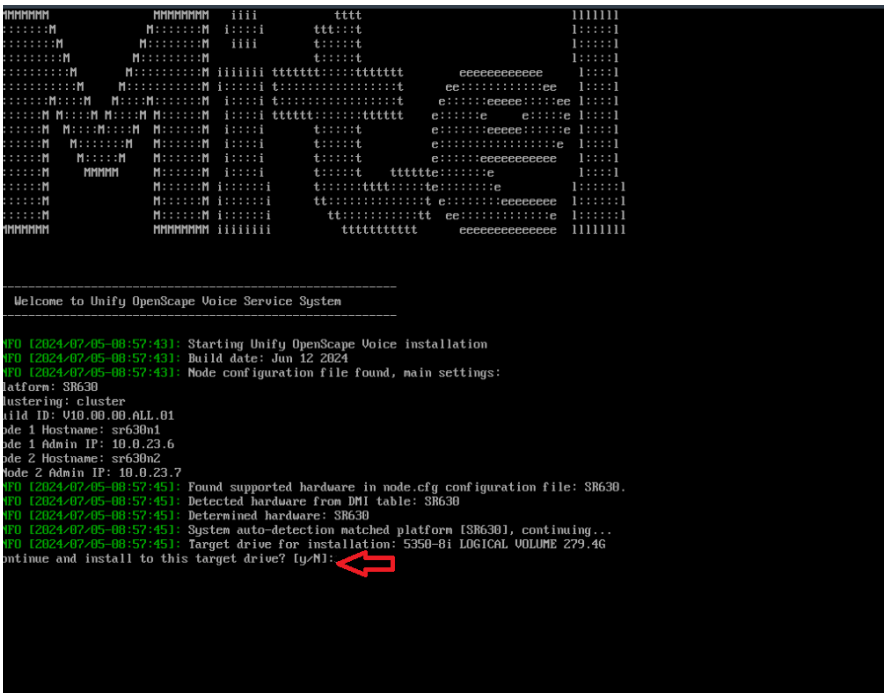
8. The **OpenScape Voice USB Service System** boots.
9. In the initial boot screen, select the first option.



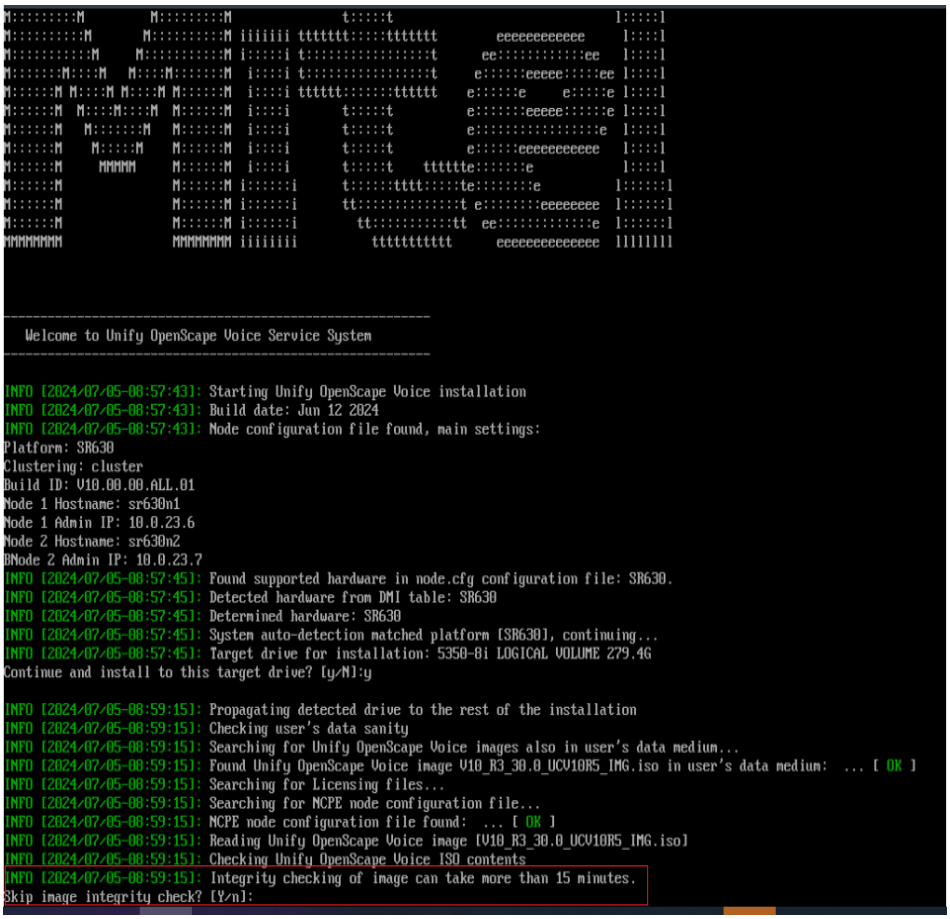
10. Select **Install Unify OpenScape Voice Installation** and press **OK**



Target disk drive for installation detected and data files found and checked.



11. When you want to perform Integrity Check, select **No.** The default value is **Yes** and the Integrity Check will be skipped. The Integrity Check will take more than 15 min.



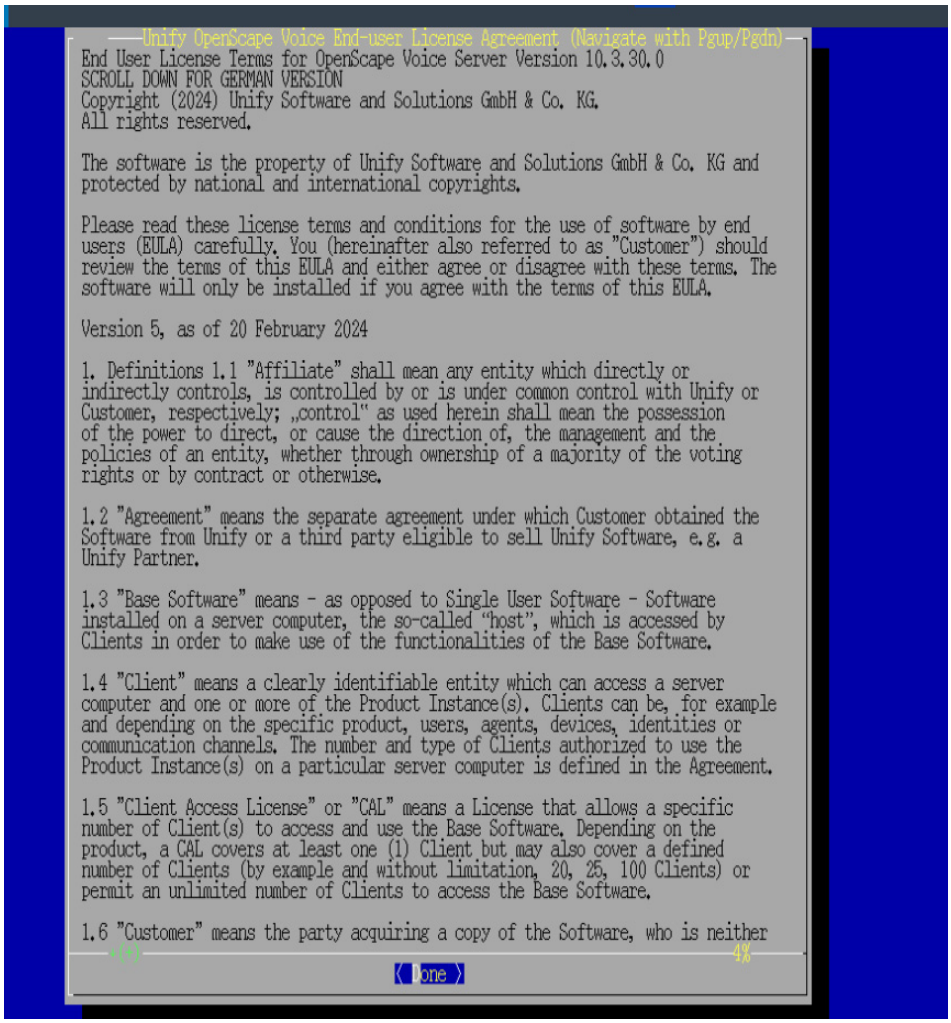
12. Accept EULA (End User License Agreement)
    The End User License Agreement (EULA) is displayed in a new window on the console screen. Review and accept the EULA as follows:

    a) Review the EULA using the Page Up/Page Down or arrow keys; when you are finished reviewing the EULA, select **Done** and press the **Enter** key.

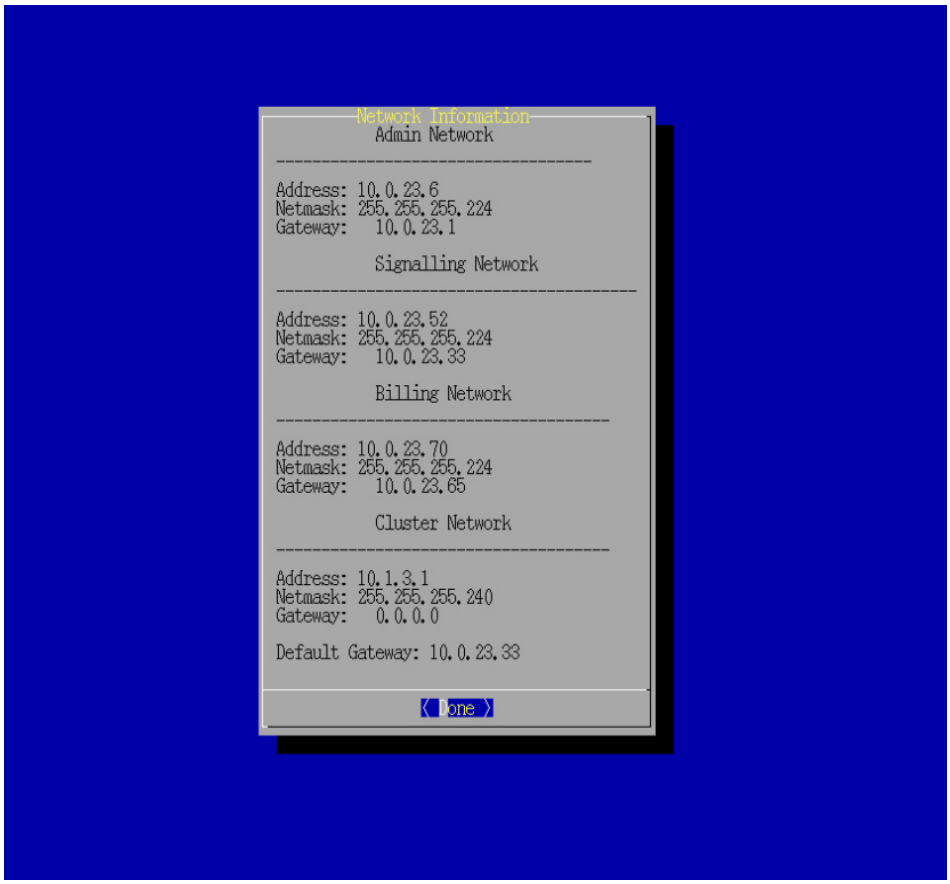
    b) A window is opened with the question: "**Do you accept the License Agreement?**" with the options '**Yes**' and '**No**'

    c) In the EULA acceptance window, use the Tab or arrow keys to select **Yes** to proceed with the image installation. Selecting '**No**' will halt the image installation.

    d) If you select '**No**' by mistake, to continue with the image installation, reboot the server and when prompted to accept the EULA, select **Yes**.



13. Press “**Done**” on the “**Network Information**” page, which is displayed as soon as the appropriate Virtual Floppy with the node.cfg is mounted.



14. Type **yes** and press enter as shown below and the Image installation will start.

- Repeat steps 9 through 12 of Section 4.2.3.3 for Node 2; making sure to select USB memory stick that contains the node.cfg.secondary.

Note: For specific details of the Image installation please refer to the Release Notes of the Image ISO.

---

15. When prompted, select the installation scenario: `yes/no/format/lockprim/locksec/verify`

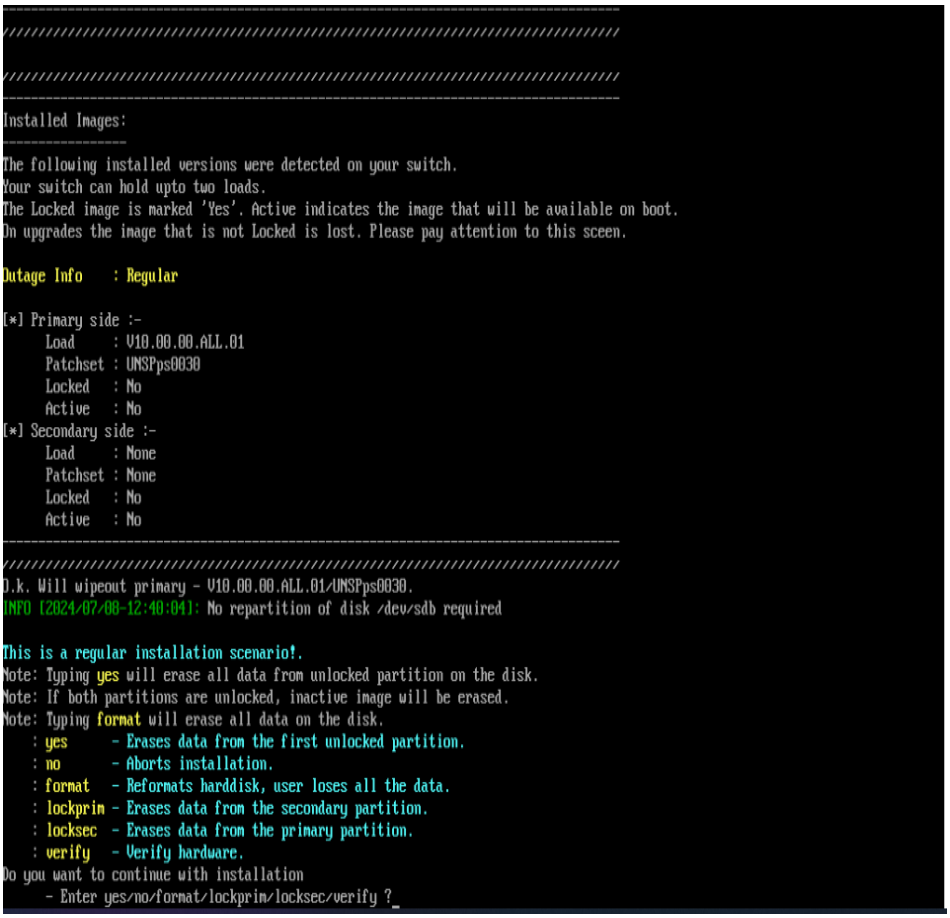
Attention: In a duplex setup, when installing a fresh system, both nodes must be installed either in the primary partition or in the secondary, not in a mixed setup, for example node1: primary, node2: secondary. Otherwise the installation process will not be synchronized between nodes and will fail.

Note: Typing yes or format will erase all data from unlocked partition on the disk.

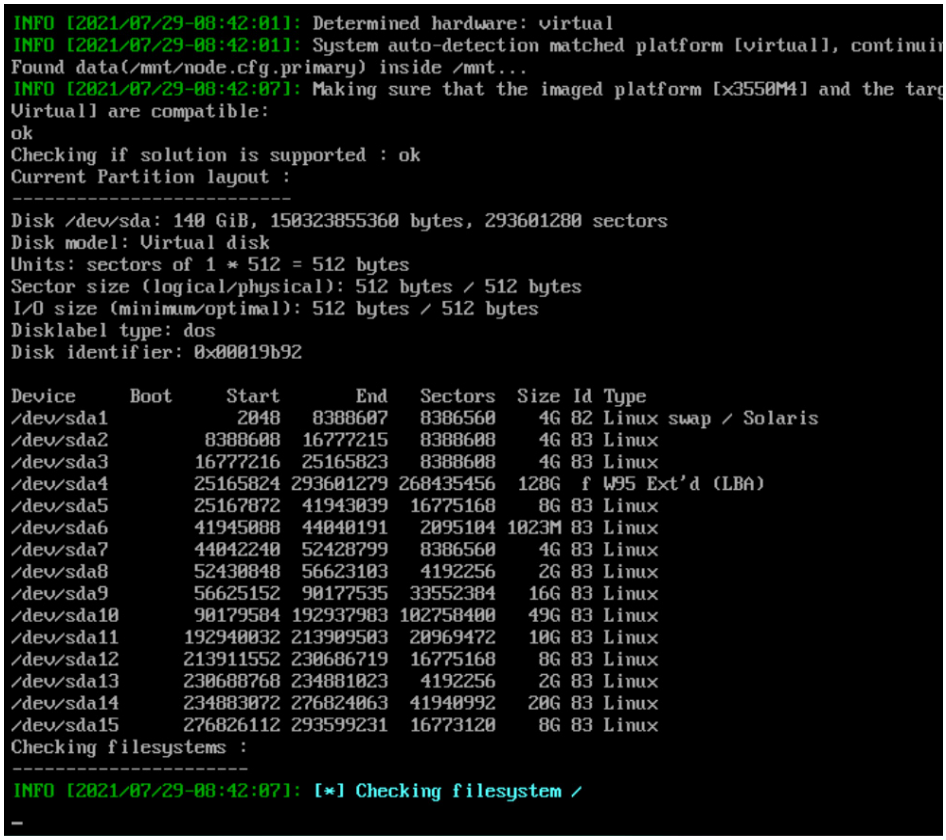
- **yes** - Erases data from the first unlocked image.
- **no** - Aborts installation.
- **format** - Reformats harddisk, user loses all the data
- **lockprim** - Erases data from the secondary partition
- **locksec** - Erases data from the primary partition
- **verify** - Verify hardware

```
Do you want to continue with installation (enter yes/no/
format/lockprim/locksec)?
```

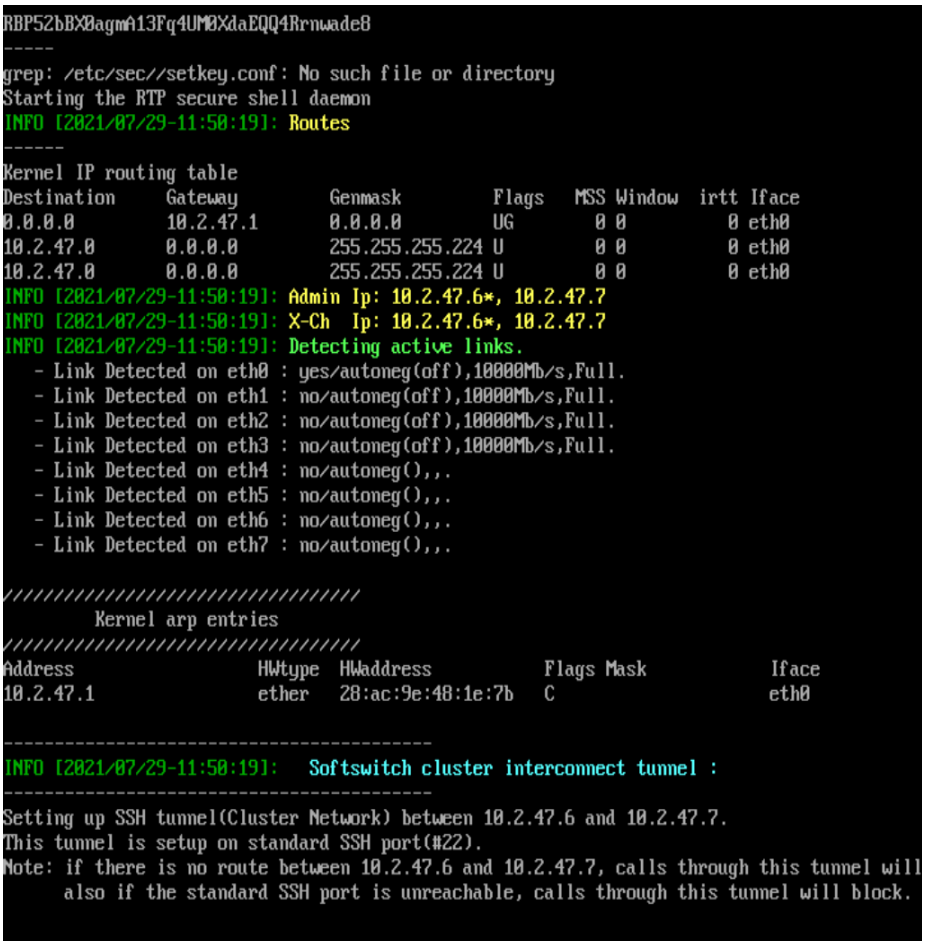
Note: Format and re-partition are necessary for fresh installation.

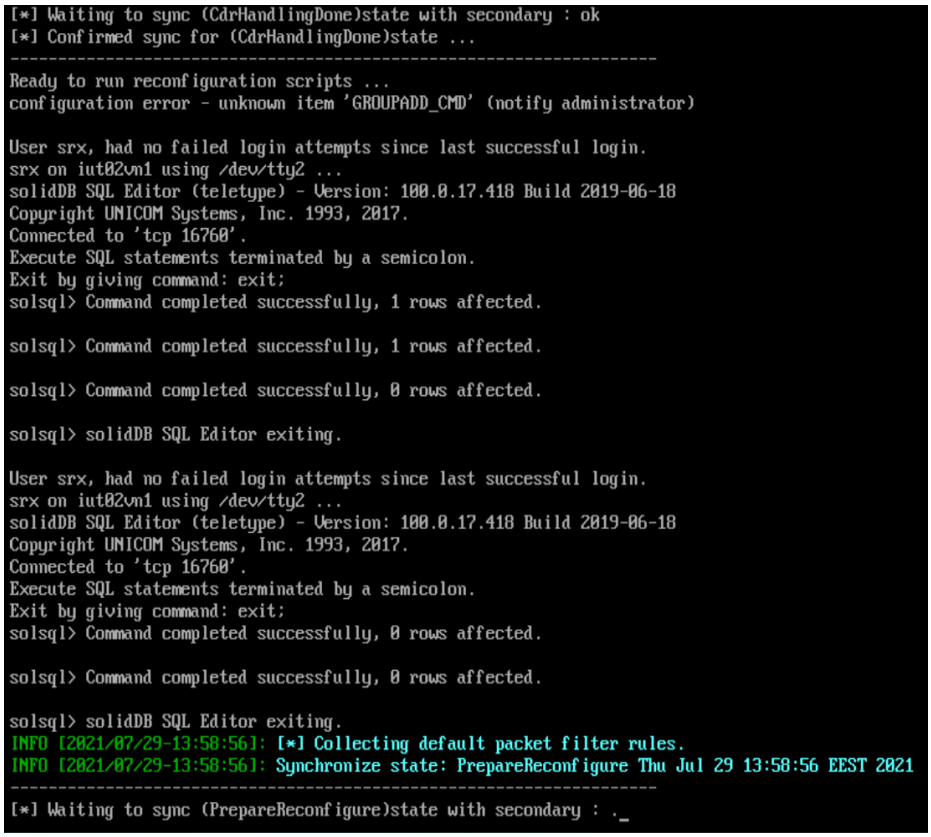


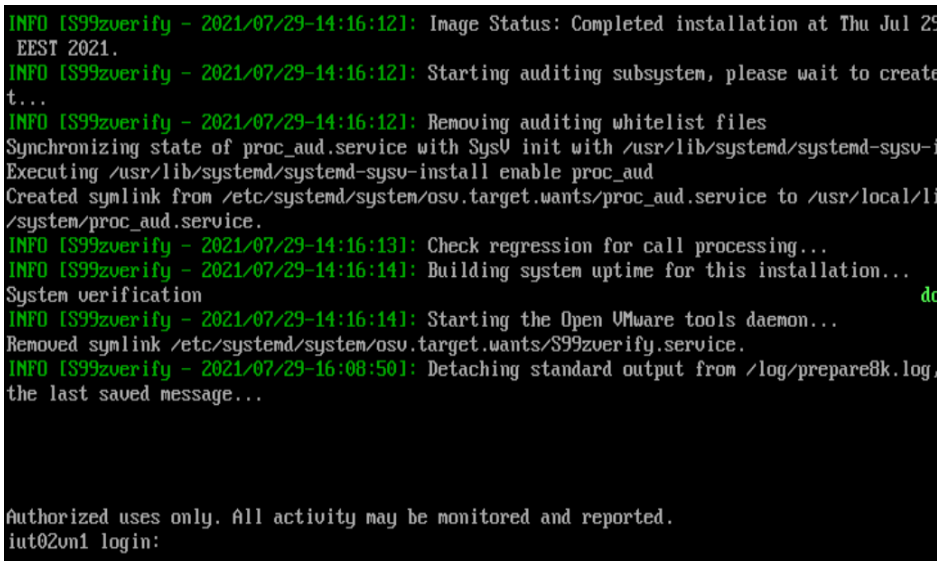
Installation starts. Wait for file system creation, checking and syncing of the image to target disk drive.



Networking is setup, cluster syncing is up and final re-configuration of the system is performed.


RBP52bBX0agmA13Fq4UM0XdaEQQ4Rrnwade8
grep: /etc/sec//setkey.conf: No such file or directory
Starting the RTP secure shell daemon
INFO [2021/07/29-11:50:19]: Routes
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 10.2.47.1 0.0.0.0 UG 0 0 0 eth0
10.2.47.0 0.0.0.0 255.255.255.224 U 0 0 0 eth0
10.2.47.0 0.0.0.0 255.255.255.224 U 0 0 0 eth0
INFO [2021/07/29-11:50:19]: Admin Ip: 10.2.47.6*, 10.2.47.7
INFO [2021/07/29-11:50:19]: X-Ch Ip: 10.2.47.6*, 10.2.47.7
INFO [2021/07/29-11:50:19]: Detecting active links.
- Link Detected on eth0 : yes/autoneg(off),10000Mb/s,Full.
- Link Detected on eth1 : no/autoneg(off),10000Mb/s,Full.
- Link Detected on eth2 : no/autoneg(off),10000Mb/s,Full.
- Link Detected on eth3 : no/autoneg(off),10000Mb/s,Full.
- Link Detected on eth4 : no/autoneg(),,.
- Link Detected on eth5 : no/autoneg(),,.
- Link Detected on eth6 : no/autoneg(),,.
- Link Detected on eth7 : no/autoneg(),,.
Kernel arp entries
Address HWtype HWaddress Flags Mask Iface
10.2.47.1 ether 28:ac:9e:48:1e:7b C eth0
INFO [2021/07/29-11:50:19]: Softswitch cluster interconnect tunnel :
Setting up SSH tunnel(Cluster Network) between 10.2.47.6 and 10.2.47.7.
This tunnel is setup on standard SSH port(#22).
Note: if there is no route between 10.2.47.6 and 10.2.47.7, calls through this tunnel will
also if the standard SSH port is unreachable, calls through this tunnel will block.





Installation is finished and logs/state are saved to archives in your USB drive under folder log or local under /log path.

Installation Log files

```
USB:

log/<DATE>_<TIME>_install.log.gz

log/<DATE>_<TIME>_install_tmpfiles.tar.gz


Openscape Voice system:

/log/<DATE>_<TIME>_install.log.gz

/log/<DATE>_<TIME>_install_tmpfiles.tar.gz

/log/prepare8k.log
```

At this point, the system will reach state 4 and should be ready for use.

OpenScape Voice V11 default users and passwords are:

Type	User	Password
Console	root	T@R63dis
Console	srx	2GwN!gb4
SFTP	cdr	MNY9$dta
SSH	sysad	1clENtk=
SSH	superad	BF0bpt@x
SSH	hipatham	kH3!fd3a
SSH	hipathcol	jO3(fdqA
SSH	secad	$ECur8t.
SSH	dbad	d8$ECur.
SSH	webad	!WE8saf. **(for Simplex configurations only)**

Table 7 Default User Passwords

Users "sysad", "superad", "secad", "dbad" and "webad" have 90 day expiry limits set on their passwords. Unless restricted by the /etc/security/access.conf file, all users have access to the OSV via the console also.

Note: If your OpenScape Voice system was Upgraded or migrated to OpenScape Voice V11, then you have maintained the expiry data of the source release. This means the "sysad", "superad". "secad" and "dbad" userid passwords will never expire. For password management advice please refer to Section 17.2.2, “Password Management”, on page 617.

The following table provides the default passwords for Solid Users.

User	Password
dba	dba
rtp	RTP_USER
sym	sym **(for Simplex configurations only)**

Table 8 Default Passwords for Solid Users

16. After the installation is complete, verify the success of the installation by logging in as user *root* and execute the following commands:

```
# cd /unisphere/srx3000/srx/startup
# ./srxqry -v
```

A successful software installation is indicated if the nodes (or node) are at run level 4 (RTP and application running with all processes started and in PROCESS_READY state).

Note: If the installation process stops prematurely or if the nodes (or node) do not reach run level 4, this is an indication of a failed installation.

The installation logs are kept on the USB memory stick in the *install.log* file. The hardware information for the platform in progress is also placed on the USB memory stick in the *current.hwinfo* file.
Regardless of installation success or failure, save the contents of the memory stick(s) onto a backup server/device for future reference or diagnostic purposes.

---

17. As user *srx*, verify that the software is at the patch set level listed in the OpenScape Voice V11 release note with the command:

```
pkgversion -ps or pkgversion -f
```

Attention: Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability. An integrated system should ensure that the applications server is updated with the latest released DVD/PatchSet/HotFix.

If the patch set level is not correct, install the corresponding patch sets using the CMP/Assistant (after installing the OpenScape Applications for a standard duplex).

18. As user *root*, verify that the system is an imaged system with the command:

```
rpm -qa | grep UNSPxtree
```

Verify that `UNSPxtree-2.0-1.x86_64` is displayed.

Note: If you were sent to this section from an upgrade or migration procedure, return to the upgrade or migration procedure rather than going to the OpenScape Voice Installation Checklist.

---

19. On the OpenScape Voice Installation Checklist in Section 2.2.4 on page 30, initial step 8 and proceed to step 9.

4.2.3.2 Image installation/System Restore USB/Service System Image Write

The **OpenScape Voice Service System USB Setup Wizard** is a graphical wizard for setting up the USB Flash Drive user data for the operations of Image Install and System Restore. The procedure described below can substitute steps 3 - 6 in Section 4.2.3.1, “Physical systems via USB”. The number of USB drives attached to the host system, determines the scenario of clustered systems. Attaching only one USB drive, the tool will allow a setup of a Simplex OSV system only.

1. Attach the USB drive or USB drives
2. Select the operation you wish to perform:
   - Service System Image Write
   - Image Installation
   - System Restore

Service System Image Write

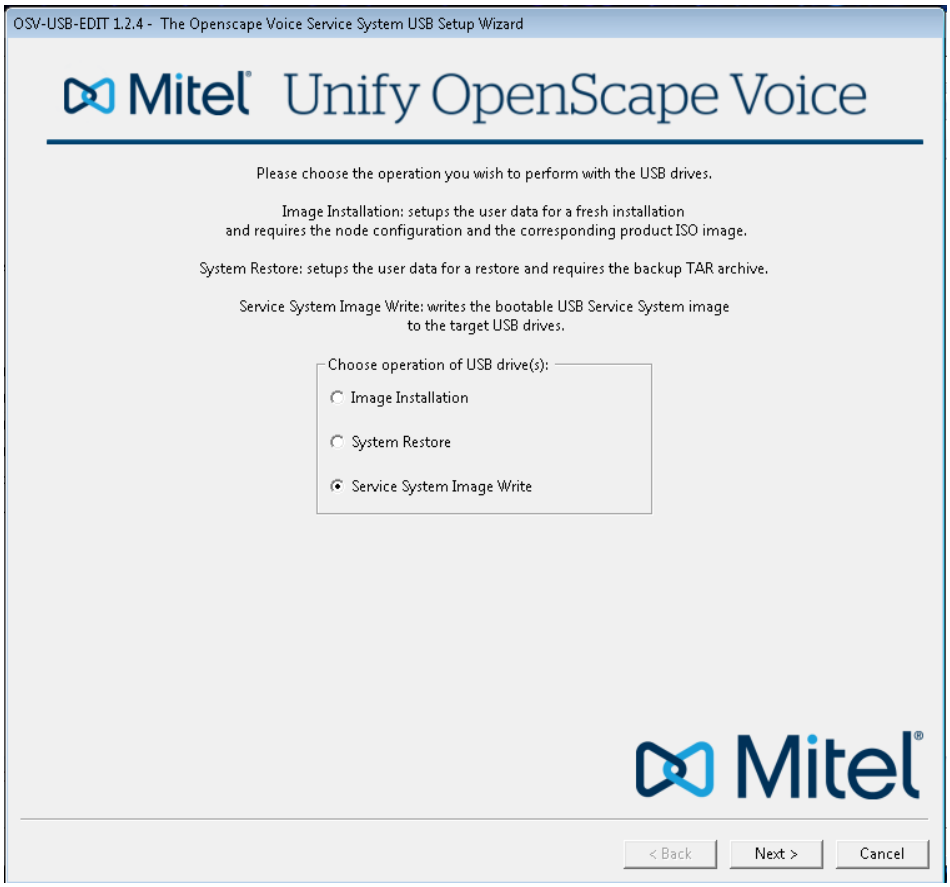


Figure 1 "Service System Image Write" option

1. Attaching a single USB drive, you get an **One Node** (Simple or Duplex) option. Attaching two USB drives, you get **Both Nodes** (Duplex Only) option. Click **Next**.

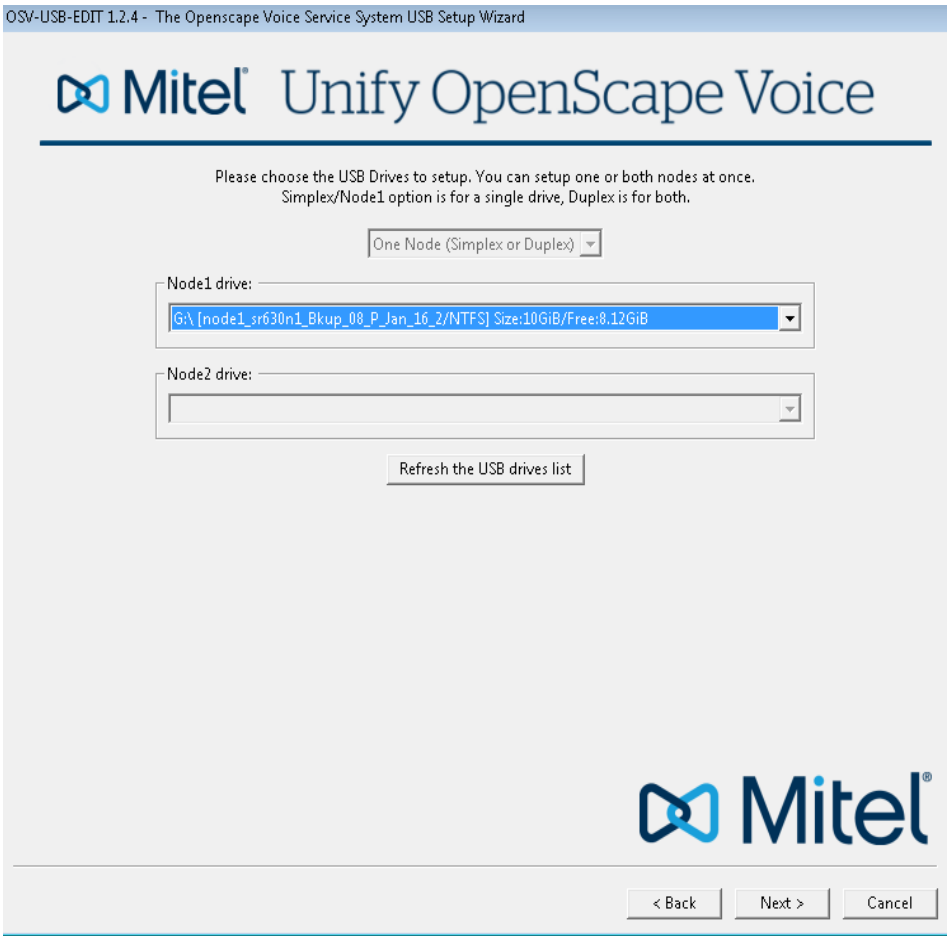


Figure 2 One Node option

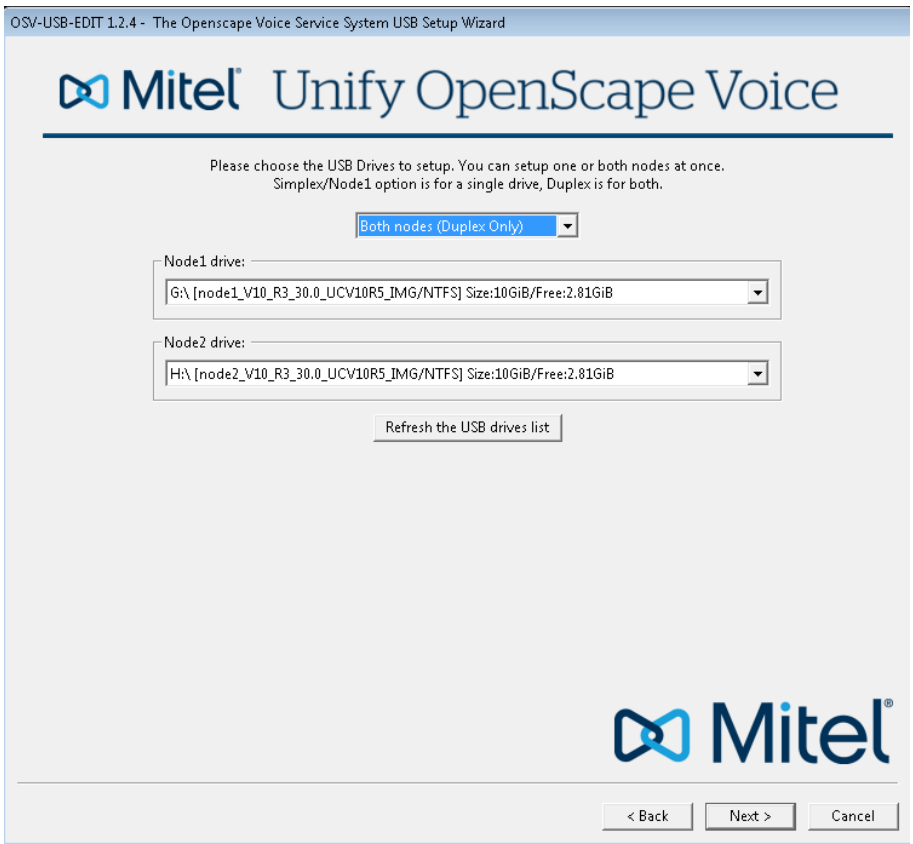


Figure 3 Both Nodes option

2. Click **Browse** to select the ISO image from your system.
3. Once the file is selected, click **Write**, to start writing the `.img` file to your USB drive(s).

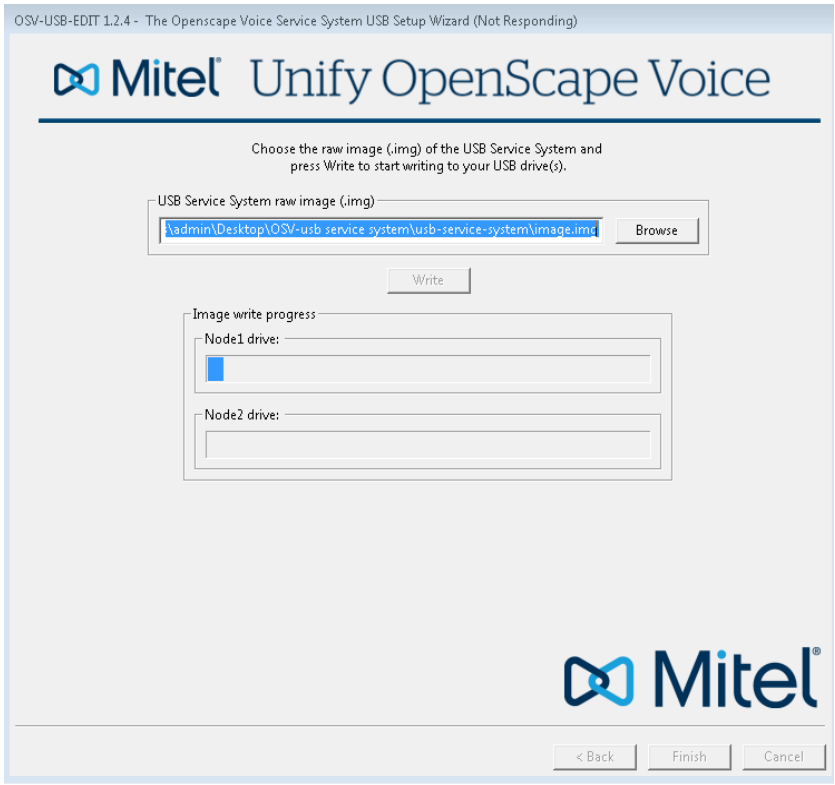


Figure 4 Writing .img file into usb drive(s)

4. The iso has been written successfully. Click **OK** and **Finish**.

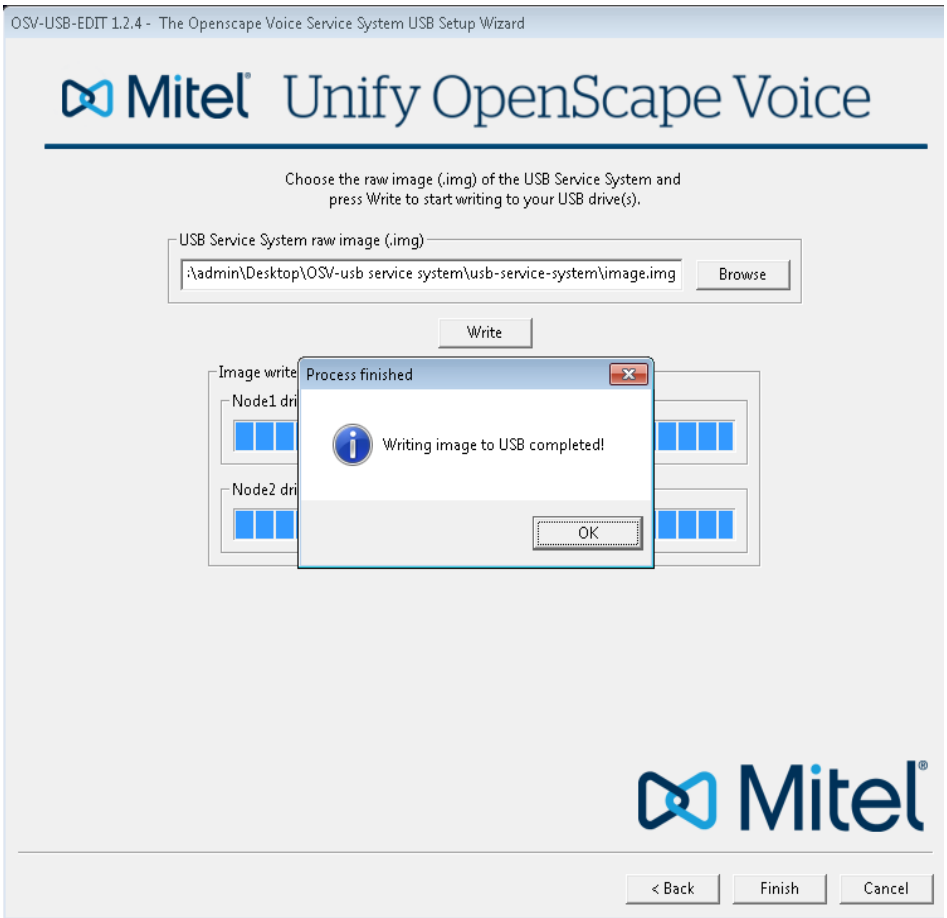


Figure 5 Writing image to USB completed

Image installation

Attaching a single USB drive, you get an **One Node (Simplex or Duplex)** option. Attaching two USB drives, you get **Both Nodes (Duplex Only)** option. Click **Next**.

Figure 6 One Node option

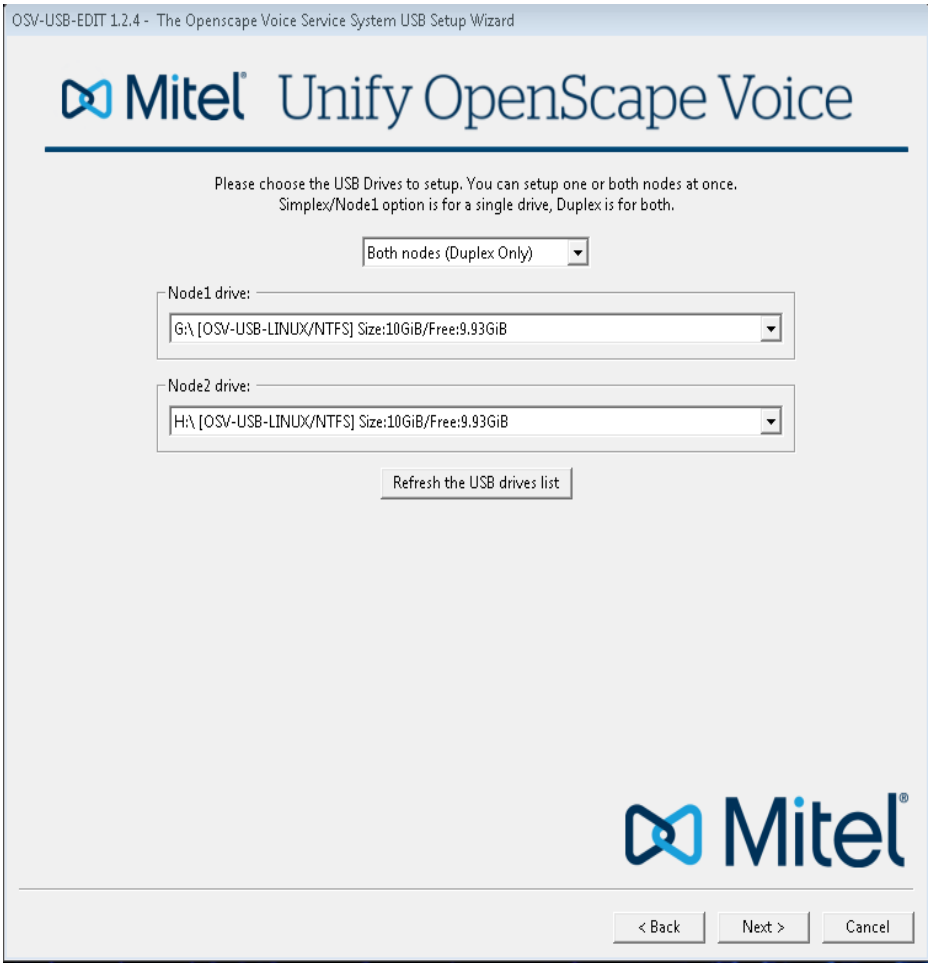


Figure 7 Both Nodes option

5. Click **Browse** to select the `node.cfg` file and the ISO image from your system.

   Once the two files are selected, decide whether to include Patchsets and/or License. Check the **Include Patchsets** checkbox and click the **Browse** button to select the Patchset zip file from your system. Perform the same actions for the License.

Figure 8 Patchset / License

6. Check that the correct files have been selected and click **Apply**.

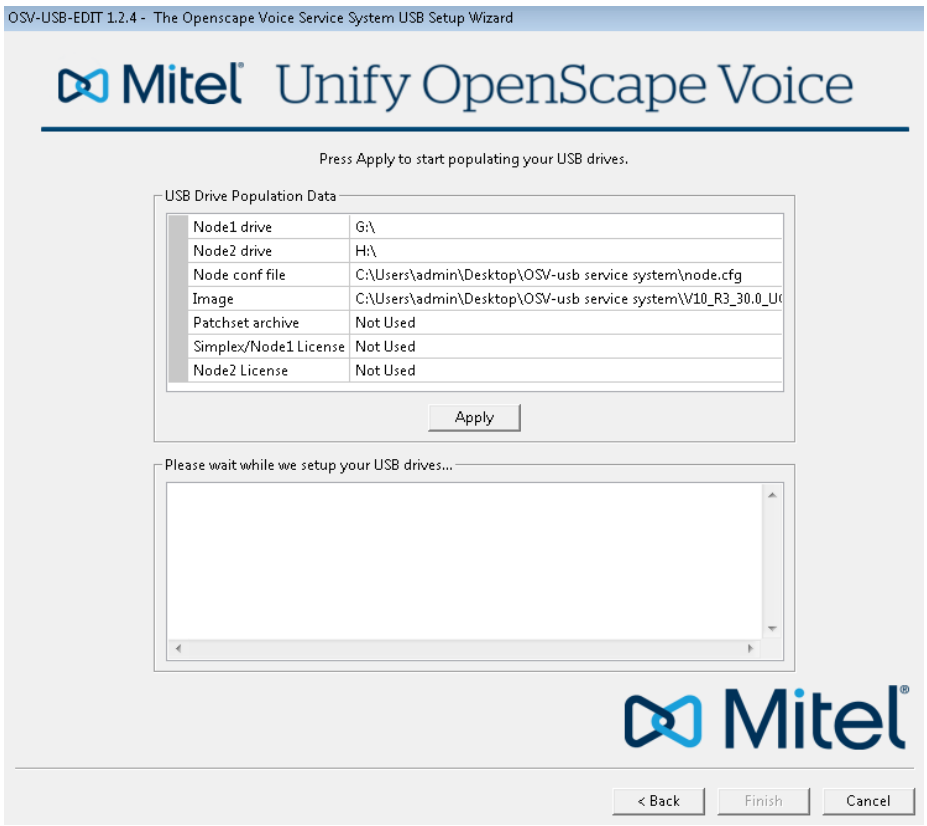


Figure 9 Process Data

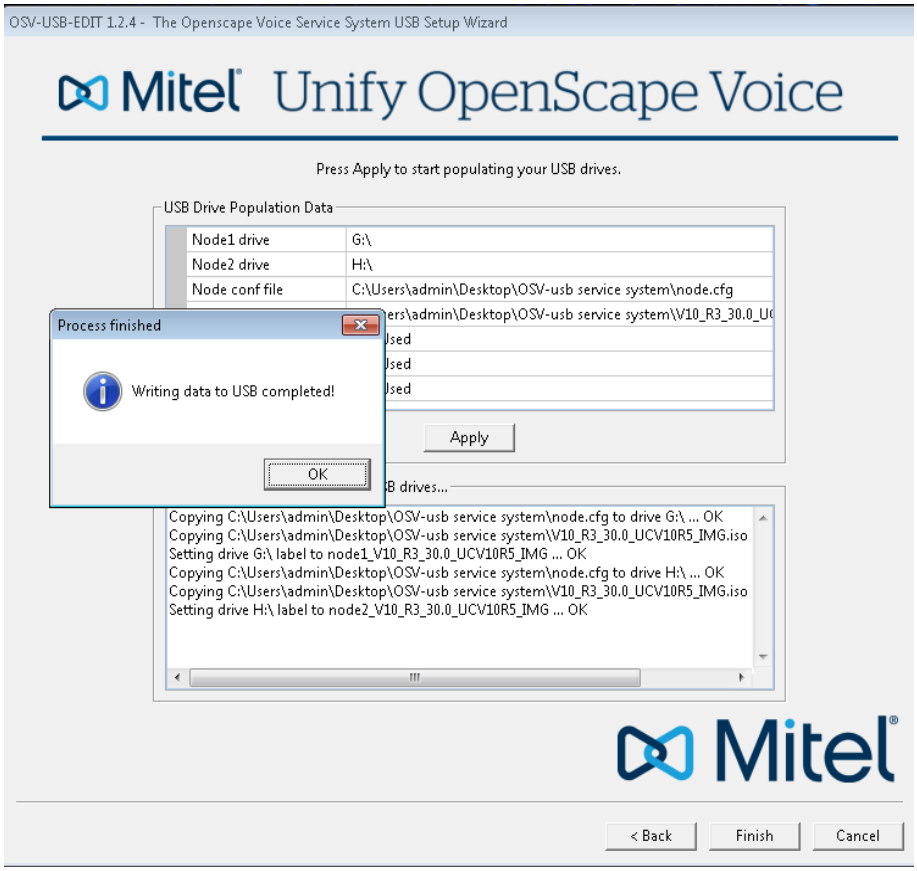


Figure 10 Process data success

7. Data is saved in the drives and the drive labels are updated.

Continue with step 6 in Section 4.2.3.1, “Physical systems via USB”

System Restore USB

1. After selecting **System Restore**, click **Next**.
2. Select the **USB Drives** to setup. Choose one or both nodes.

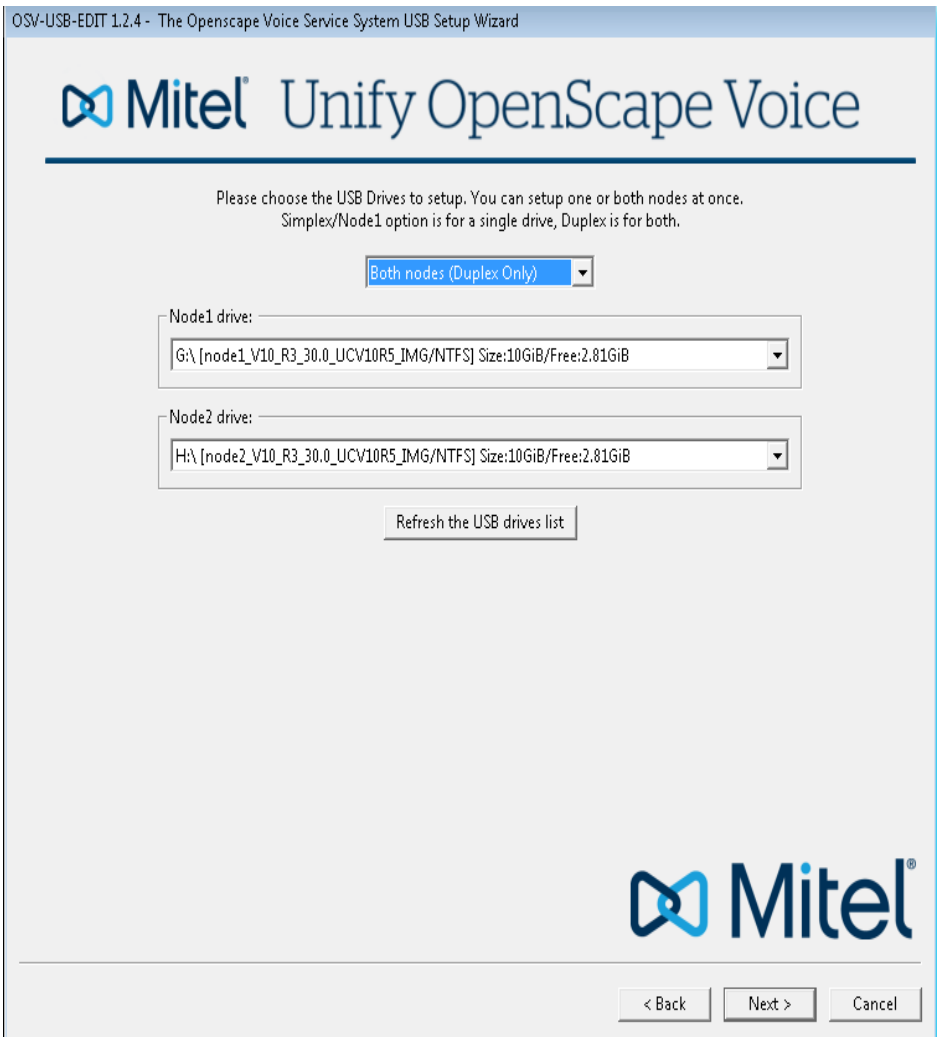


Figure 11 Choose the USB Drives to setup

3. Click **Browse** to select the backup tar file from your system. The backup archive filename is important here.

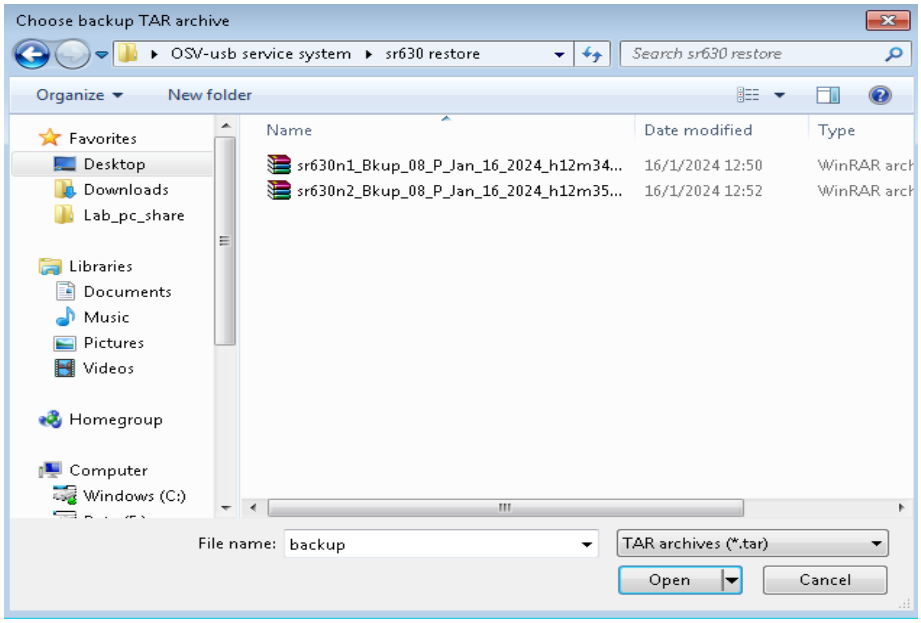


Figure 12 System Backup restore file

4. Click **Open**.
5. Check that the correct file has been selected and click **Apply**.

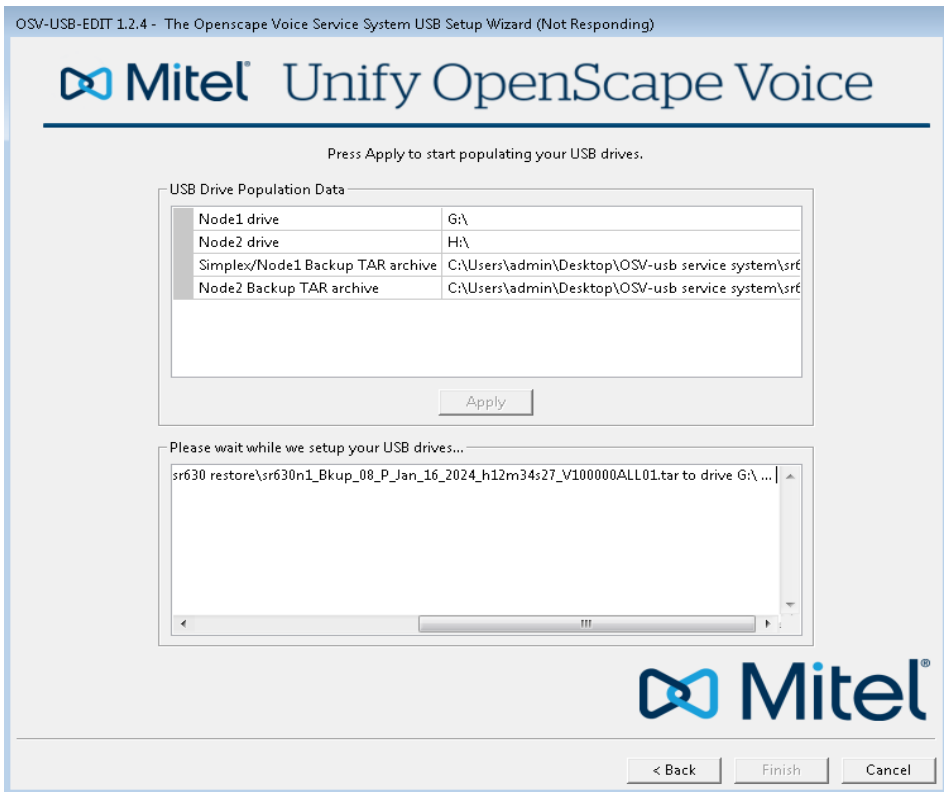


Figure 13 Process Backup tar

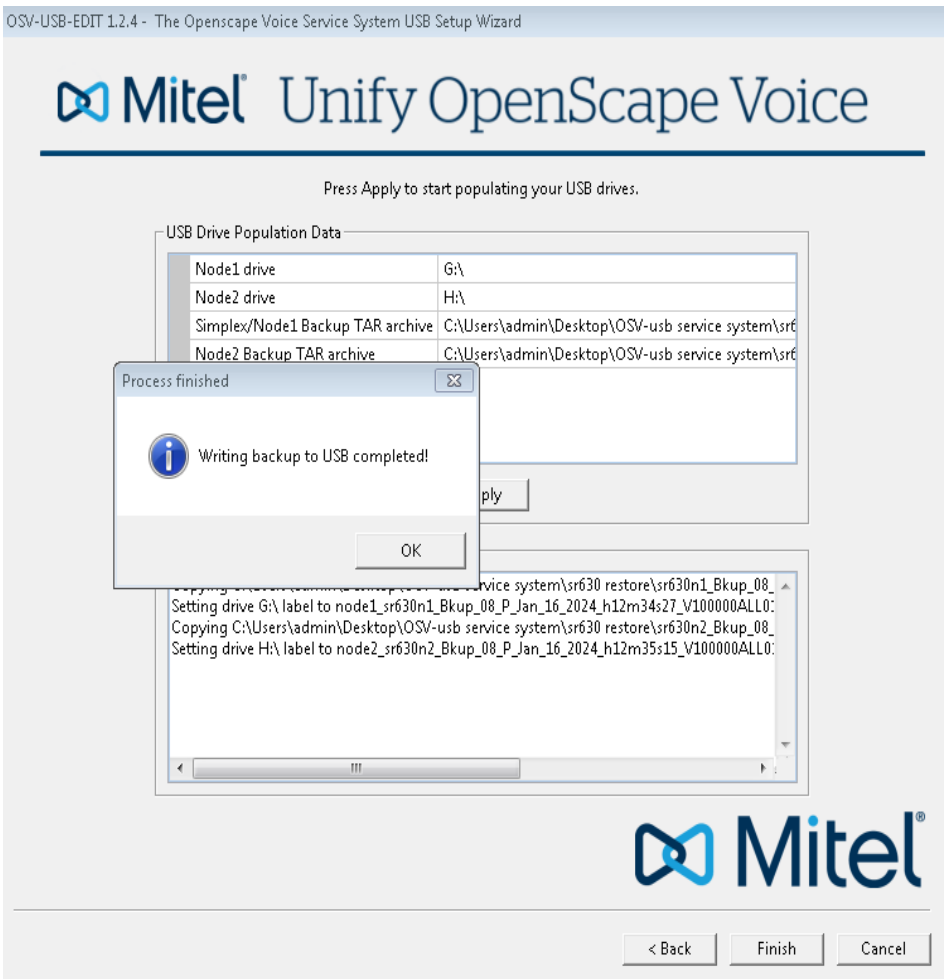


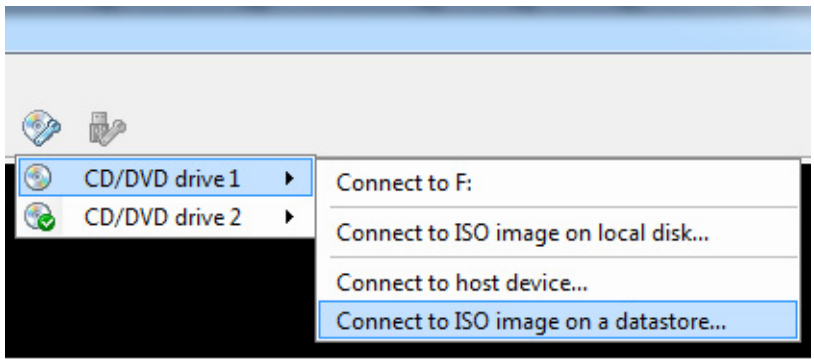
Figure 14 Process Backup tar success

6. The archives are saved to the drive(s) and the labels are updated.

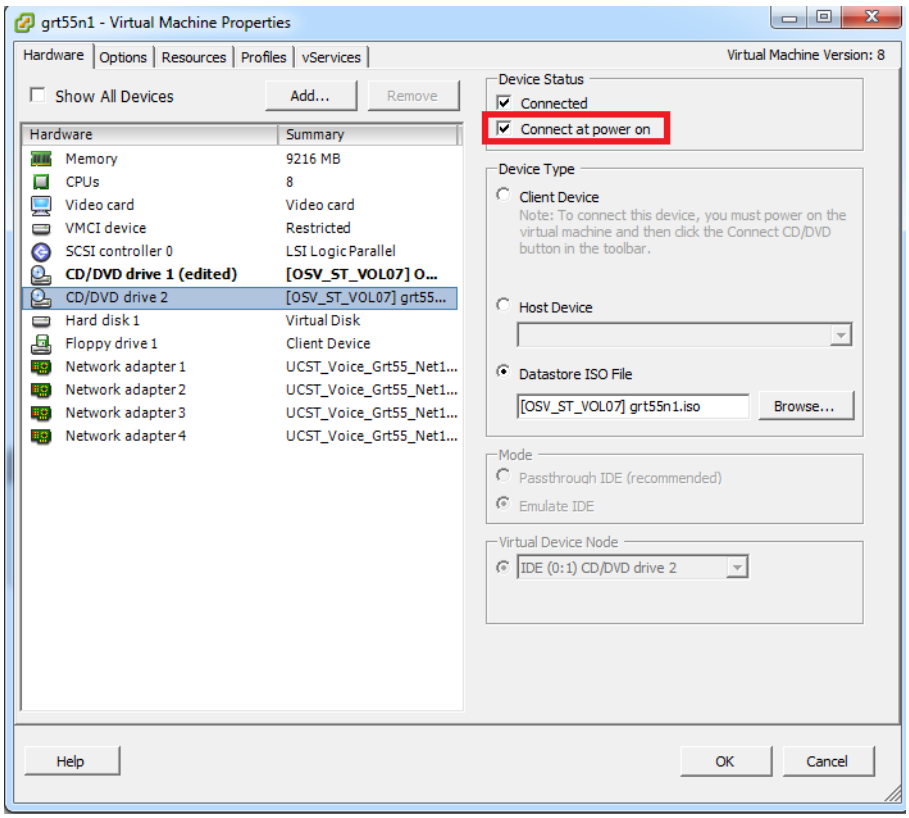
4.2.3.3 Virtual systems via Virtual CD/DVD

Attention: Make sure that the whole process described in Section 4.3, “Virtualization Environment Setup” has already been implemented.

1. Connect the image ISO file to the CD/DVD Drive 1



or



2. Connect the device that contains the `node.cfg` file;

   - Follow step 2a if the node.cfg has been saved to a Virtual Floppy File. Refer to Section 4.3.4.3, “Creating a Virtual Floppy Disk”

     Note: For Node A or Integrated Simplex Rename the `node.cfg` file as **node.cfg.primary**. If this is a duplex OSV, make another copy of the `node.cfg` named **node.cfg.secondary**.

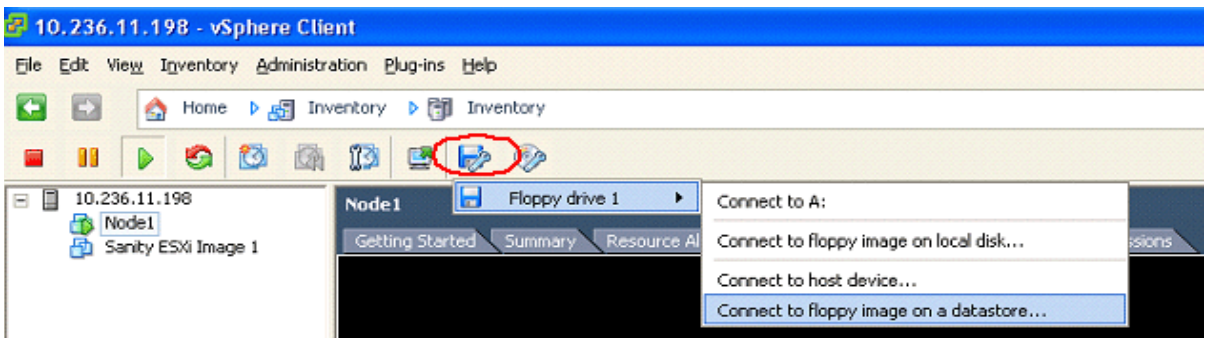
   - Follow step 2b if the node.cfg (and patchsets) has been saved to a Installation ISO Image. Refer to Section 4.3.4.2, “Saving the node.cfg, license and patch sets to an Installation ISO Image”

     Note: For Node A or Integrated Simplex Rename the `node.cfg` file as **node.cfg.primary**. If this is a duplex OSV, make another copy of the `node.cfg` named **node.cfg.secondary**.

   a) Follow this step if the node.cfg has been saved to a Virtual Floppy File.

      Attention: If the node.cfg (and patchsets) have been saved to a Installation ISO Image, skip step 7a and proceed to step 7b.

      - Exit VM capture (**CTRL+ALT**),
      - Click on the floppy icon on the vSphere UI.
      - Choose the **Floppy Drive** icon and from its sub-menu select “Connect to floppy image on a datastore…” as shown below:

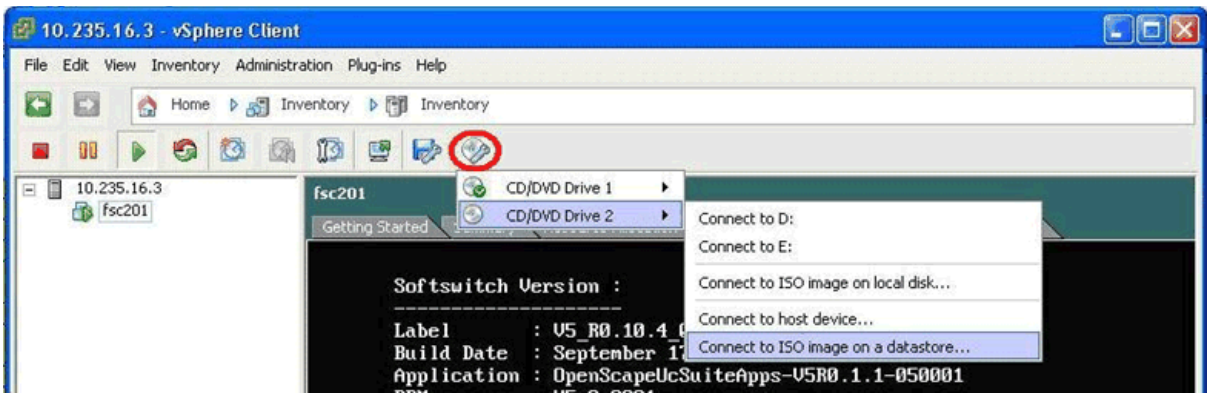


      - **Now proceed to step 3.**

b) Follow this step if the node.cfg (and patchsets) have been saved to a Installation ISO Image.
After step 7b is complete proceed to step 3.

Attention: If the node.cfg has been saved to a Virtual Floppy Files follow step 7a.

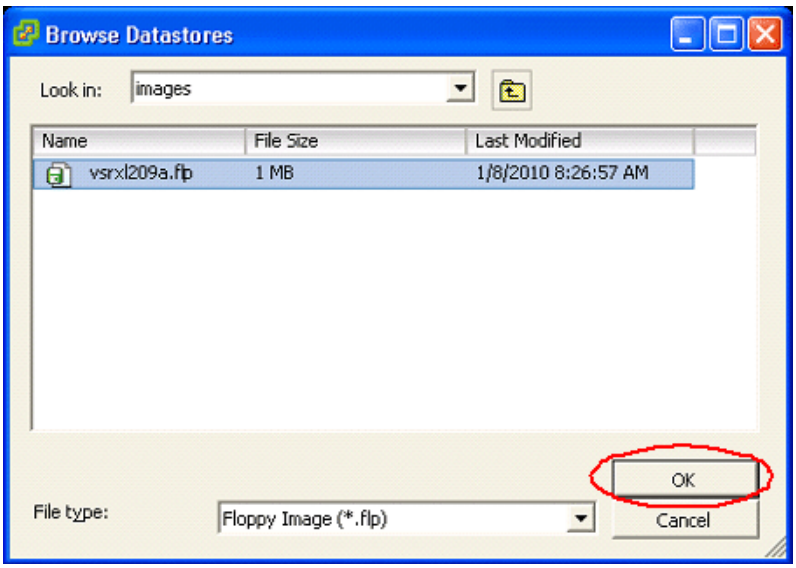
- Exit the VM console capture (CTRL+ALT),
- Click on the CD/DVD icon, select CD/DVD Drive 2 and from its sub-menu select “Connect to ISO image on a datastore…” as shown below:



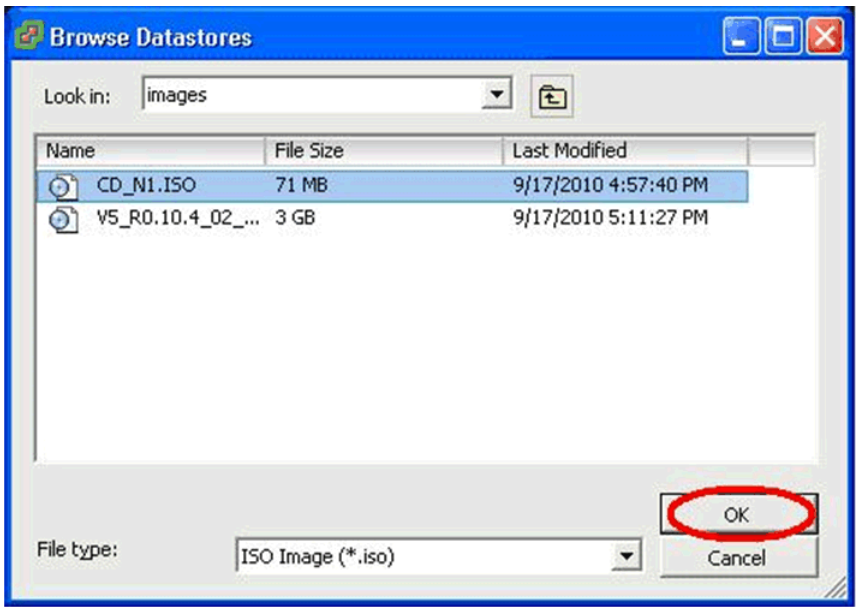
- **Now proceed to step 3.**

3. Navigate the datastore to the Virtual Floppy file or Installation ISO file. Choose the appropriate file and select **OK** (two example snapshots follow).

   Virtual Floppy file selection;



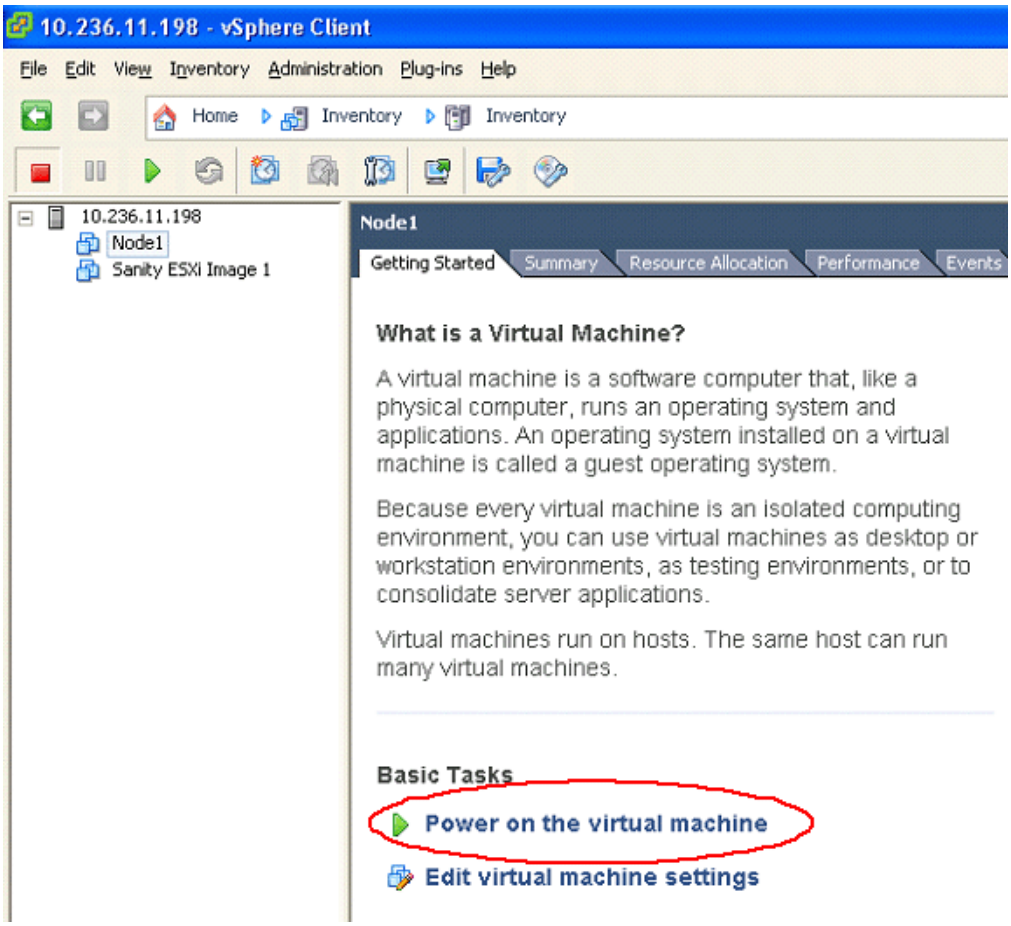
Installation ISO file selection;



Attention: Before starting the virtual machines, make sure that the virtual CD/DVD Drive 1 and CD/DVD Drive 2 (or virtual Floppy) are connected. Otherwise node.cfg file cannot be detected.

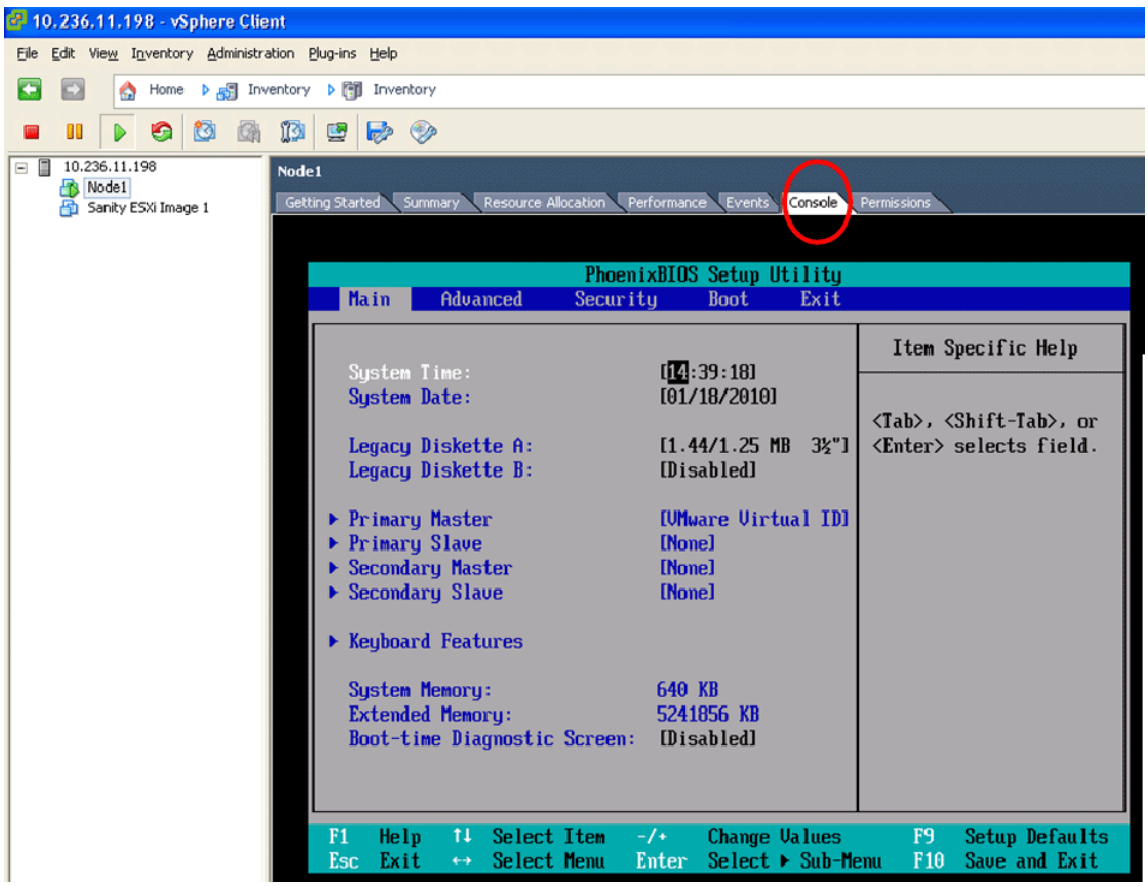
---

4. Power on the guest machines just created.

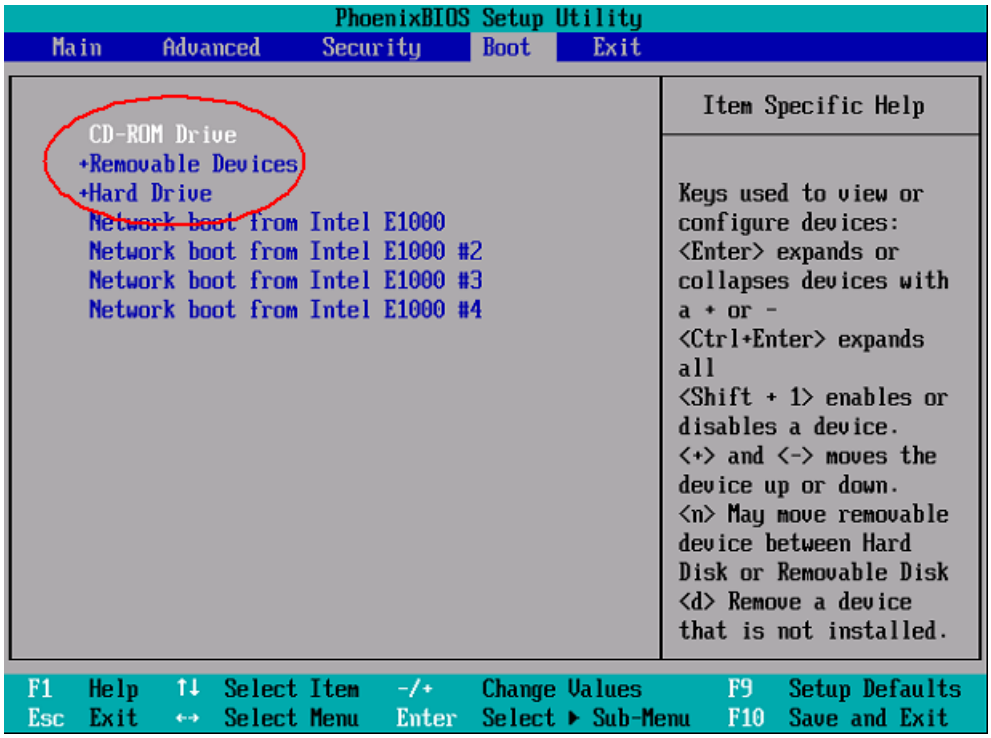

10.236.11.198 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.236.11.198
Node1
Sanity ESXi Image 1
Node1
Getting Started Summary Resource Allocation Performance Events
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.
Virtual machines run on hosts. The same host can run many virtual machines.
Basic Tasks
Power on the virtual machine
Edit virtual machine settings

5. Open up the vSphere Client's **Console** tab, click in the console window and hit return to connect to the guest Linux environment OSV will run in. At this point the BIOS screen should appear. Verify/update the System Date and Time.

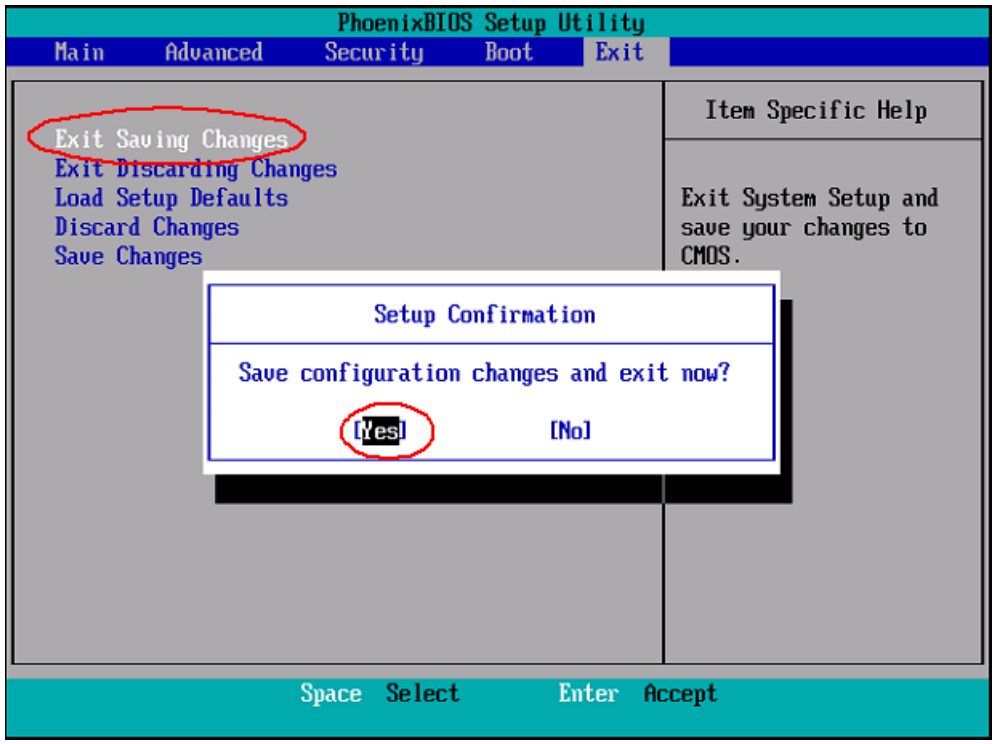
Note: To switch between the WMware console window and desktop environments;
- click into the Console window to enter the Console.
- '**CTRL-ALT**' will leave the Console.



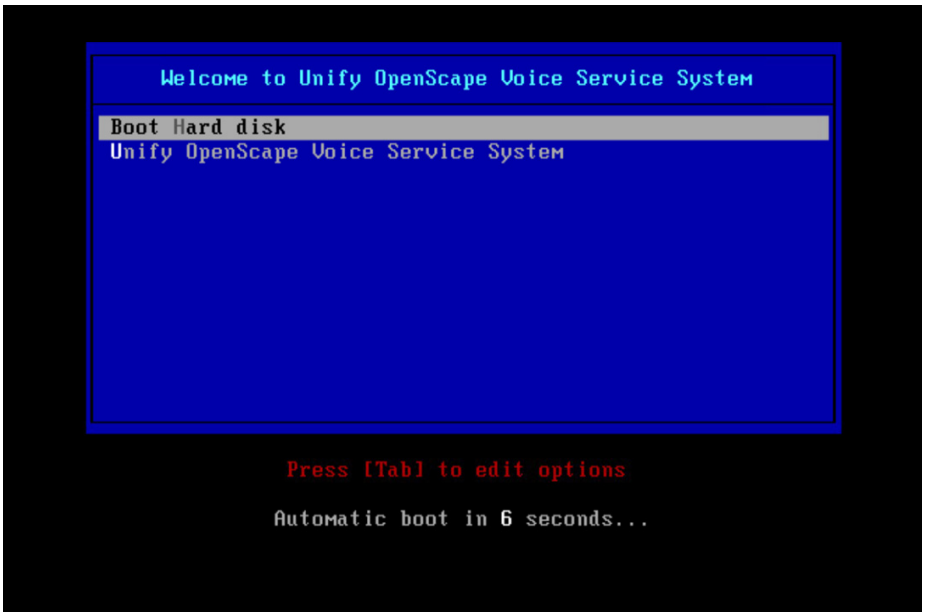
6. Select the BIOS screen's **BOOT** tab and move the CD ROM to the top of the list and the Floppy to the second position.



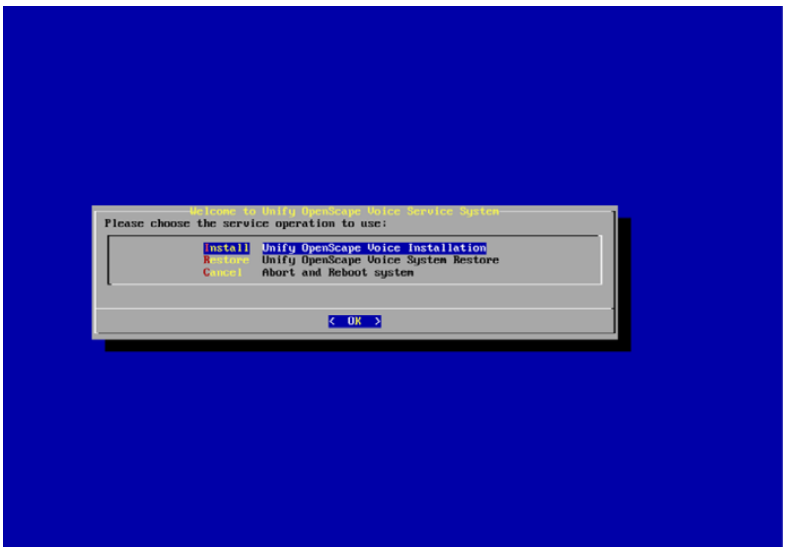
7. Press the **Esc** key to exit this menu, then select **Exit Saving Changes**. In the Setup Confirmation window select **Yes** to “Save configuration changes and exit now?”.



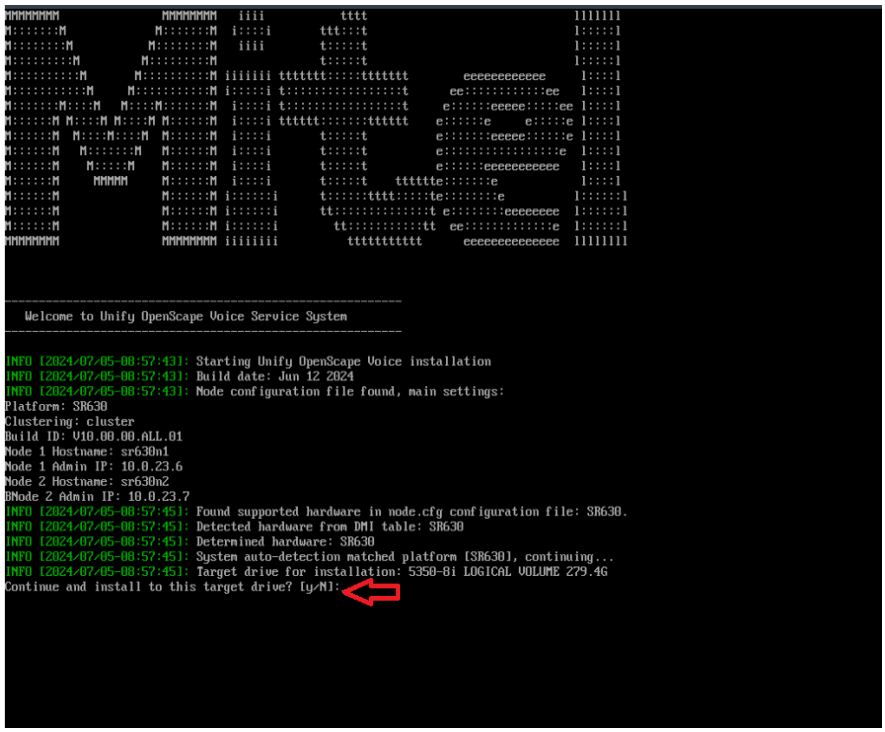
8. In the menu presented after boot, select **Unify OpenScape Voice Service System**



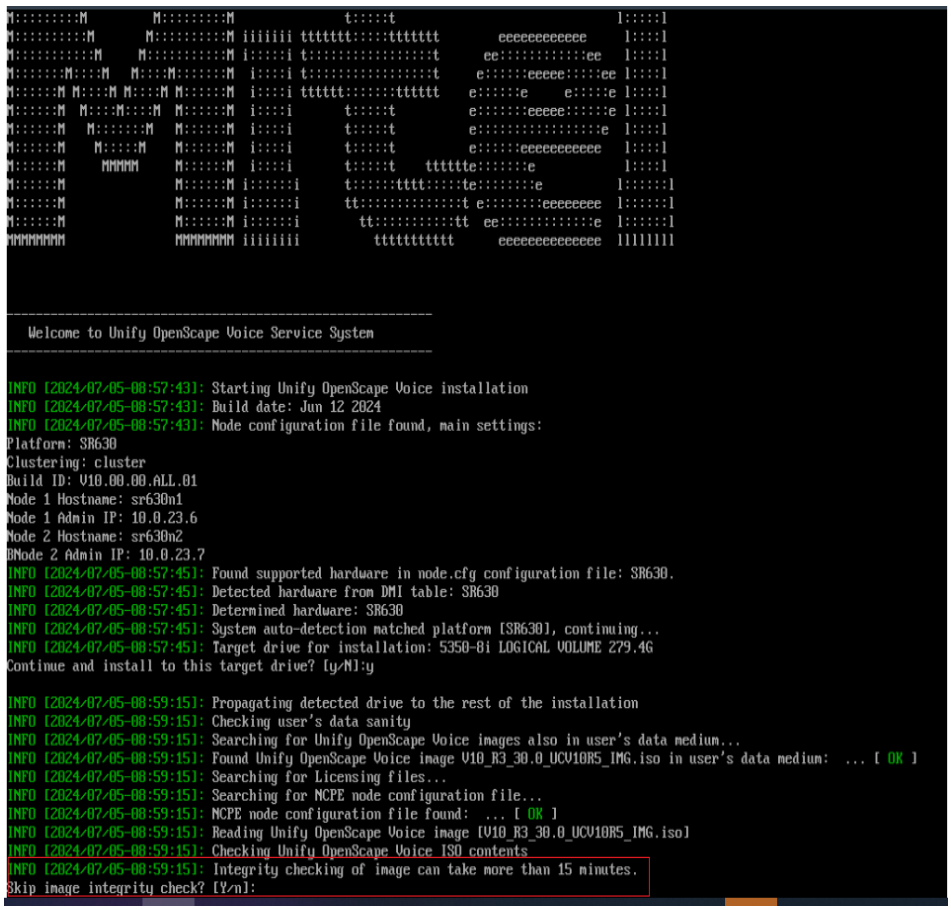
9. Select **Install Unify OpenScape Voice Installation** and press **OK**



Target disk drive for installation detected and data files found and checked.



10. When you want to perform Integrity Check, select **No.** The default value is **Yes** and the Integrity Check will be skipped. The Integrity Check will take more than 15 min.



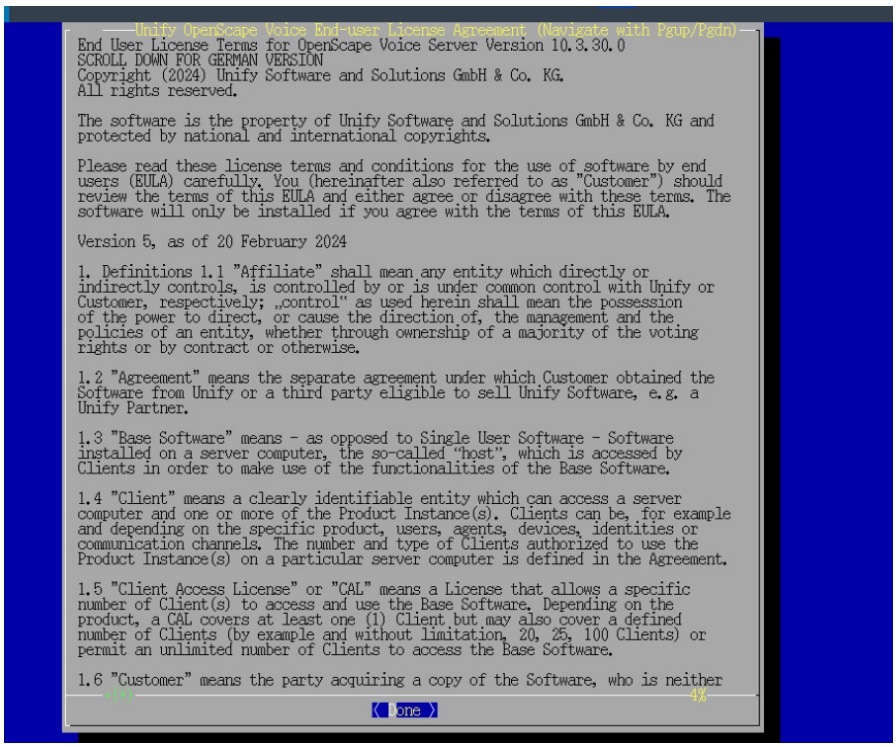
11. Accept EULA (End User License Agreement)
    The End User License Agreement (EULA) is displayed in a new window on the console screen. Review and accept the EULA as follows:

    a) Review the EULA using the Page Up/Page Down or arrow keys; when you are finished reviewing the EULA, select **Done** and press the **Enter** key.

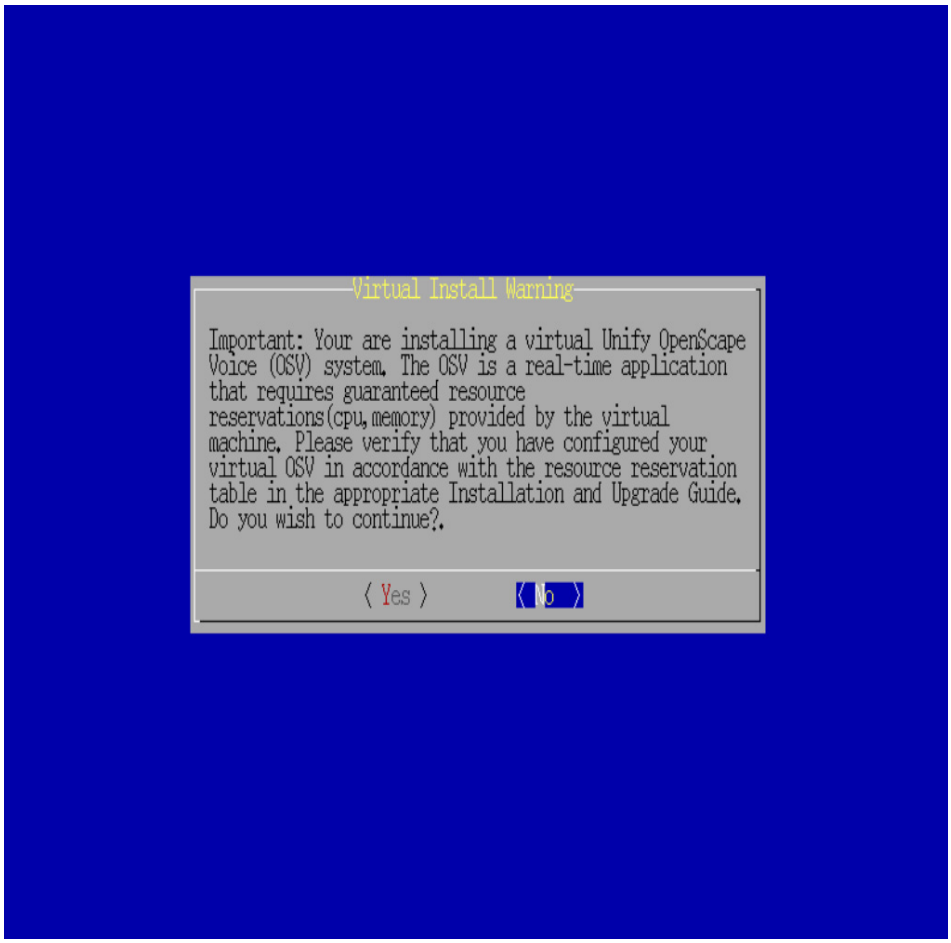
    b) A window is opened with the question: "**Do you accept the License Agreement?**" with the options '**Yes**' and '**No**'

    c) In the EULA acceptance window, use the Tab or arrow keys to select **Yes** to proceed with the image installation. Selecting '**No**' will halt the image installation.

    d) If you select '**No**' by mistake, to continue with the image installation, reboot the server and when prompted to accept the EULA, select **Yes**.



12. Verify that the virtual OSV specifications are in accordance with the resource reservation described in Section 4.3, “Virtualization Environment Setup”



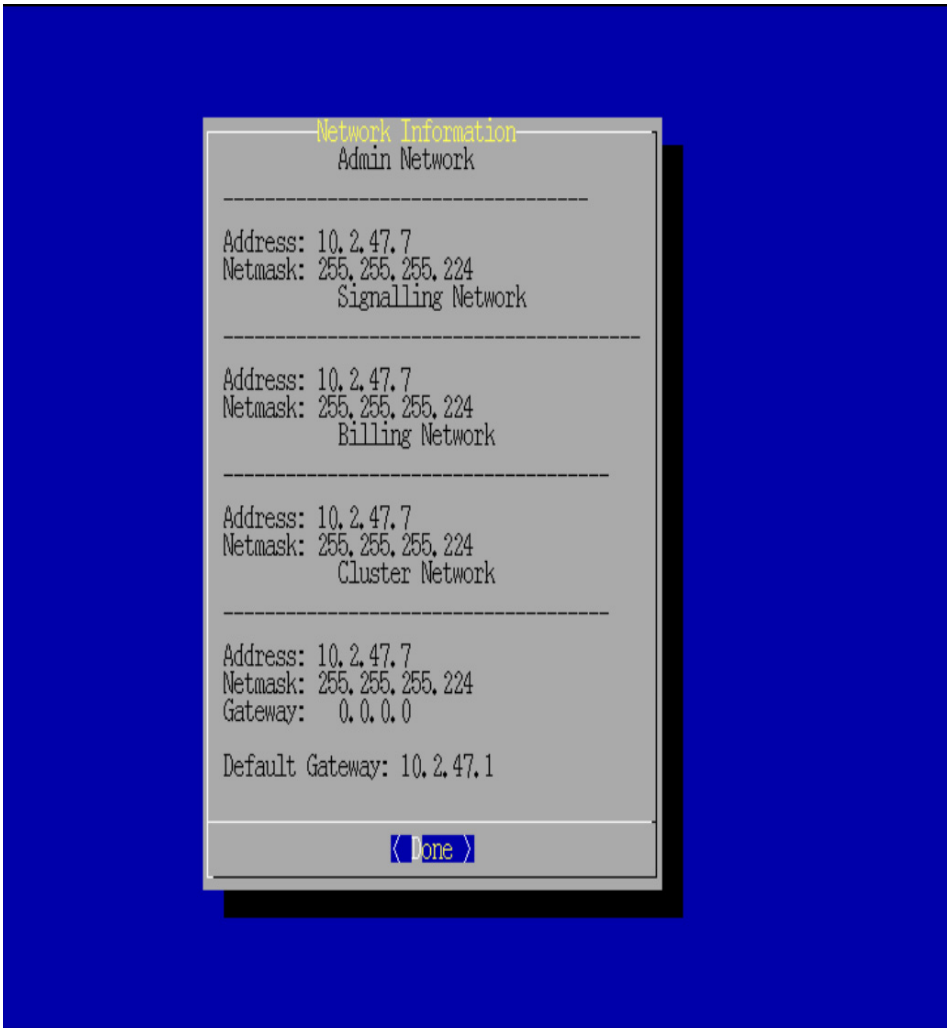
Select **Yes.**

13. Type **yes** and press enter as shown below and the Image installation will start.

    - Repeat steps 9 through 12 of Section 4.2.3.3 for Node 2; making sure to select the appropriate virtual floppy which contains the node.cfg.secondary.

    Note: For specific details of the Image installation please refer to the Release Notes of the Image.

14. Press **Done** on the **Network Information** page, which is displayed as soon as the appropriate Virtual Floppy with the node.cfg is mounted.



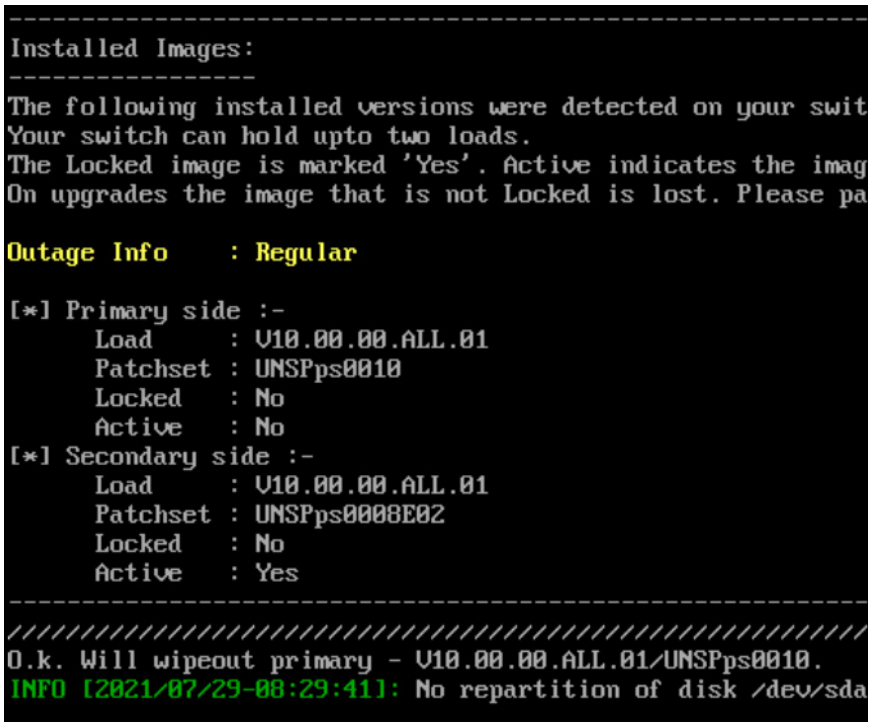
15. When prompted, select the installation scenario: `yes/no/format/lockprim/locksec/verify`

Note: Typing yes or format will erase all data from unlocked partition on the disk.

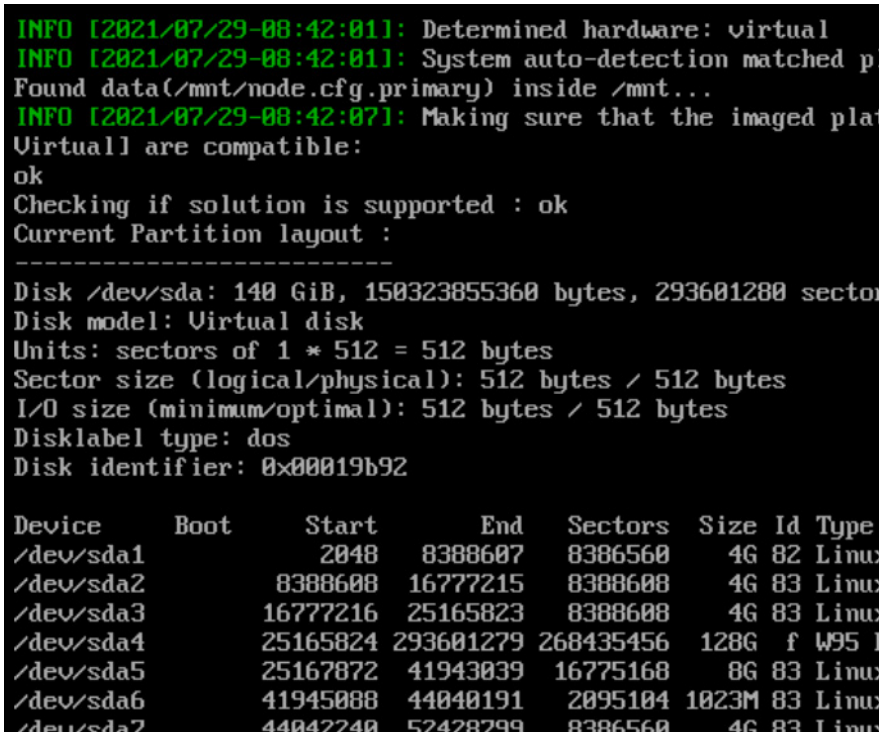
- **yes** - Erases data from the first unlocked image.
- **no** - Aborts installation.
- **format** - Reformats harddisk, user loses all the data
- **lockprim** - Erases data from the secondary partition
- **locksec** - Erases data from the primary partition
- **verify** - Verify hardware

```
Do you want to continue with installation (enter yes/no/
format/lockprim/locksec)?
```

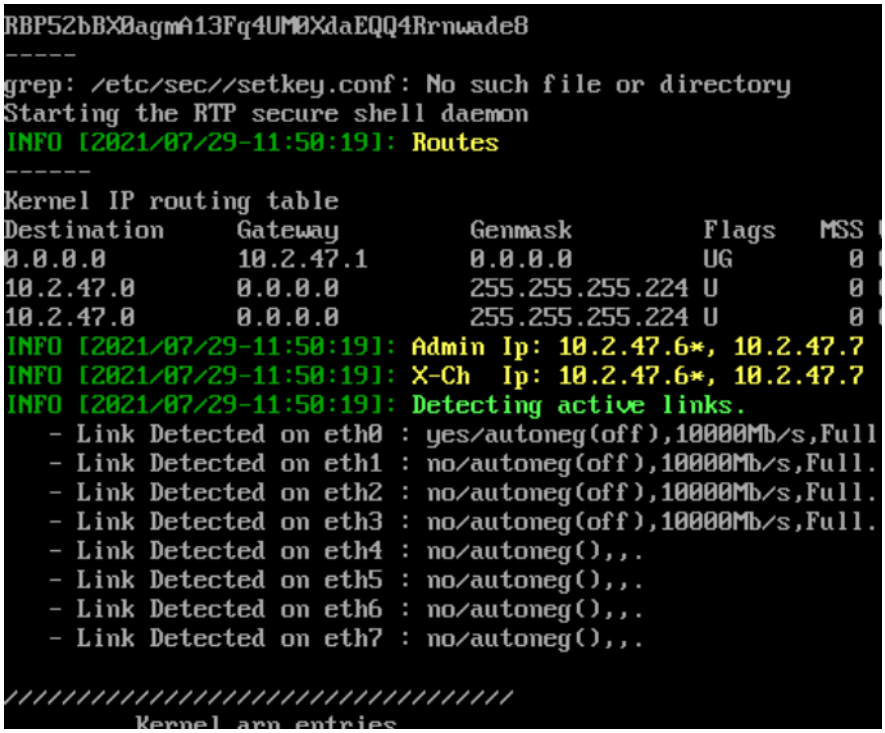
Note: Format and repartition are necessary for fresh installation.

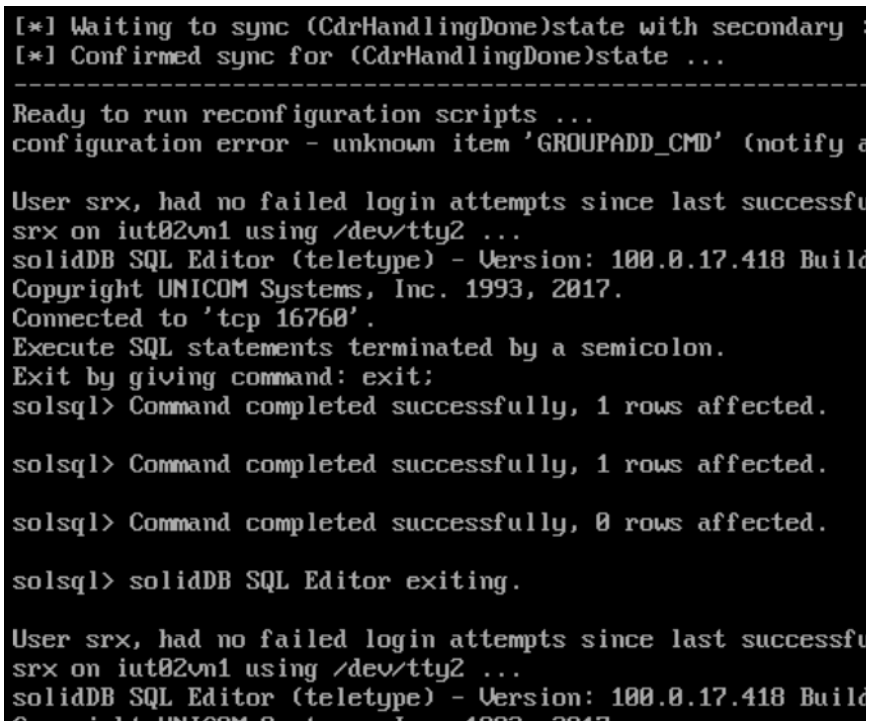


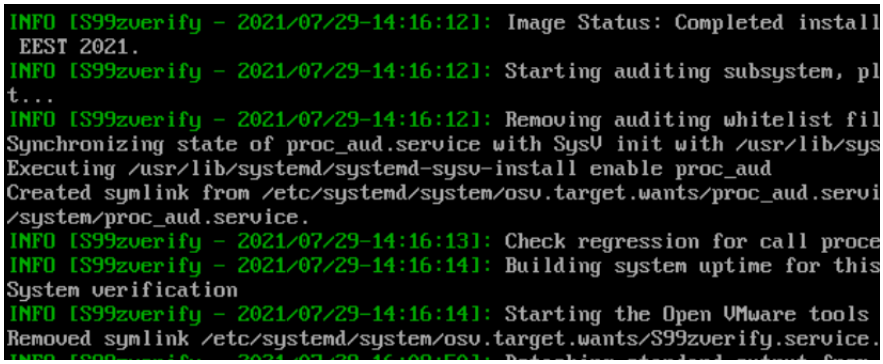
Installation starts. Wait for filesystem creation, checking and syncing of the image to target disk drive.



Networking is setup, cluster syncing is up and final reconfiguration of the system is performed.


RBP52bBX0agmA13Fq4UM0XdaEQQ4Rrnwade8
grep: /etc/sec//setkey.conf: No such file or directory
Starting the RTP secure shell daemon
INFO [2021/07/29-11:50:19]: Routes
Kernel IP routing table
Destination Gateway Genmask Flags MSS
0.0.0.0 10.2.47.1 0.0.0.0 UG 0
10.2.47.0 0.0.0.0 255.255.255.224 U 0
10.2.47.0 0.0.0.0 255.255.255.224 U 0
INFO [2021/07/29-11:50:19]: Admin Ip: 10.2.47.6*, 10.2.47.7
INFO [2021/07/29-11:50:19]: X-Ch Ip: 10.2.47.6*, 10.2.47.7
INFO [2021/07/29-11:50:19]: Detecting active links.
- Link Detected on eth0 : yes/autoneg(off),10000Mb/s,Full
- Link Detected on eth1 : no/autoneg(off),10000Mb/s,Full.
- Link Detected on eth2 : no/autoneg(off),10000Mb/s,Full.
- Link Detected on eth3 : no/autoneg(off),10000Mb/s,Full.
- Link Detected on eth4 : no/autoneg(),,.
- Link Detected on eth5 : no/autoneg(),,.
- Link Detected on eth6 : no/autoneg(),,.
- Link Detected on eth7 : no/autoneg(),,.


[*] Waiting to sync (CdrHandlingDone)state with secondary
[*] Confirmed sync for (CdrHandlingDone)state ...
Ready to run reconfiguration scripts ...
configuration error - unknown item 'GROUPADD_CMD' (notify
User srx, had no failed login attempts since last successfu
srx on iut02vm1 using /dev/tty2 ...
solidDB SQL Editor (teletype) - Version: 100.0.17.418 Build
Copyright UNICOM Systems, Inc. 1993, 2017.
Connected to 'tcp 16760'.
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;
solsql> Command completed successfully, 1 rows affected.
solsql> Command completed successfully, 1 rows affected.
solsql> Command completed successfully, 0 rows affected.
solsql> solidDB SQL Editor exiting.
User srx, had no failed login attempts since last successfu
srx on iut02vm1 using /dev/tty2 ...
solidDB SQL Editor (teletype) - Version: 100.0.17.418 Build



Installation is finished and logs/state are saved to archives in your USB drive under folder log or local under /log path.

Installation Log files

`Openscape Voice system:`

`/log/<DATE>_<TIME>_install.log.gz`

`/log/<DATE>_<TIME>_install_tmpfiles.tar.gz/log/prepare8k.log`

`At this point, the system will reach state 4 and should be ready for use.`

You can then remove/disconnect the devices.

Use this link to jump to d on page 736 (within Section 24.2, “Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)”).

At this point, the system will reach state 4 and should be ready for use.

OpenScape Voice V11 default users and passwords are:

Type	User	Password
Console	root	T@R63dis
Console	srx	2GwN!gb4
SFTP	cdr	MNY9$dta
SSH	sysad	1clENtk=
SSH	superad	BF0bpt@x
SSH	hipatham	kH3!fd3a
SSH	hipathcol	jO3(fdqA
SSH	secad	$ECur8t.
SSH	dbad	d8$ECur.

Table 9 Default User Passwords

Type	User	Password
SSH	webad	!WE8saf. **(for Simplex configurations only)**

Table 9 Default User Passwords

Users "sysad", "superad", "secad", "dbad" and "webad" have 90 day expiry limits set on their passwords. Unless restricted by the /etc/security/access.conf file, all users have access to the OSV via the console also.

Note: If your OpenScape Voice system was upgraded or migrated to OpenScape Voice V11, then you have maintained the expiry data of the source release. This means the "sysad", "superad". "secad" and "dbad" userid passwords will never expire. For password management advice please refer to Section 17.2.2, “Password Management”, on page 617.

The following table provides the default passwords for Solid Users.

User	Password
dba	dba
rtp	RTP_USER
sym	sym **(for Simplex configurations only)**

Table 10 Default Passwords for Solid Users

16. After the installation is complete, verify the success of the installation by logging in as user *root* and execute the following commands:

```
# cd /unisphere/srx3000/srx/startup
# ./srxqry -v
```

A successful software installation is indicated if the nodes (or node) are at run level 4 (RTP and application running with all processes started and in PROCESS_READY state).

Note: If the installation process stops prematurely or if the nodes (or node) do not reach run level 4, this is an indication of a failed installation.

The installation logs are kept on the USB memory stick in the *install.log* file. The hardware information for the platform in progress is also placed on the USB memory stick in the *current.hwinfo* file.

If the installation has failed and the reason is not obvious from the general system behavior or the *install.log* file, contact your next level of support for assistance.

Regardless of installation success or failure, save the contents of the memory stick(s) onto a backup server/device for future reference or diagnostic purposes.

17. As user *srx*, verify that the software is at the patch set level listed in the OpenScape Voice V11 release note with the command:

    `pkgversion -ps or pkgversion -f`

    Attention: Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability. An integrated system should ensure that the applications server is updated with the latest released DVD/PatchSet/HotFix.

    If the patch set level is not correct, install the corresponding patch sets using the CMP/Assistant (after installing the OpenScape Applications for a standard duplex).

18. As user *root*, verify that the system is an imaged system with the command:

    `rpm -qa | grep UNSPxtree`

    Verify that `UNSPxtree-1.0-1` is displayed.

    Note: If you were sent to this section from an upgrade or migration procedure, return to the upgrade or migration procedure rather than going to the OpenScape Voice Installation Checklist.

On the OpenScape Voice Installation Checklist in Section 2.2.4 on page 30, initial step 8 and proceed to step 9.

4.2.4 Backup and Restore via USB

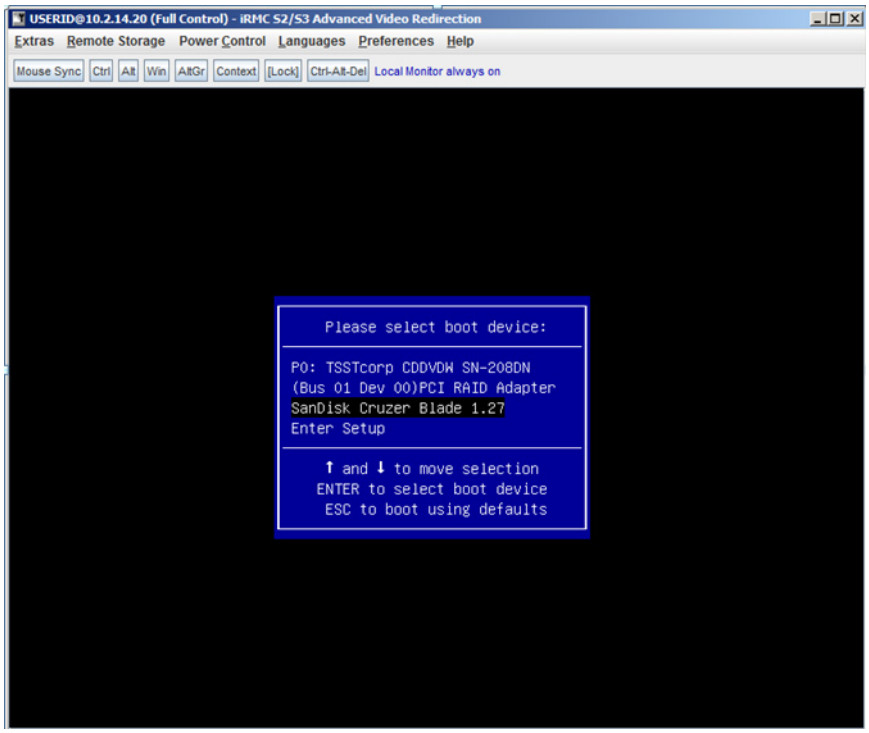
The USB stick adds the restoration software and prompts you for all the required information in order for the restore procedure to commence.

In order to restore OpenScape Voice, you need to have a backup file. The backed-up data may be on an external server, a USB hard disk or even copied onto the same USB device as the restore software.

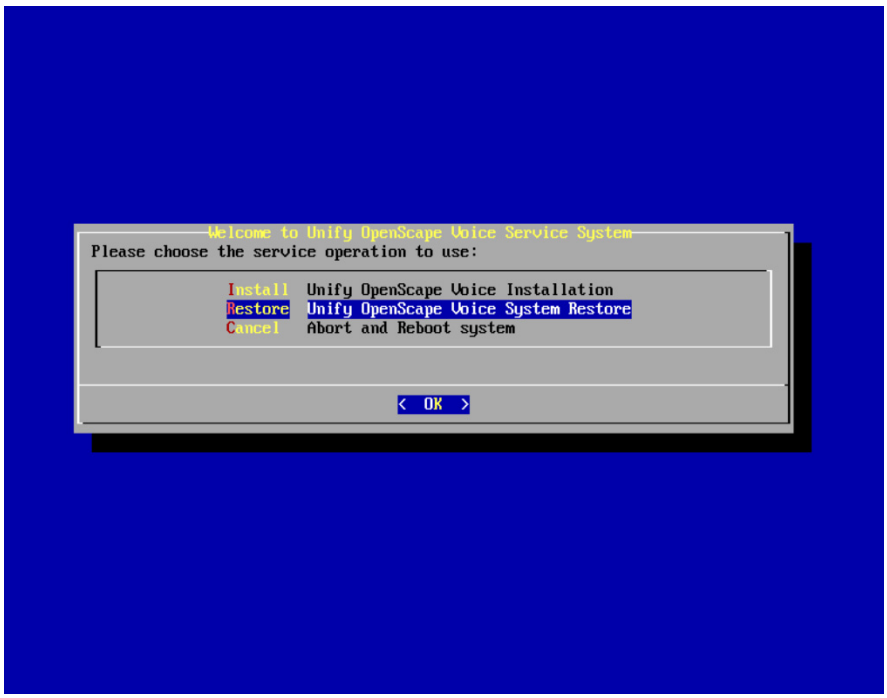
Note: In case you want to place the backup tar file in a USB stick, follow the instructions in Section 4.2.3.2, “Image installation/System Restore USB/Service System Image Write”

The restore procedure is the following:

1. Insert a restore USB stick in each node.
2. Power up the node(s) and click **F12** in order to access the boot menu.
3. From the boot menu, select your USB stick.



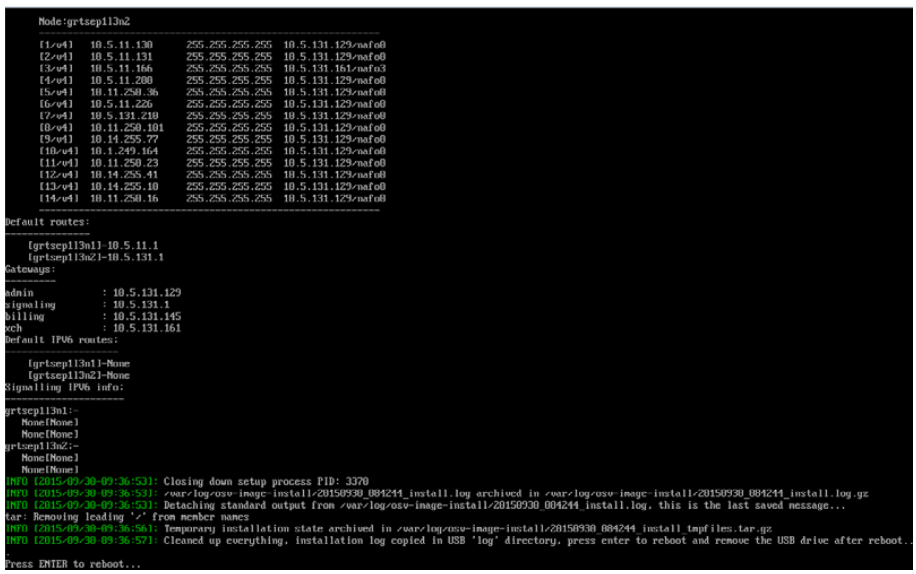
4. The **Unify OpenScape Voice USB Service System** boots.
5. In the menu presented after boot, select **Unify OpenScape Voice Service System**
6. When prompted, select option **Unify OpenScape Voice System Restore**



7. Select the backup source.

   The USB stick contains required data to perform the restore. The restore script will:

   1. Erase existing partitions.
   2. Restore OpenScape Voice without further user input.
   3. Select **Enter** to reboot node (s)



The last step takes around 15 min. to finish.

4.3 Virtualization Environment Setup

Note: Knowledge of VMware and KVM operations and practices is required to deploy virtual machines.

Attention: Because a virtual OSV node will shut down when it loses its storage device, it is recommended that each OSV node be connected to its own storage device (i.e.; SANs or disks) to avoid a total OSV cluster outage in case the storage device fails.

For configurations where the OSV VMs are connected to a Storage Array Network (SAN);
If a OSV VM node loses connectivity to the SAN, that node will reboot. The average time before the node reboot action is less than 3 minutes. The maximum is 5 minutes.

Attention: Both nodes of a cluster (duplex OSV system) must be installed as virtual machines. A cluster configuration where one node is deployed as native hardware and the other as a virtual machine is not supported.

The following provides a guideline for installing an OpenScape Voice (OSV) image onto a virtualized platform. The installation of the virtual environment is outside the scope of this guide.

Usage of Virtual Machine Snapshots:

Note: Snapshots are used as part of official service procedures. However, the following restrictions must be observed.

1. Snapshots are NOT to be taken on production systems during normal operation.
2. Snapshots taken previously must NOT remain active on a production system during normal operation.
3. Snapshots can be taken, if needed (i.e., snapshots can be a valuable mechanism during maintenance operations. For example, they allow a quick rollback to a well-defined state of the VM if a mass provisioning script fails.), during maintenance windows, or during an installation procedure.

4. Note that Snapshots are used internally by backup tools such as VDP or VDR. It must be ensured that (a) these backup operations are scheduled off business hours, and (b) that any Snapshots generated by these tools are deleted at the conclusion of the backup operation.

4.3.1 Virtualization — Overview

Attention: The installation described herein is not the only possible virtual OSV installation. The host, not the OSV VM, needs to be configured with NIC teaming if network redundancy is required.

Virtualization is supported for simplex and standard duplex (co-located and geographically separated) configurations.

Note: In this document, one more subnet to control the virtual management interface is added. This is not necessary if the desired management interface can be tied to a valid and available IP in the admin subnet.

Viewing the Document with Adobe Reader

When viewing the document with Adobe Reader, add the “Previous View” icon to the Reader toolbar. This will ease the navigation between this procedure and associated sections of the document.

Characteristics of the Virtual OpenScape Voice

The virtual OSV has the following characteristics;

- Supports OSV images in a Storage Area referred to as a “datastore”.
- Is HW independent.
- Has no maintenance controller interfaces (RSA, IMM, iRMC, VMK).
- Does not support HW Alarming.
- Currently supports and requires a fixed number of 4 (virtual) Ethernet ports for all configurations (including simplex virtual machines).
- Supports simplex OSV configurations.
- Supports 2 node clustering in co-location and network geographical separation. The co-located OSV can be deployed on 1 (both nodes on same physical host) or 2 hosts. A geo-separated OSV should be deployed on 2 hosts.

- The OSV virtual Machine can use internal or SAN storage.
- For OSV compatibility with ESXi or Proxmox please check the Support VMware vSphere And Proxmox versions.
- Virtual machine disk size of at least 140 GB.
- OSV redundancy depends on Survival Authority. Without Survival Authority a single node failure or interconnection failure may bring down the whole cluster. This is valid for all co-located and geo-separated configurations.
- OSV StandAlone Service is only allowed for a L3-geo-separated configuration (i.e., a configuration that does not provide a virtual IP failover).

  For the StandAlone Service feature to be available in a virtual environment the node.cfg parameter **Node Separation = separate** must be selected. The **Stand Alone Service is enabled by default in this configuration.**

Disk Space Limitations:

If you choose to install from an ISO image file instead of a DVD, please allocate at least 10 GB of disk space in a node's datastore for the placement of the Virtualization Image DVD ISO and Node Configuration files.

Other Limitations:

The virtual OSV system is hardware (HW) independent. It is assumed that the HW platform is installed, supervised and maintained by the customer. This includes the installation and configuration of the virtual machine that will host the OSV.

The virtual OSV assumes it has one disk and 4 Ethernet ports (including the simplex virtual machines).

Disk location (local or network), disk redundancy (RAID), any kind of HW redundancy, and network redundancy (bonding driver) are outside the scope of virtual OSV control and need to be installed by the customer.

4.3.2 Checklist for Virtualization

This procedure assumes that steps 1 on page 31 through 8 on page 32 of Section 2.2.4, "OpenScape Voice Installation Checklist", have already been completed. Please review these steps before proceeding.

At the end of the Virtual Machine Environment setup, you will be referred back to the Installation Checklist to perform other installation tasks (as required for your environment).

Task	Description
1	Determine if Physical Server hardware is supported by the selected Hypervisor.
2	Determine the datastore to be used for the VM (local hard disk or a networked device).
3	If a SAN will be connected then determine if it is supported by the selected Hypervisor.
4	Have an operational Windows or Linux system at hand in order to build the installation node.cfg. For virtual machine node.cfg instructions refer to Section 4.3.4, “Creating a Virtual Machine Node.cfg File”, on page 181.
5	Determine the Network Port to VMNIC mapping.
6	Determine what type of installation configuration you will be conducting (co-Located duplex, geo-separated duplex, or a simplex deployment).
7	For Co-Located configurations determine if the guest servers will be running on 1 physical host server or 2 physical host servers.
8	Determine network cabling based on the decisions made in steps 5 through 7.
9	When creating the VMs, be sure to follow the instructions in the latest issue of the *OpenScape Voice Vx Service Manual: Installation and Upgrades, Installation Guide* (where *x is the software release version*).
10	Install the OSV Image on the guest VMs.

Table 11 Checklist for Virtualization

4.3.3 Virtual Machine Guidelines

Attention: The installation described herein is not the only possible virtual OSV installation. The host, not the OSV VM, needs to be configured with NIC teaming if network redundancy is required.

Note: Reference the virtual solution compatibility guides for software and hardware recommendations, overhead characteristics and upgrade instructions.

Note: The configuration of the virtual machine must be done prior to the installation of the OSV software.

Note: For OpenScape Voice it is recommended to use SLES 15. For OSV compatibility with VM Hardware Version, follow the link https://kb.vmware.com/kb/2007240. For OSV compatibility with the selected Hypervisor please check the relevant chapter in the latest *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide*.

4.3.3.1 Requirements to Underlying Host Hardware

Due to the resource and configuration requirements of the VMs for OpenScape Voice, the following dependencies to the hardware of the ESXi hosts need to be considered before system setup:

- **CPU**

  For each VM, CPU resources shall be reserved as described in Section 4.3.3.2. For lower number of users on a given deployment, less CPU resources might be required.

- **RAM**

  All OpenScape Voice nodes require RAM reservation based on the values in Section 4.3.3.2. This means that a VM's memory needs to exist as physical memory in the host.

- **Storage**

For each VM, hard disk space must be reserved as described in Section 4.3.3.2. This space may either be local to the ESXi host or reside on a SAN, provided the SAN is equivalent to a local hard disk from a performance point of view.

Note: Disk redundancy (RAID) is outside the scope of virtual OSV control and needs to be installed by the customer.

4.3.3.2 Virtual Machine Configuration Parameters Overview

Document *OpenScape Solution Set V11 Virtual Machine Resourcing and Configuration Guide* lists the configuration parameters needed to configure each OpenScape Voice node.

Note: The line *VM RAM [GB] + reservation* includes the memory to be reserved for the VM. For overall memory sizing, include at least 2.5 GB of RAM for the ESXi.

Note: See Section 4.3.3.7, “Virtual Machine Disk Requirements” for additional HD overhead required on the physical host.

Both nodes of a duplex OpenScape Voice deployment can be installed on the same host/ server, but it is recommended the nodes be installed on separate servers (for redundancy reasons).

The simplex option is available for the virtual environment deployments.

The following additional notes have to be taken into account for this product:

- OSV figures in the table indicate requirements for each node
- OSV figures in the table are based on a typical Enterprise Feature set
- OSV figures in the table are based on old OSV (V7) versions default RTT trace settings (24-7 extern)/distributed registration/Nodes on Separate servers/Active-Standby mode
- For duplex configurations; OSV nodes are recommended to reside on separate physical servers for HW redundancy.
- OSV uses additional disk space (on the server/SAN) to hold things like images, patch sets, mass provisioning files, restore CD, CDC ISO, etc)
- OSV Backup and Restore procedures are recommended to be used versus snapshots.

- vCPU: Intel Xeon Processor x5650 / 2.66 GHz, 12 MB Cache or equivalent CPU.
- OSV NW and Disk usage may vary based on call usage and Feature mix
- OSV cps (Calls per Second) formula = # of users*5/3600*5 (5 calls per user per hour with a loading factor of 5 for features). Example: 1000 users = 6.94 cps.
- OSV NW Total Bandwidth KB/s Requirement formula = cps*26.
- For duplex configurations; OSV X-channel Bandwidth KB/s Requirement formula = cps*13

  Note: Cross channel compression is turned on by default

- OSV HD KB/s formula = cps*3.33

For a detailed overview of the configuration parameters, see chapter **OpenScape Voice** in the latest *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide.* Also in this document the overhead requirements per physical system for the OSV solution are listed. Some values can not be defined because they are based on the configuration of the host (physical) server.

4.3.3.3 Overview of the OSV Virtual Machine Solutions

Simplex One Physical Server:

- 3 subnets reserved for Admin, Billing, Signaling

Note: A Simplex virtual machine has no 'cross-over' connectivity requirement

---

Co-located Duplex One Physical Server:

- 3 subnets reserved for Admin, Billing, Signaling
- Cross-over connected via virtual switch

Co-located Duplex Two Physical Servers:

- Two Options for Subnets:
  - Three Subnets + one Private
    - Three subnets reserved for Admin, Billing, Signaling and one Private for Cross-over
    - Cross-over cable connection between the nodes
  - Four Subnets
    - Four Subnets reserved for Admin, Billing, Signaling and Cross-over
    - Cross-over connectivity occurs through a layer 2 switch

Geo/Network-Separated Duplex Two Physical Servers:

- Four Subnets per node for a total of eight subnets total
  - Four Subnets reserved for Admin, Billing, Signaling and Cross-over for node 1.
  - Four Subnets reserved for Admin, Billing, Signaling and Cross-over for node 2.

4.3.3.4 Virtual Machine Network Requirements

The OSV requires that 4 Ethernets be presented to it as labels during virtual machine creation. Each of these labels needs to be in a different subnet as presented to the OSV. These subnets are used in building the node.cfg file. These are:

- Admin subnet - used for admin/maintenance information
- Signaling subnet - used for SIP/CSTA/MGCP signaling

- Cross Connect - used for call state synchronization in duplex configurations.
  - For the case of a co-located on the same host, this is a Vswitch only connection.
  - For co-located systems on separate hosts it is a direct gigabit quality Ethernet cable cross connect.
  - In the case of a geo-separated system it can be either a L2 bridged connection or a L3 routed connection.
- Billing subnet - This is used for sending CDRs to the billing server.

The connection of the labels to the real network is dependent on the customer network configuration. This can be a flat or segmented network and can also use each Hypervisor's VLAN capability. Network interface redundancy can also be used if required.

The exception to this is the duplex OSV cross connect link, a standard routable IP interface, which due to the heavy traffic should be a dedicated link.

The Survival Authority shutdown agent configuration is installed with the OpenScape Voice image and will be verified as part of a duplex virtual machine installation.

The **Flexible Ethernet circuit and IP Address Configuration** feature allows for a flexible configuration of Ethernet circuits and IP addresses. For more details, refer to Appendix 16, "Flexible Ethernet circuit and IP Address Configuration Examples".

Note: X-channel and CIGroup references apply to virtual duplex deployments.

The following node.cfg parameters impact the Ethernet port and IP address configuration of the OpenScape Voice server.

a) Share Mgmt with X-channel button: **Select the associated box if the X-channel (Cluster Interconnect Group- CIGroup) is to share the same subnet (and Ethernet ports) as the Management Network.** When this box is selected, the CIGroup parameters are grayed out and the CIGroup is placed in the Management Network subnet address scheme; the default last octet of the CIGroup IPs are '4' for node 1 and '5' for node 2.

   - The CIGroup IPs are set to the same IP as the Node 1 (or 2) IP of the Management network.

b) Subnet Sharing: **This parameter dictates the number of Ethernet ports used and the IP addressing schema for the Mgmt, Billing and Signaling subnets.** The following is an overview of the Subnet Sharing choices available and how they impact the Ethernet port and IP address configuration of the OpenScape Voice server;

- **Mgmt-Billing-Signaling-Separated:** Default configuration. All 8 Ethernet port pairs are used. Each subnet is assigned to ports as defined in Chapter 3 of this document (in the “Connecting the Cables” section of each platform).
- **Mgmt-Billing-Shared:** The Mgmt and Billing subnets are merged - the Signaling and Cluster ports are separate. The Billing ports are not used.
- **Mgmt-Billing-Signaling-Shared:** Mgmt, Billing and Signaling subnets are merged - Cluster ports are separate. Billing and Signaling ports are not used.

Attention: IF ‘Share Mgmt with X-channel’ was selected, THEN the CIGroup is also merged with the Mgmt subnet. In this scenario, the CIGroup (X-channel) ports are not used.

The virtual OSV always needs to be created with 4 network connections, in the following sequence:

- NIC 1: admin (is mapped to virtual NIC 0 in the VM properties window).
- NIC 2: signaling (is mapped to virtual NIC 1 in the VM properties window).
- NIC 3: billing (is mapped to virtual NIC 2 in the VM properties window).
- NIC 4: cross_connect (is mapped to virtual NIC 3 in the VM properties window).

As an example; a **Flexible Ethernet circuit and IP Address Configuration** case where node.cfg parameter **Subnet Sharing = Mgmt-Billing-Signaling-Shared.**

The Billing and Signaling ports are not used in this configuration. In this case, the craft might want to assign virtual NICs 2 and 3 a different label (e.g.; "unused2" and "unused3").

Note: All 4 virtual NICs have to be defined because they are internally mapped to the virtual OSV Ethernet ports.
- Eth0/virtual NIC 0 is mapped to virtual properties NIC 1
- Eth1/virtual NIC 1 is mapped to virtual properties NIC 2
- Eth2/virtual NIC 2 is mapped to virtual properties NIC 3
- Eth3/virtual NIC 3 is mapped to virtual properties NIC 4

Even if eth3 (virtual NIC 3) is not used, it cannot be removed because OSV still needs eth3 for the x-channel.

4.3.3.5 Virtual Machine Memory Requirements

Refer to Section 4.3.3.2, “Virtual Machine Configuration Parameters Overview” and the Virtual Resource Management Guide for additional memory required for Virtual machine overhead.

4.3.3.6 Virtual Machine CPU Requirements

Refer to Section 4.3.3.2, “Virtual Machine Configuration Parameters Overview” and the Virtual Resource Management Guide for Virtual CPU requirements.

4.3.3.7 Virtual Machine Disk Requirements

The OSV requires that the virtual machine present a single SCSI disk on target (0:0). The **virtual machine disk size** should be 140 GB. The virtual machine requires an additional 40 GB over and above the virtual machine disk size.

The **host server disk drive** should be at least 180 GB for a **single OSV virtual machine on a dedicated server (140 GB + 40 GB)**.

The **host server disk drive** should be at least 320 GB for a **co-located OSV virtual system on one physical server (140 Gb + 140 Gb + 40 GB)**.

Calculations for the physical HD sizing including allowances for VMware and ISO images are based on the following;

- New Image + old Image during upgrade: 10 GB
- Allowed for VMware machine overhead: 3 GB (140 GB VM disk size)
- Allowed for VMware system disk overhead: 17 GB

Note: The calculations for the physical HD sizing does not include space that would be needed for snapshots or other swap space for other VMs that do not reserve their memory.

Attention: The virtual SCSI controller must be adapted before saving the Virtual Machine.

The physical disks can be onboard the host or connected by SAN. VSAN configuration has not been tested yet. Any level of raid can be used.

Disk reservation parameters should be left as their default.

4.3.3.8 Other Parameters to Consider for the Virtual Machine

Most other parameters should be left as their default. The exceptions are:

- Hyperthreading should be turned on if it is available to increase the number of virtual processors available to the system.
- The CDROM must be on virtual device node IDE(0:0)
- For ease of installation the CDROM should be set to connect on power on.
- For ease of installation the force BIOS flag on next reboot should be set in the boot options.

4.3.4 Creating a Virtual Machine Node.cfg File

The node.cfg file is used by the installation process to determine which image will be installed on your OpenScape Voice server. The determination is based on the platform you select. For Virtual machines:

- **Virtual-OSV** should be selected for the **Hardware Platform** type.
- The default **Configuration** for the H**ardware Platform Virtual-OSV** is **Standard-Duplex. Integrated Simplex** can be chosen from the **Configuration** drop down menu.

Note: Recommended practices for file transfer and burning of CD/DVD media;
1. If a checksum, md5sum or sha file is delivered with OpenScape software it is a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. If necessary, third party software can be used to calculate these values.
2. When burning a file to a CD/DVD media use a lower burning speed (i.e.; 4x).
3. Use the 'verify' option of the burning application to ensure data integrity after the DVD burning is complete.

4.3.4.1 Preparation of the node.cfg files using a Linux or Windows Environment

---

Note: An installation ISO image for each OSV node can be created and used for the installation and upgrade procedures of an OSV virtual system. This Installation ISO image of each OSV node includes the appropriate node.cfg file, license, Migration Toolkit and patch sets (including emergency patch sets). **This Installation ISO image is sometimes referred to as a CD ISO image.**

Download (from SWS) the latest "OpenScape Voice Installation Wizard" zip file that corresponds to the OSV software version that you are installing.

Note: If necessary, refer to the OpenScape Voice base software release note on G-DMS for the link to SWS to download the Installation Wizard zip file.

---

a) Unzip the downloaded file. Now there should be a parent directory named 'ncpe-OfflineWizard-<version_number>'. Change to the bin path located one level below 'ncpe-OfflineWizard-<version_number>'.

b) For Windows systems; open (double click) the file named ifgui.cmd.

   For Linux systems; open the file named ifgui.

   Note: For Linux users, if needed, export the DISPLAY of the output to your PC by entering "export DISPLAY=<IP address>:0", where the IP address of the destination of the DISPLAY is to be sent is used. This step is done as the root user.

   ---

c) On the Installation Framework options screen, select **Install** and click **Next**.

d) The Configuration and Hardware (1/1) page will be presented. Select the **Hardware Platform Virtual-OSV**. This selection sets the value of **Configuration** to S**tandard-Duplex. Integrated Simplex** can be chosen from the **Configuration** drop down menu.

Note: A link back to this location is provided in the sections referenced in the next step.

---

e) Refer to Section 2.6, “Creating a Node.cfg File”, on page 50 for further details regarding the node.cfg creation. Complete Section 2.6.2 through Section 2.6.9, step 6 on page 64.

   When Section 2.6.2 through Section 2.6.9, step 6 on page 64 are complete return to this step.

   Note: References to node.cfg.primary apply to the installation node.cfg for the single node of a simplex virtual deployment or node 1 of a duplex virtual deployment. The node.cfg.secondary references apply to the installation node.cfg for node 2 of a duplex virtual deployment.

The user has two choices for the node.cfg medium when installing the Image;

1. A Installation ISO image that can include the node.cfg.primary (or node.cfg.secondary), license file (for that node) and any released patch sets that are not included with the delivered Image. Refer to Section 4.3.4.2, “Saving the node.cfg, license and patch sets to an Installation ISO Image”, on page 183.
2. A virtual floppy that includes the node.cfg only. Refer to Section 4.3.4.3, “Creating a Virtual Floppy Disk”, on page 185.

Note: It is recommended to install with a Installation ISO image that includes the node.cfg, license file and any released patch sets (not included with the delivered image). This automates the installation by:

1. Negating an OSV software update by the craft after the installation completes.
2. Removing the manual step to apply the OSV license file to the node(s).

4.3.4.2 Saving the node.cfg, license and patch sets to an Installation ISO Image

A Installation ISO image which includes the appropriate `node.cfg` file and patch sets (including emergency patch sets) may be employed for the image installation.

For the installation, this Installation ISO image has to be created with the same structure as a native machine USB stick (as described in Section 2.7, “Including Patch Sets and License files on the USB Memory Stick(s)”). The process is summarized in steps 1 through 6 of this section.

Note: If you reached this section from a Upgrade or Migration scenario, perform steps 2 through 6.

---

1. The node.cfg file(s) should be generated as per the instructions in Section 4.3.4, “Creating a Virtual Machine Node.cfg File”. **There is no need to create virtual floppies for the Installation ISO image procedure.**
2. The root level directory of the ISO image should contain the *node.cfg.primary* and license file for node1.

Attention: In simplex migration scenarios the root level directory of the Installation ISO image should also contain the "response.cfg.primary file".

---

3. An empty file, *dev.8kps*, should be **under the */patch* directory**.

4. Put the patch sets and the emergency patch sets, including the SPA files, into the *patch* directory. Generally, **this means the needed tar files from the latest cumulative patch set and all the tar files of the latest cumulative emergency patch set.**

   For example, if the latest image is delivered with PS07.E02 and PS12.E05 is required as part of the image installation;

   - Download cumulative PS12 including the associated SPA file.
   - Download cumulative emergency PS12.E05 including the associated SPA file.
   - Place the downloaded patch sets and SPA files in the patch directory.

   Note: Including the SPA file in this step will trigger an md5sum check of the patch sets before they are installed. A patch set md5sum check failure will be reported to the console and the installation will abort. If cumulative patch sets are not available, tar files of the regular patch sets can be placed in the patch directory as well as the related tar files of the emergency patch sets. The standard naming convention of the patch sets **must** be maintained. **Remember to include the patch set SPA files in order to trigger the md5sum check during the installation.**

   Attention: Name the Installation ISO image appropriately to ensure that the proper ISO image is selected for the image install; Sample naming convention:
   - Node 1 Installation ISO filename: CD_N1.iso
   - Node 2 Installation ISO filename: CD_N2.iso

   ---

5. Generate the Installation ISO image. For Microsoft based systems, many third party image burning tools can create an ISO image from a directory structure. These third party tools are outside the scope of this document.

   Some Linux based systems have a built in capability to generate ISO images from the command line. The OpenScape voice and applications servers can be employed to generate the Installation ISO image, if you prefer. Prepare your directory with the node.cfg.primary, the appropriate license file and patch sets (as defined in steps 1 through 4 of this section then refer to Appendix 22, “Building an ISO file on the OSV or Applications Server”.

6. For a duplex configuration, repeat this procedure for node 2. This Installation ISO should contain the node.cfg.secondary in the top level of its structure. The patch sets, emergency patch sets and empty *dev.8kps* file should be **under the */patch* directory**.

The Installation ISO image is now ready for transfer to the datastore Section 4.3.5.2 on page 189 contains instructions for uploading a file to the datastore.

4.3.4.3 Creating a Virtual Floppy Disk

The user has a choice of installing the Image via a virtual floppy that includes the node.cfg or with a Installation ISO image that can include the node.cfg, the licence file, and any released patch sets that may not be included with the delivered Image.

- To install with a Installation ISO image, which will allow patch sets to be installed automatically during the Image installation process, please refer to the Uploading to the Datastore section on each Hypervisor respectively.

For the Windows OS there are special imaging software packages, e.g. winImage, which would create a virtual floppy file which can be used in VMware ESXi server. The following is an example of creating a virtual floppy in the Linux environment.

Note: Simplex virtual deployments should only create and save a Node1.flp file.

---

1. As root user type the following commands:

```
dd if=/dev/zero of=/tmp/Node1.flp bs=1024 count=1024
mkfs.msdos /tmp/Node1.flp
cp /tmp/Node1.flp /tmp/Node2.flp
```

This will create two virtual floppy devices under the /tmp directory named *Node1.flp* and *Node2.flp*. A snapshot of the commands and results follow;

```
root@fsc501:[/tmp] #216
# dd if=/dev/zero of=/tmp/Node1.flp bs=1024 count=1024
1024+0 records in
1024+0 records out
1048576 bytes (1.0 MB) copied, 0.004398 seconds, 238 MB/s

root@fsc501:[/tmp] #217
# mkfs.msdos /tmp/Node1.flp
mkfs.msdos 2.11 (12 Mar 2005)

root@fsc501:[/tmp] #218
# cp /tmp/Node1.flp /tmp/Node2.flp




root@fsc501:[/tmp] #219
# ll /tmp/Node*
-rw-r--r-- 1 root root 1048576 Feb 17 17:35 /tmp/Node1.flp
```

```
-rw-r--r-- 1 root root 1048576 Feb 17 17:35 /tmp/Node2.flp
```

4.3.4.4 Saving the node.cfg File to Virtual Floppy Files

Copy the node.cfg file created in Section 4.3.4 to the */tmp* directory. As root user type the following commands:

- For Node 1:

```
mount -o loop /tmp/Node1.flp /media/floppy
cp node.cfg.primary /media/floppy/node.cfg.primary
umount /media/floppy
```

- For Node 2:

```
mount -o loop /tmp/Node2.flp /media/floppy
cp node.cfg.secondary /media/floppy/node.cfg.secondary
umount /media/floppy
```

The *Node1.flp* and *Node2.flp* files are now ready for transfer to the datastore.

Note: Please refer to the Uploading to the Datastore section in Section 4.3.5.2 on page 189 for instruction on uploading a file to the datastore.

4.3.5 VMware - vSphere Client

Note: When an OpenScape Voice is deployed as a virtual machine using VMware, the Open VM Tools are included as part of the IMG Installation/Upgrade.

Note: The version of the Open VM Tools is dependent on the SLES version that is included in the OpenScape Voice image and should be the latest compliant.

Note: Manual installation/update of the Open VM Tools is not supported as it could lead to incompatibility issues, this means that Open VM Tools will be delivered only via the OSV IMG installation/upgrade for virtual deployments.

The following VMware features are tested:

- VMware HA

- Migration with VMotion
- VMware DRS
- Snapshots (of a Virtual machine)

Note: If a vMotion or DRS activity is performed during high traffic periods, a slight degradation in service may be observed. On an Integrated Simplex, the feature is only supported with minimum or without load.

Usage of VM snapshots

When taking a snapshot using vSphere, check the Quiesce guest file system option.

Whenever an administrator takes a snapshot using vSphere checking the *Quiesce* guest file system option will gracefully persist all IBM Solid or MySQL transaction logs (*/usr/sbin/pre-freeze-script.sh* is executed).

For additional information regarding Snapshots, please consult the VMware Knowledge Base (KB). A good starting point is KB Article 1025279-Best Practices for virtual machine snapshots in the VMware environment. Here is a link:

http://kb.vmware.com/kb/1025279

Feature information can be accessed from the vSphere client toolbar Help menu.

More information regarding Migration with vMotion and VMware can be found in the following manual:

- vSphere Datacenter Administration Guide (for the recommended ESX and vCenter Server versions).

Information regarding VMware HA can be found in the following manual:

- vSphere Availability Guide (for the recommended ESX and vCenter Server versions)

More information regarding Snapshots can be found in the following manual:

- vSphere Virtual Machine Administration Guide (for the recommended ESX and vCenter Server versions).

Note that the following VMware specific features have not been tested:

- VMware vCenter Update Manager

- VMware vSphere 5.1 API for Data Protection (VDP)

- VMware vShield Zones

- VMware Storage vMotion

- VMware DPM

Note: The VSAN environment has not been tested.

Note: Reference the VMware Compatibility Guides for software and hardware recommendations. As an example, for information regarding using *Nehalem* processors in the Virtual machine host, see the VMware Resource Management Guide for virtual machine overhead characteristics. These guides are available at the VMware homepage (www.vmware.com).

Note: The VMware manual MAC is no longer used to lock OSV license files for Virtual deployments. Thus, the CLS must be used to calculate the Advanced Locking ID for OSV license files.

Note: The virtual SCSI controller must be type LSI Logic parallel and has to be adapted before saving the Virtual Machine.

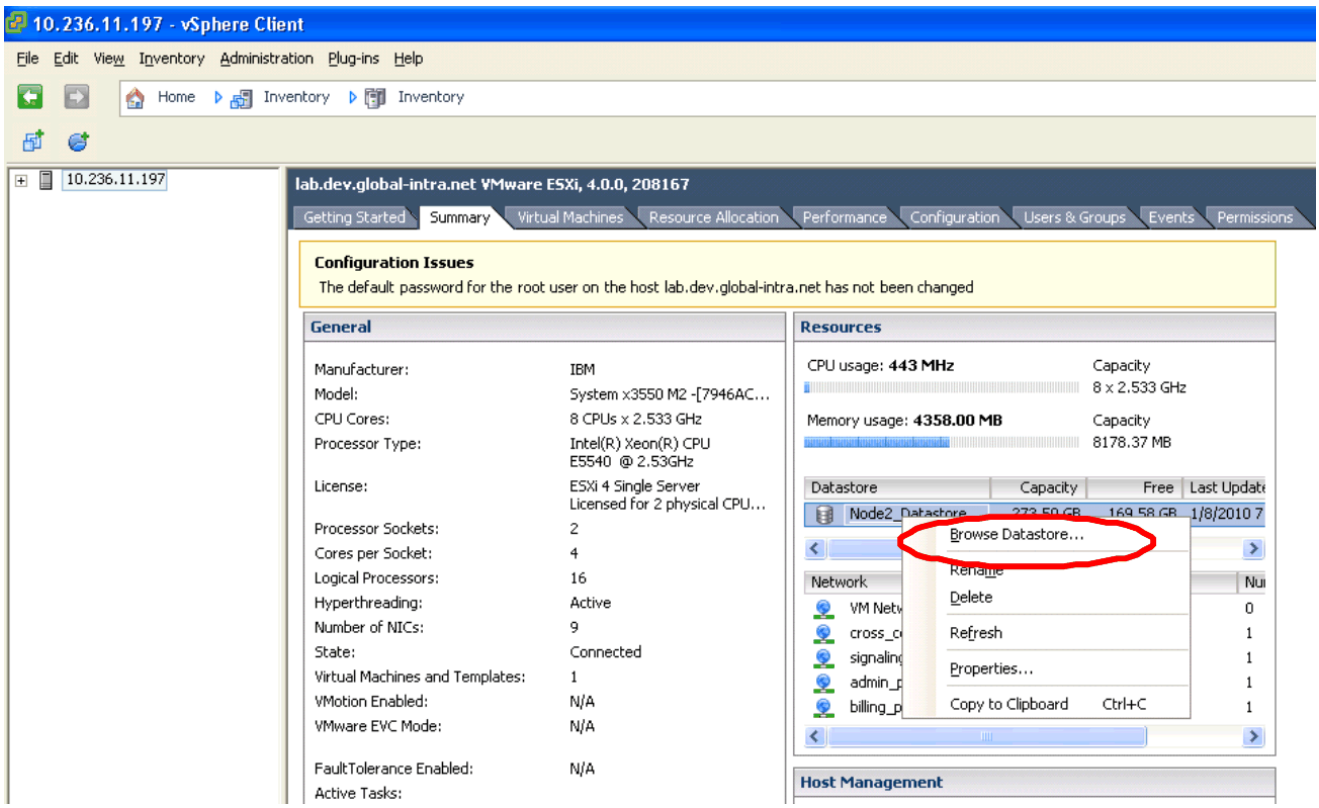
4.3.5.1 Configuration of Login Credentials in VMware vSphere Client

Proceed as follows:

1. Open the VMware vSphere Client and Enter the Login Credentials:
   - Enter the IP address/Name: Management IP of the Virtual server or VCenter server serving the host machine.
   - Enter the User name: root (or VCenter login)
   - Password: Password creation is optional when installing the VMware. If a VMware password was created it must be entered here.
2. Select **Login**.

4.3.5.2 Uploading a File to the Datastore

1. Select the Summary tab of the Virtual Machine.
2. On the Summary tab of the Virtual Machine right click on the datastore and choose **Browse Datastore**. As shown below:



3. Select the root directory and click on the following icon to create a logical folder under the datastore's root "/" directory called "images":

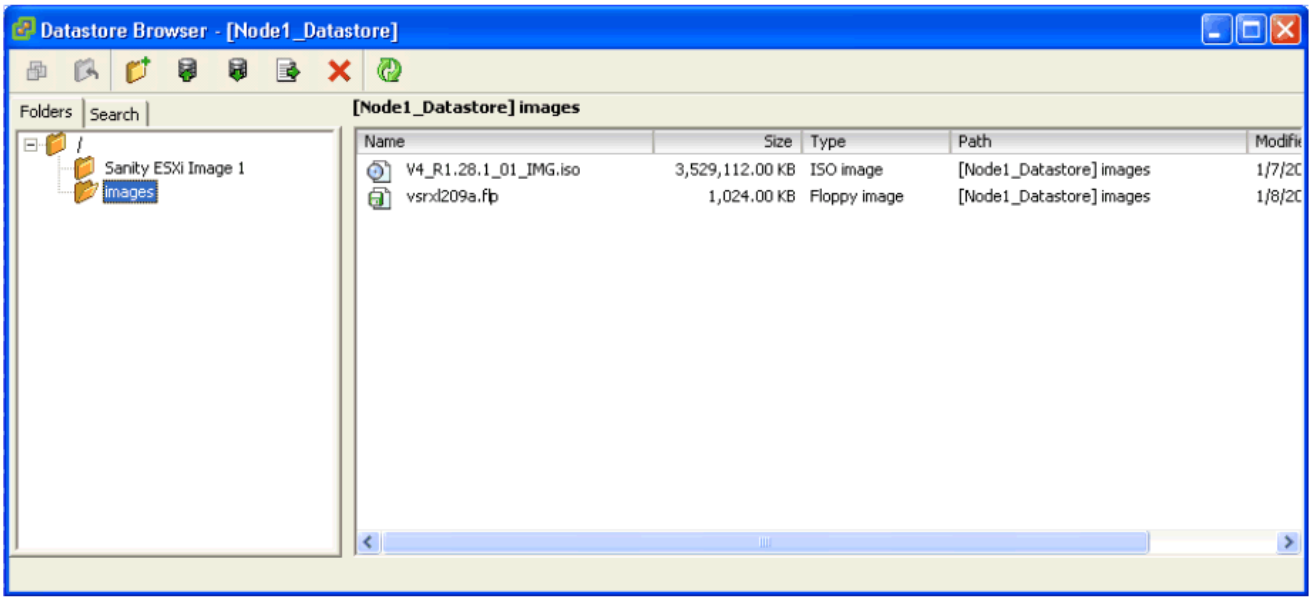
Note: This folder can be named anything you choose.

- Enter the new name (e.g. "images") for the directory in the **New Folder** window.
- Click the **OK** button to confirm the name.

4. Select the new directory and click on the "Upload File" icon to upload a file.

- Select **Upload File...**.

- Select a file from the next dialog and click **Open** to initiate the transfer to the datastore.



Note: This procedure needs to be done for the Image ISO as well as the Installation ISOs (or Virtual Floppy Disks if you chose to build Virtual Floppy Disks).

- If **1 Physical Server** is being used, upload the following files to the "images" directory of the datastore:
  - Image.iso
  - Node 1's Installation ISO file (or Node1.flp)
  - Node 2's Installation ISO file (or Node2.flp)
- If **2 Physical Servers** are being used, then upload the following files to the "images" directory of node 1's datastore:
  - Image.iso
  - Node 1's Installation ISO file (or Node1.flp)

  Then upload the following files to the "images" directory of node 2's datastore:
  - Image.iso

– Node 2's Installation ISO file (or Node2.flp)

Note: Items in the datastore can easily be modified by right clicking on an item and choosing the appropriate operation from the context menu presented.

4.3.6 Preparation of the VMware Virtual Switches

4.3.6.1 Preparation of the VMware Virtual Switches: Two Physical Servers Setup (Co-Located or Geo-Separated)

Note: These instructions apply to Duplex and Integrated Simplex OSV VMware Virtual Switch preparation. Some of the steps have different headings like "**Duplex:**" and "**Simplex:**" depending on the VM system being prepared. Choose the selections listed for your VM deployment.

When the Virtual Switch preparation for a Simplex OSV is complete the user will be directed to the next section by a doclink.

For a co-located system running on 2 physical servers, the Crossover interconnect can be either a direct or a bridged unrouted physical connection.

The user can define any VMNIC association with a subnet label. For example, the user could choose to make VMNIC1 the admin_primary and VMNIC5 the signaling_primary; however for illustration purposes, the procedures in this document will use the mapping defined below.

VMNIC	Subnet Label	Example of Physical NIC
VMNIC0	admin_primary	0
VMNIC1	signaling_primary	1
VMNIC2	billing_primary	2
VMNIC3	cross_connect_primary	3 (depending on the configuration this may not be used)
VMNIC7	Management Network interface	7 (chosen during VMware install)

Attention: VMNIC3 (cross-connect_primary) would not be required for simplex virtual machine deployment. All 4 VM NICs have to be defined because they are internally mapped to the virtual OSV Ethernet ports.

- Eth0/VMNIC0 is mapped to VM properties NIC 1.
- Eth1/VMNIC1 is mapped to VM properties NIC 2.
- Eth2/VMNIC2 is mapped to VM properties NIC 3.

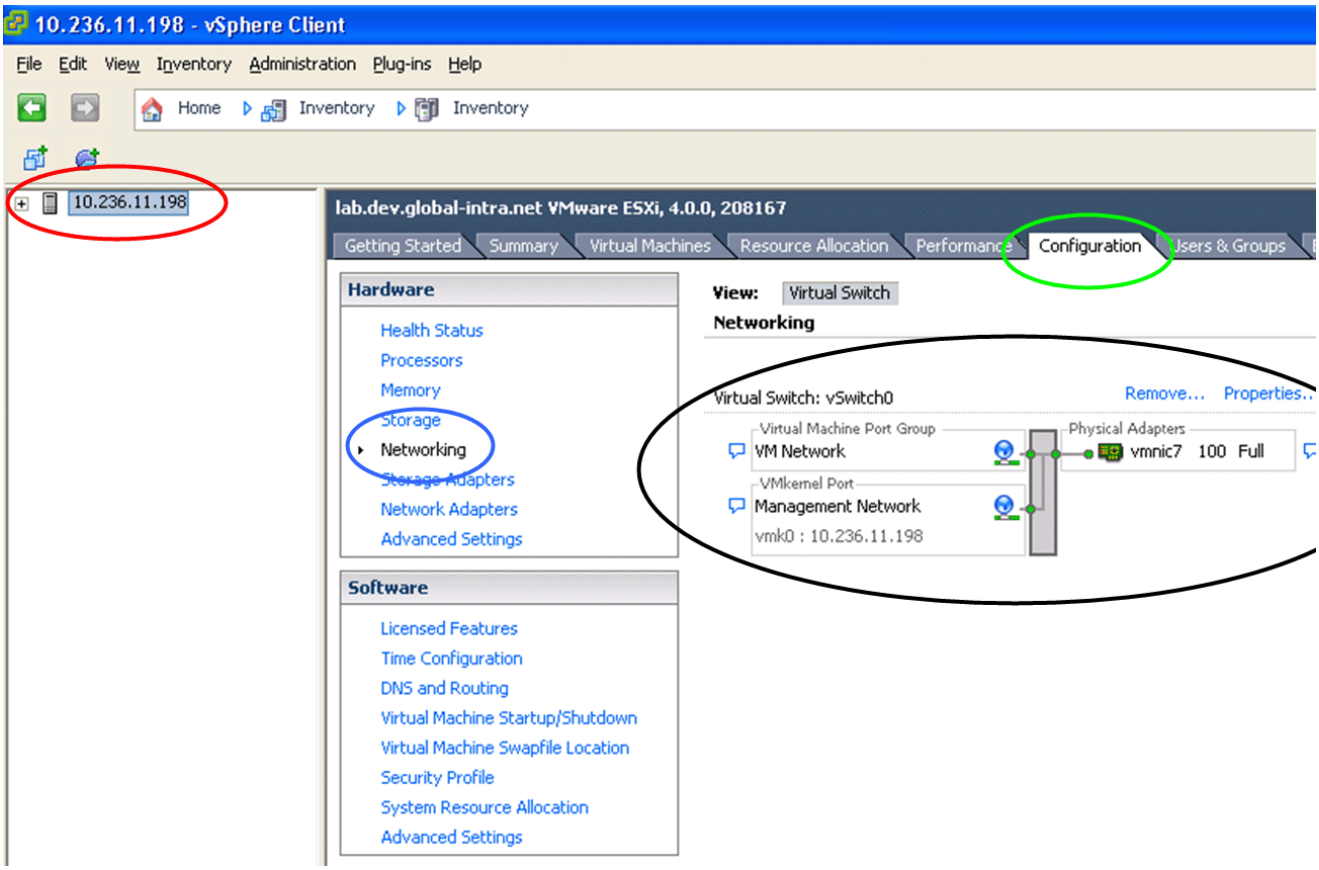
- Eth3/VMNIC3 is mapped to VM properties NIC 4.

If Eth3/VMNIC3 is not used, it cannot be removed because the OSV still needs the eth3/VMNIC3 mapping. In this case, the craft might want to assign VMNIC3 a different label (e.g.; "unused3"). The same naming convention could be applied to other VMNICs that are not used.

Configuring the Virtual Switches

Proceed as follows to configure the virtual switches:

1. Select the ESXi servers Management IP address (see red ellipse in figure below) and click on the **Configuration** tab (see green ellipse).



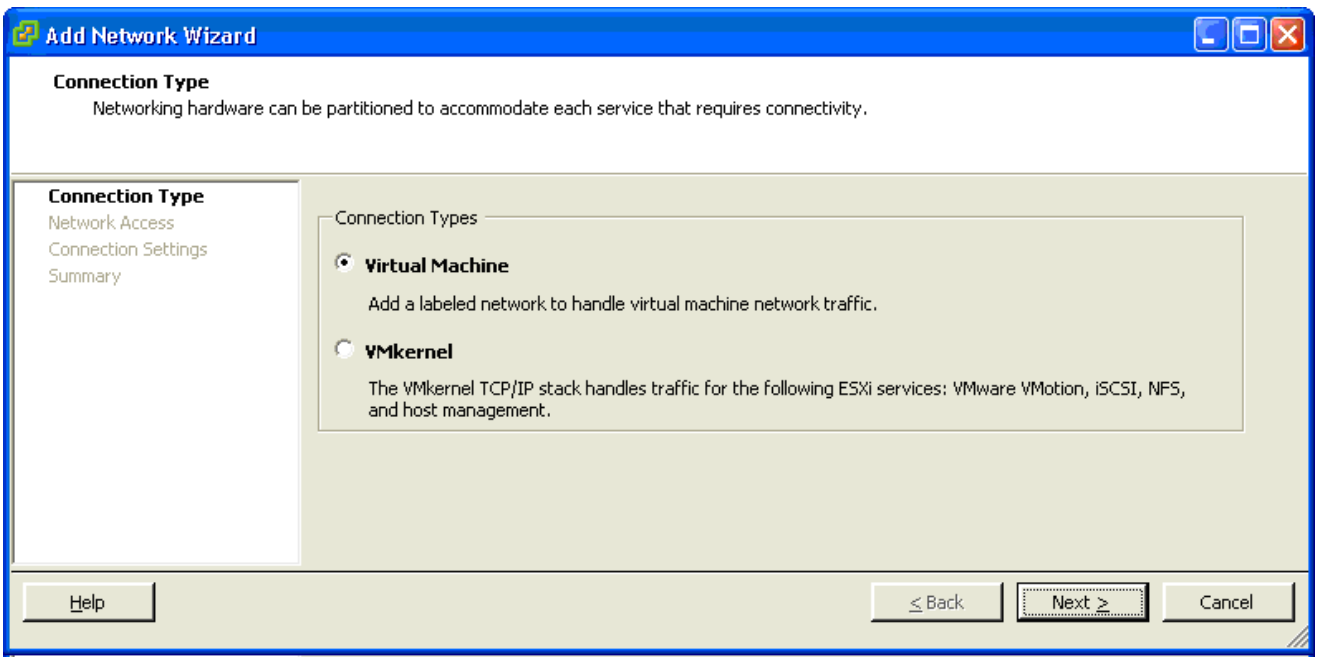
2. Select **Networking** (see blue ellipse in figure above) in the **Hardware** menu.
3. Initially, configure one Virtual Switch which the ESXi Management interface will be associated with (see black ellipse in figure above).

Note: Co-Located with one Physical Server setup is a special case. Please follow the procedures in Section 4.3.6.2, “Preparation of the VMware Virtual Switches: Co-Located with one Physical Server”, on page 199.

---

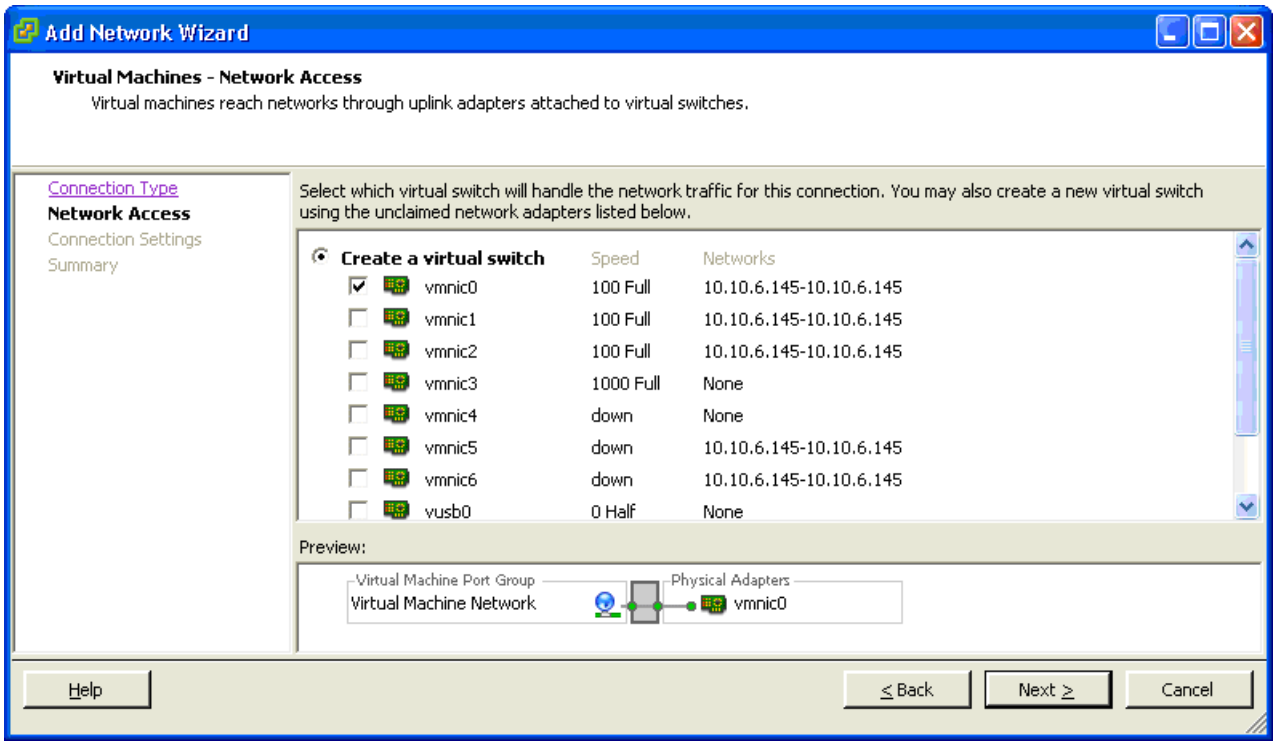
4. Add four More Virtual Switches by clicking on the “**Add Networking**...” option located in the top right segment as shown below:

The **Add Network** window appears:

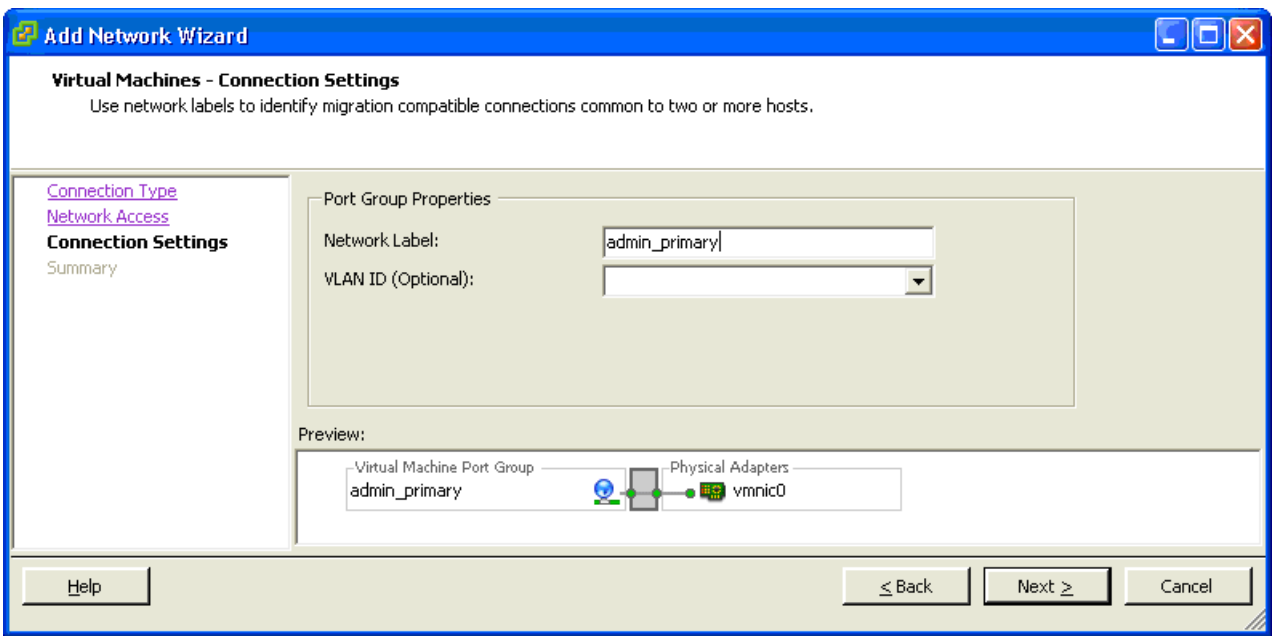


5. Select the **Virtual Machine** option for the connection type and click the **Next** button.

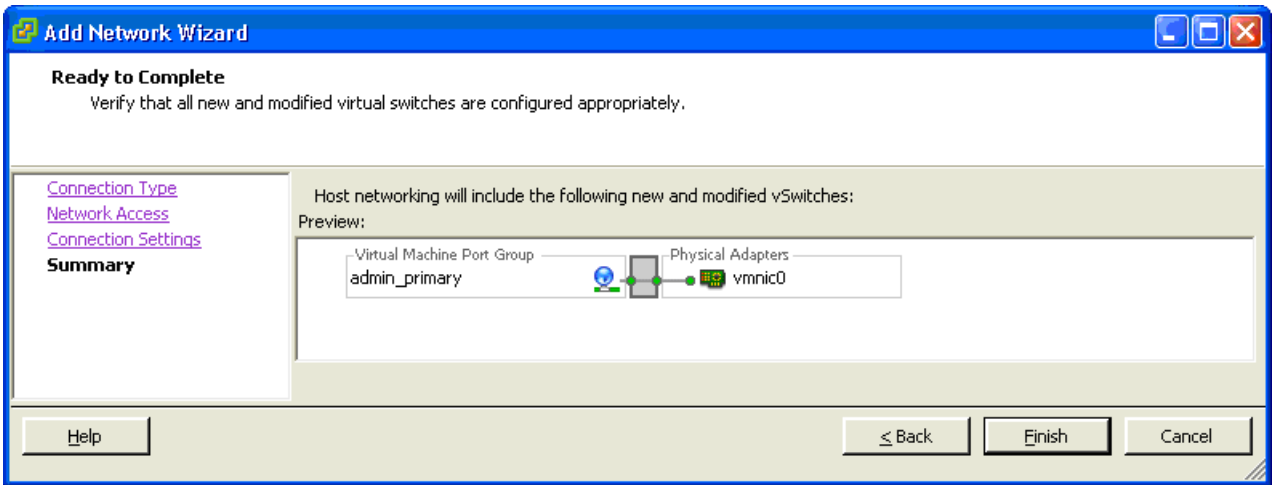
   The **Virtual Machines - Network Access** dialog appears.



6. Click the **Next** button. The **Add Network Wizard – Connection Settings** dialog appears:



7. Enter `admin_primary` in the **Network label** field and click the **Next** button. The **Add Network Wizard – Ready to Complete** dialog appears.



8. Click the **Finish** button.
9. Continue with the subnet additions (based on your deployment).

   For Duplex and Simplex systems: If you intend to use VMotion/HA then the network labels used must be unique in your network.

Duplex: Repeat steps 2 - 8 three more times to add the other subnets, remembering to follow the order in Table 12. The names below are only examples and are not mandatory.

Subnet	Network Label
vmnic0	admin_primary
vmnic1	signaling_primary
vmnic2	billing_primary
vmnic3	cross_connect_primary

Table 12 Network Labels Primary Server - Standard Duplex Node 1

Simplex: Repeat steps 2 - 8 three more times to add the other subnets. Two examples of Network labeling are provided here.

The names below are only examples and are not mandatory. For an Integrated Simplex Virtual Machine there is no cross-connect switch but the fourth VMNIC (VMNIC3) must be created.

1. Table 13: Network Labels - Integrated Simplex VM with All Subnets Shared (1 port) configuration example
2. Table 14: Network Labels - Integrated Simplex VM with Separate Subnets (3 port) configuration example.

Subnet	Network Label
vmnic0	admin_primary
vmnic1	unused1
vmnic2	unused2
vmnic3	unused3

Table 13 Network Labels - Integrated Simplex VM with All Subnets Shared (1 port) configuration example

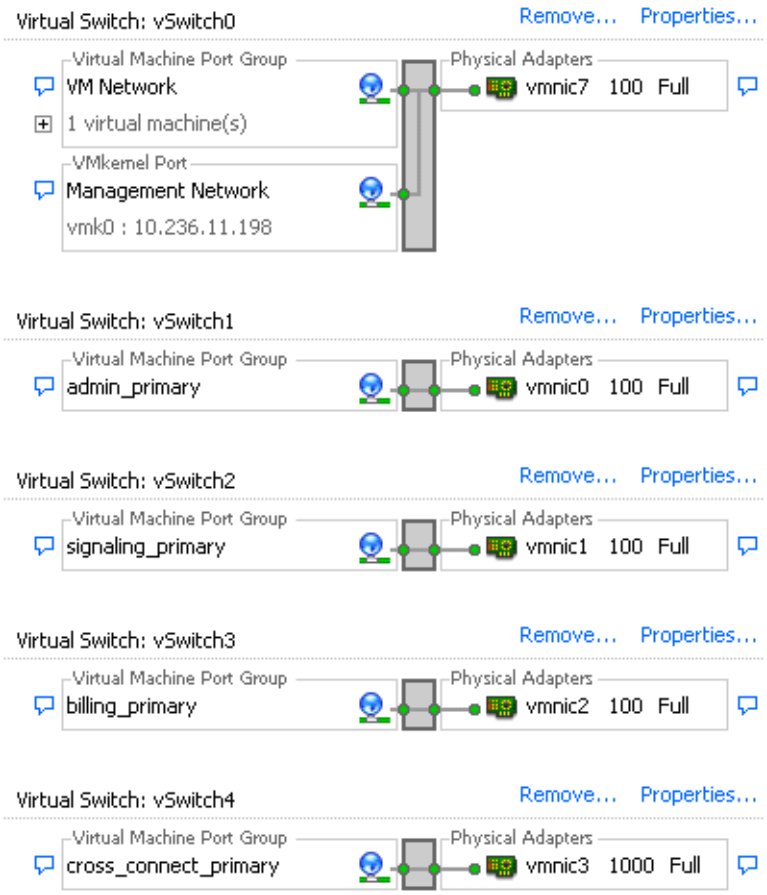
Subnet	Network Label
vmnic0	admin_primary
vmnic1	signaling_primary
vmnic2	billing_primary
vmnic3	unused3

Table 14 Network Labels - Integrated Simplex VM with Separate Subnets (3 port) configuration example

Simplex: The Virtual Switch preparation for a Simplex OSV is complete. Please proceed to **Section 4.3.6.3, "Preparation of the VMware Guest Machines - One Physical Server Solution", on page 207**.

- Example:

  The following is an example of the completed VMware switch preparation:



10. **Duplex:** Repeat the same procedure on the second physical server, naming the interfaces (for example) as follows:

Subnet	Network Label
vmnic0	admin_secondary
vmnic1	signaling_secondary
vmnic2	billing_secondary
vmnic3	cross_connect_secondary

Table 15 *Network Labels Secondary Server - Standard Duplex VM deployment Node 2*

4.3.6.2 Preparation of the VMware Virtual Switches: Co-Located with one Physical Server

Conduct the steps 1 - 9 described in Section 4.3.6.1, “Preparation of the VMware Virtual Switches: Two Physical Servers Setup (Co-Located or Geo-Separated)”, on page 191 to create the virtual switches for the admin, signaling and billing subnets.

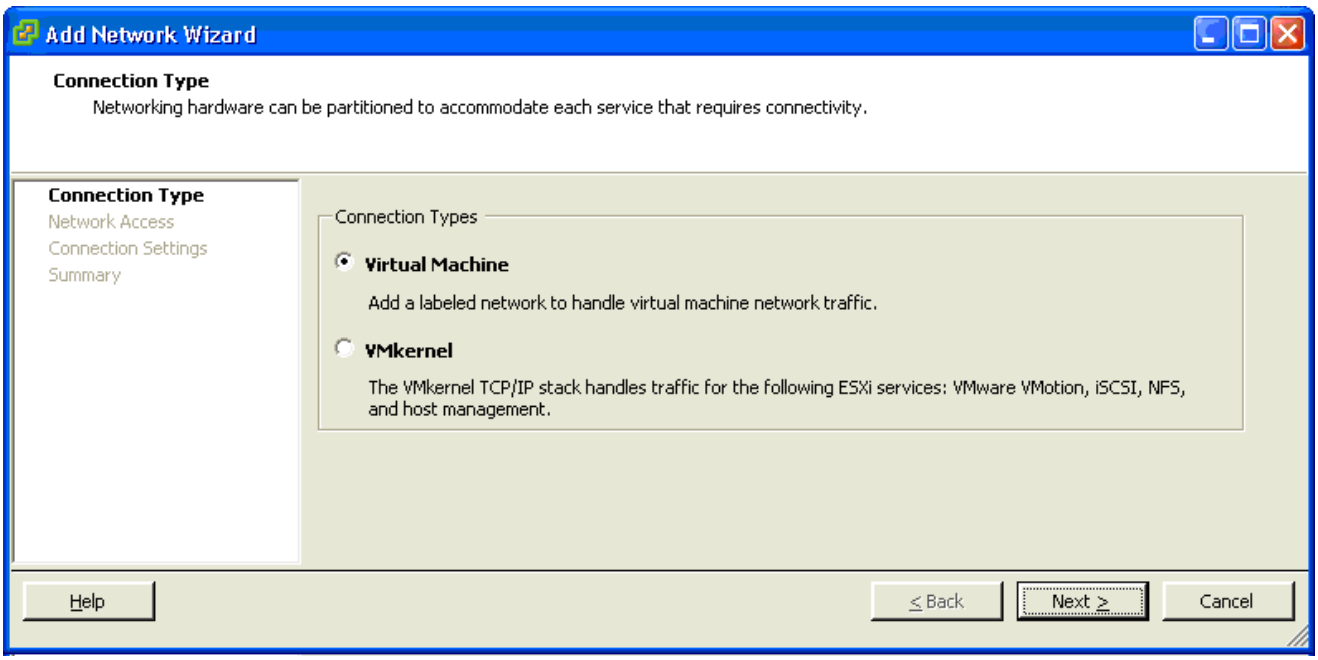
Attention: The cross-connect virtual switch is not required in a virtual simplex deployment. To create the simplex deployment virtual switches for the admin, signaling and billing subnets, refer to Section 4.3.6.1, “Preparation of the VMware Virtual Switches: Two Physical Servers Setup (Co-Located or Geo-Separated)”, on page 191, steps 1 - 9 .

After the simplex virtual switches are prepared users will be directed by a doclink to Section 4.3.6.3, “Preparation of the VMware Guest Machines - One Physical Server Solution”, on page 207.

Follow the procedure below for the cross-connect virtual switch:

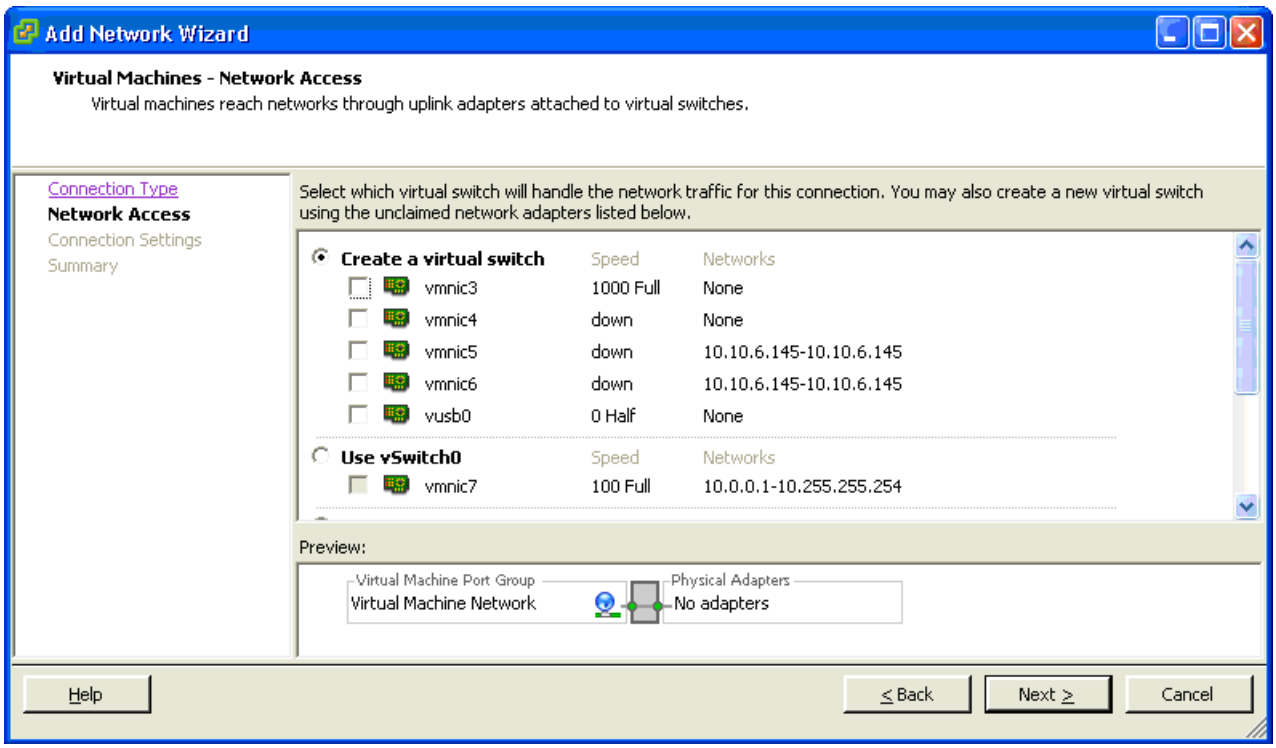
1. Select the ESXi servers Management IP address and click on the **Configuration** tab.
2. Select **Networking** in the **Hardware** menu.
3. Click on the “**Add Networking**...” option located in the top right segment.

The **Add Network Wizard - Connection Type** window appears:

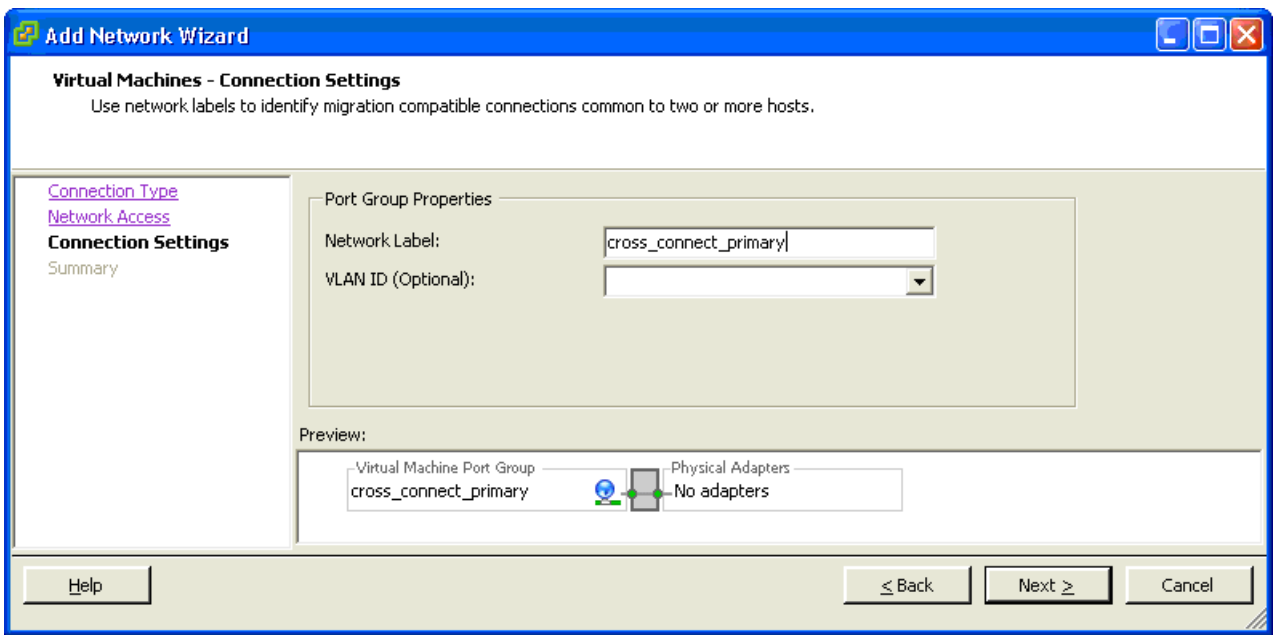


4. Select the **Virtual Machine** option for the connection type and click the **Next** button.

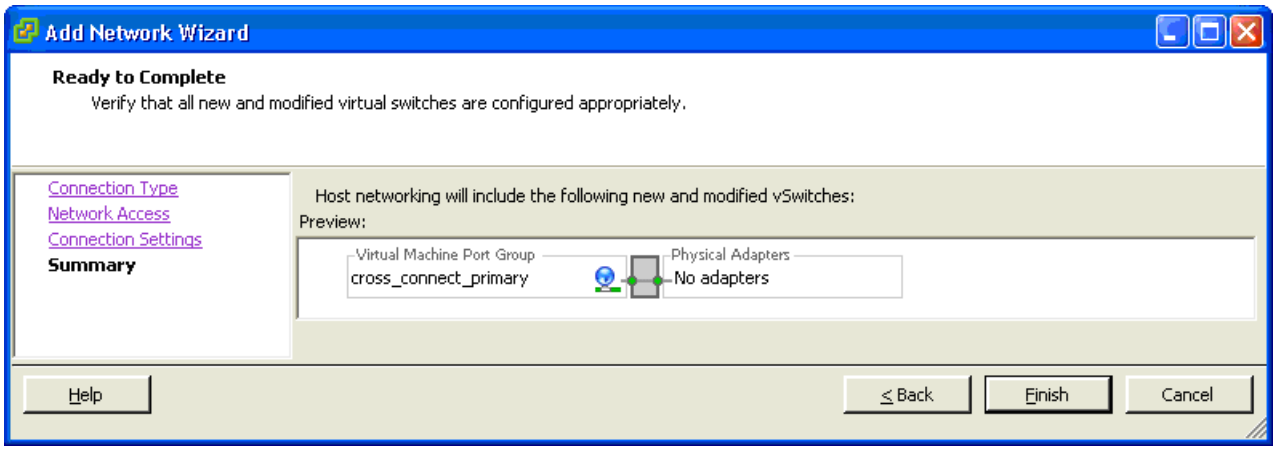
   The **Virtual Machines - Network Access** dialog appears.



5. De-select vmnic3 and click on the **Next** button.
   The **Add Network Wizard – Connection Settings** dialog appears:

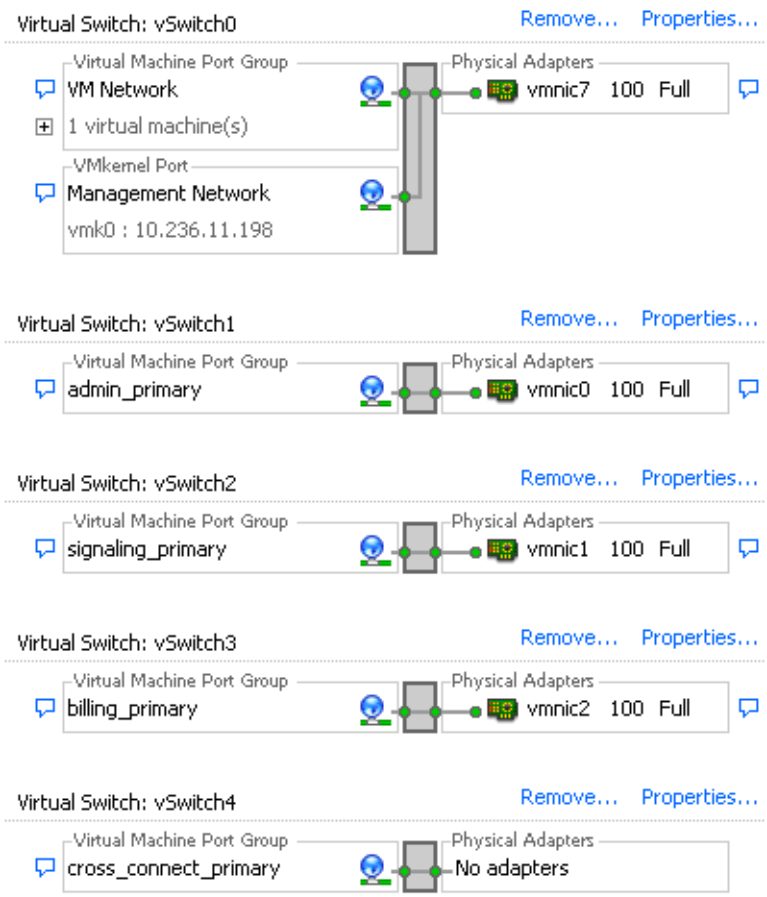


6. Enter `cross_connect_primary` in the **Network label** field and click the **Next** button. The **Add Network Wizard – Ready to Complete** dialog appears.



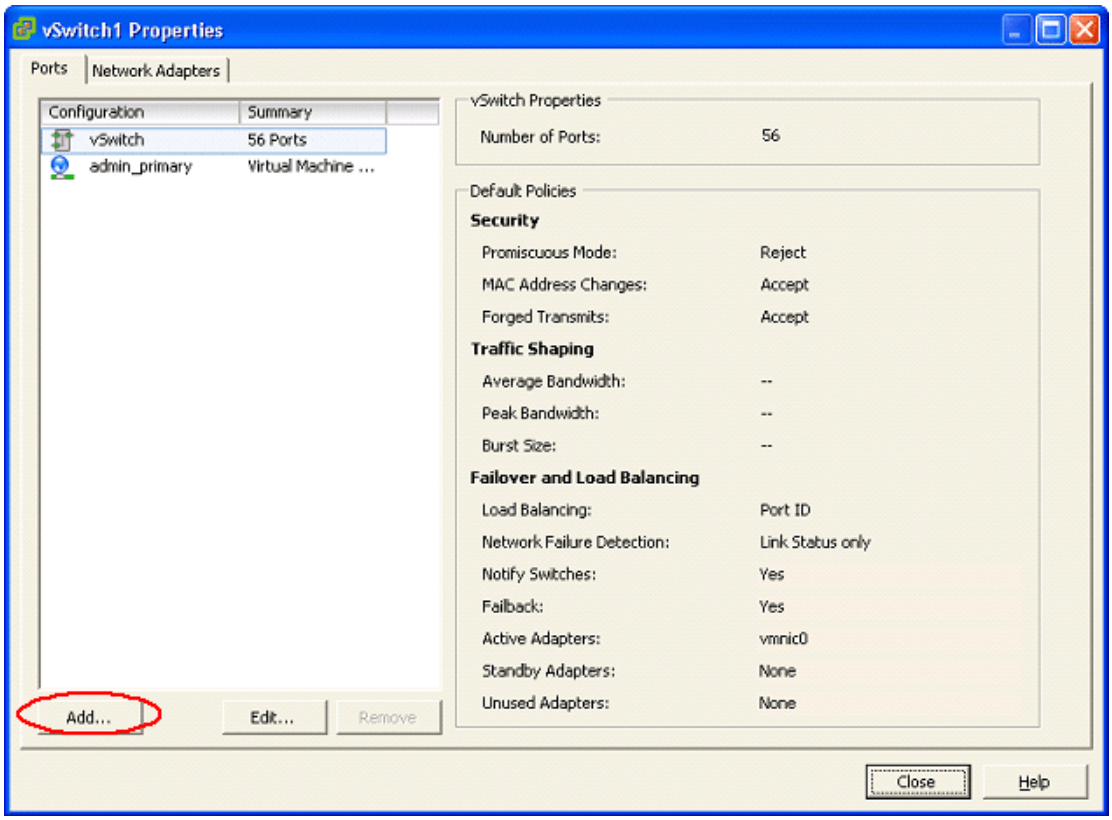
7. Click the **Finish** button.

   The following is an example of the completed virtual switches:



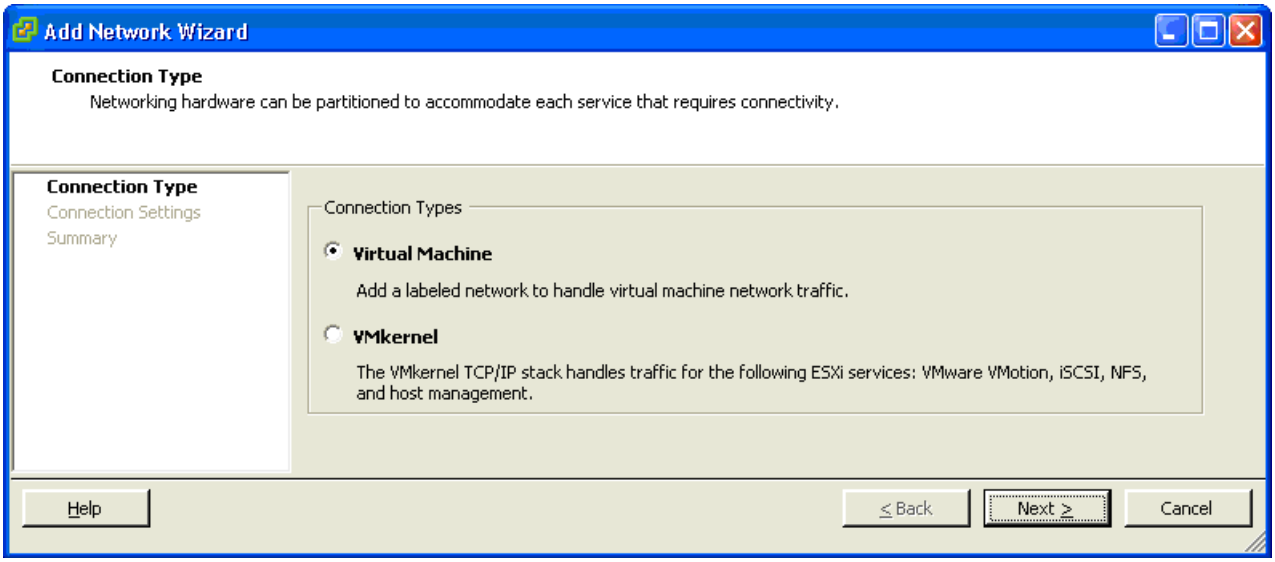
8. Since both the servers will be maintained on the same physical server, connections for this server on the virtual switches have to be created. In order to do this continue the configuration as follows:

   - Click on **Properties ...** for vSwitch1
   - The **vSwitch1 Properties** window appears.

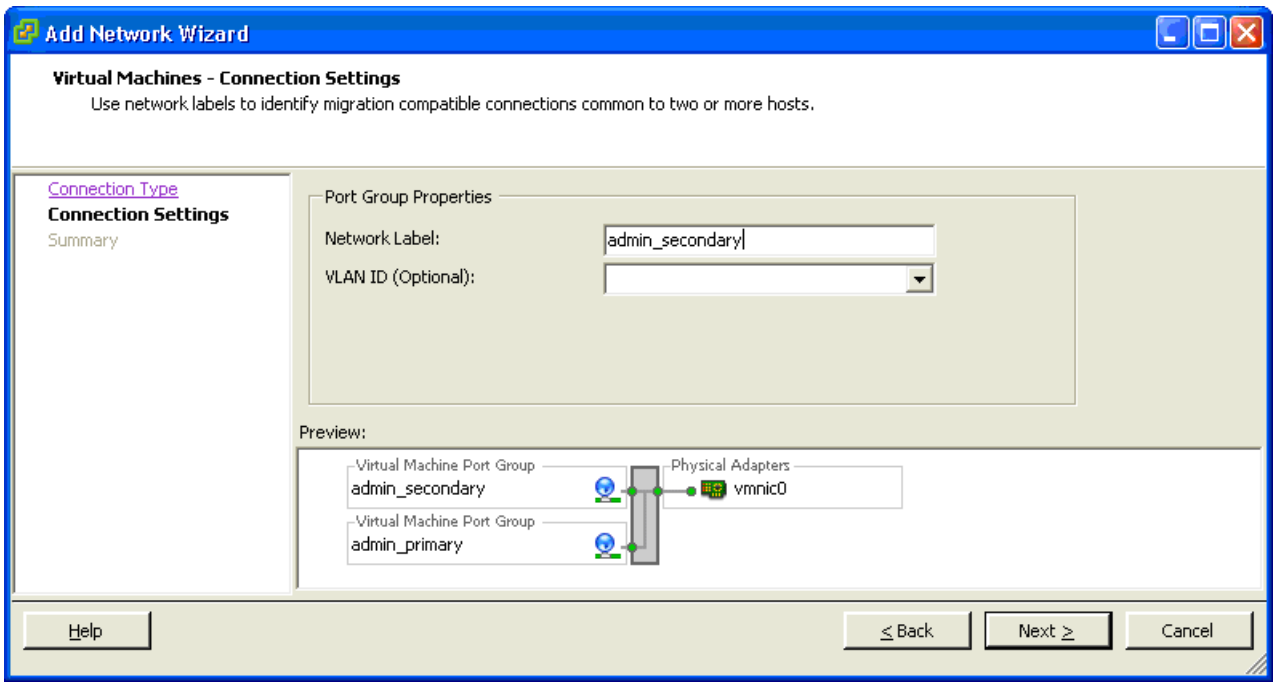


9. Click on the **Add...** button.

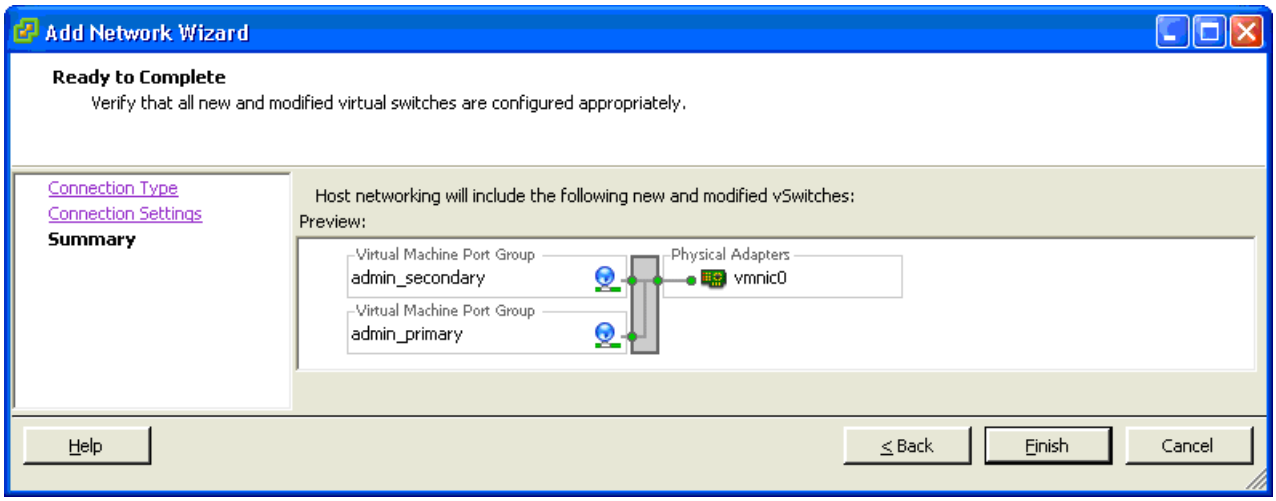
   The **Add Network Wizard - Connection Type** window appears:



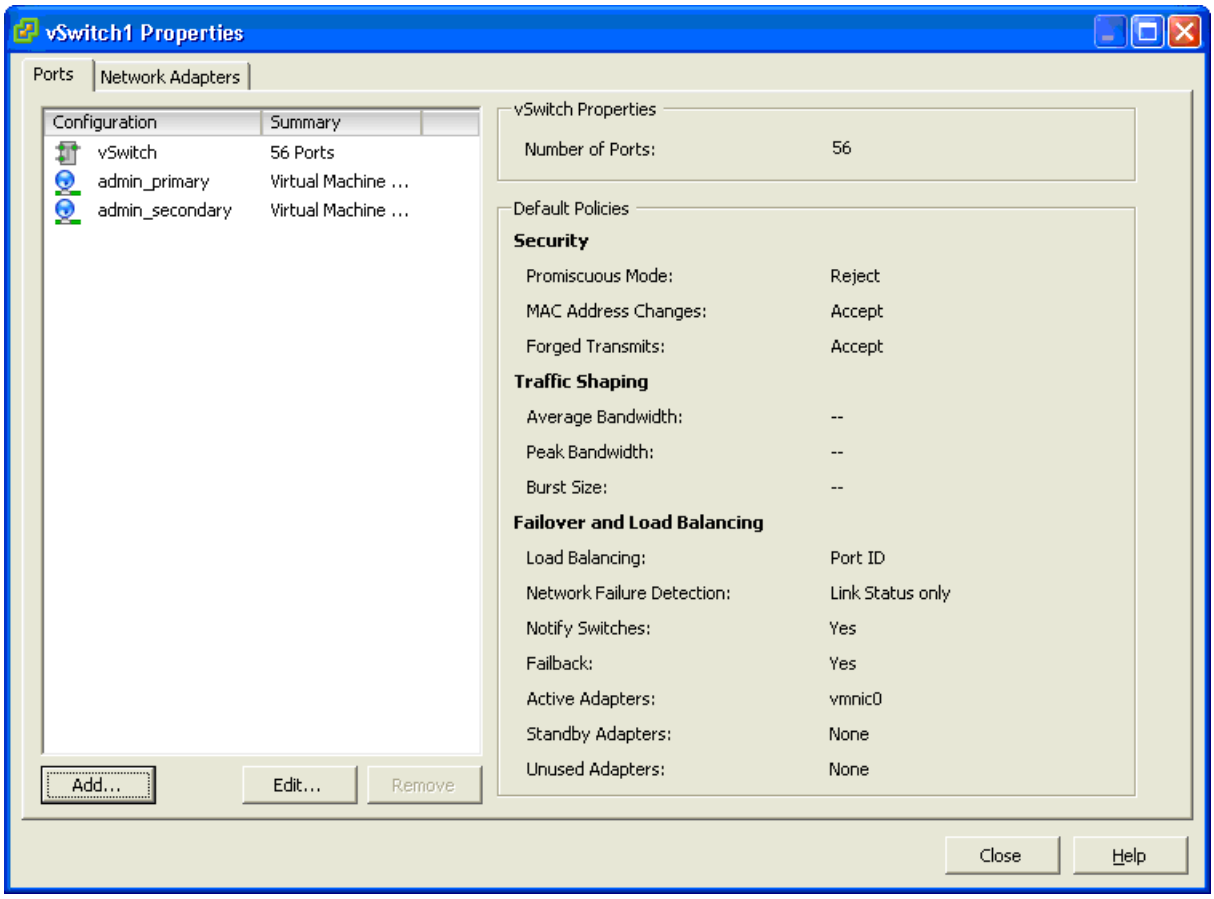
10. Click on the **Next** button.



11. Enter `admin_secondary` in the **Network label** field and click the **Next** button. The **Add Network Wizard – Ready to Complete** dialog appears.



12. Click the **Finish** button. The **vSwtch1 Properties** window appears containing the new connection.

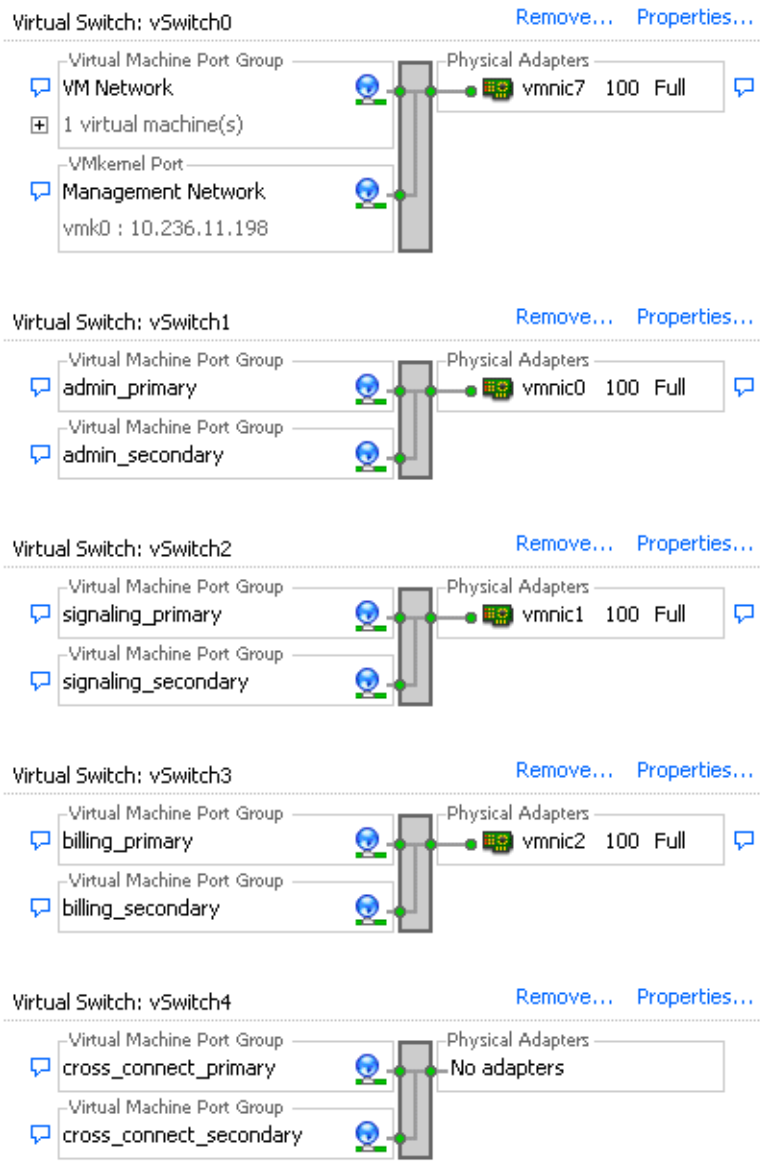


13. Click the **Close** button.

14. Repeat the procedure for the remaining Virtual Switches, in turn creating:

- signaling_secondary
- billing_secondary
- cross_connect_secondary

15. In the end your configuration should look like the following:



4.3.6.3 Preparation of the VMware Guest Machines - One Physical Server Solution

---

Note: These instructions apply to Duplex and Integrated Simplex OSV VM Guest preparation. Some of the steps have different headings like "**Duplex:**" and "**Simplex:**" depending on the VM system being prepared. Choose the selections listed for your VM deployment.

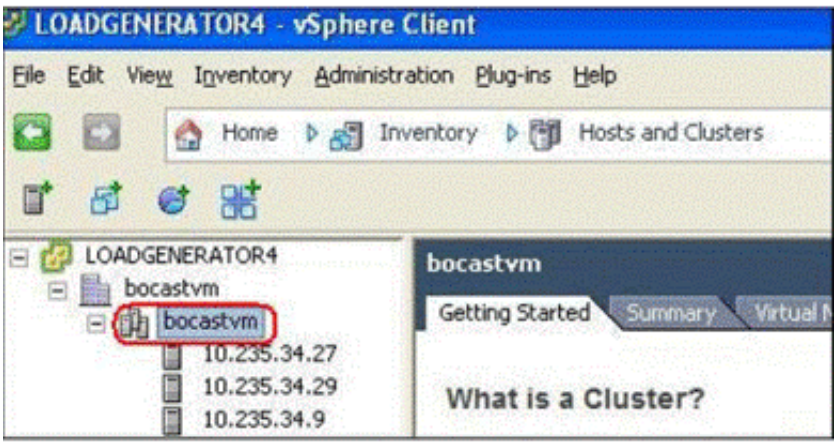
Attention: The following values are presented as examples only. The values may require adjustment based on a site's particular installation environment. Document *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide* lists the configuration parameters needed to configure each OpenScape Voice node.

Attention: Mandatory settings for these steps in this section.
- The virtual disk drive should be set to SCSI 0:0 in step 12.
- The CD/DVD Virtual Device Node should be set to IDE (0:0) in step 15.

Attention: Default values should be used during the configuration process unless specified otherwise. **U**sing other than the default values may result in unexpected behavior.

The Create New Virtual Machine wizard will be used to configure the virtualized OSV installations. This procedure assumes that the Datacenter and Cluster are already configured.

Select your Cluster (the cluster element is with in the red border in the following figure.)



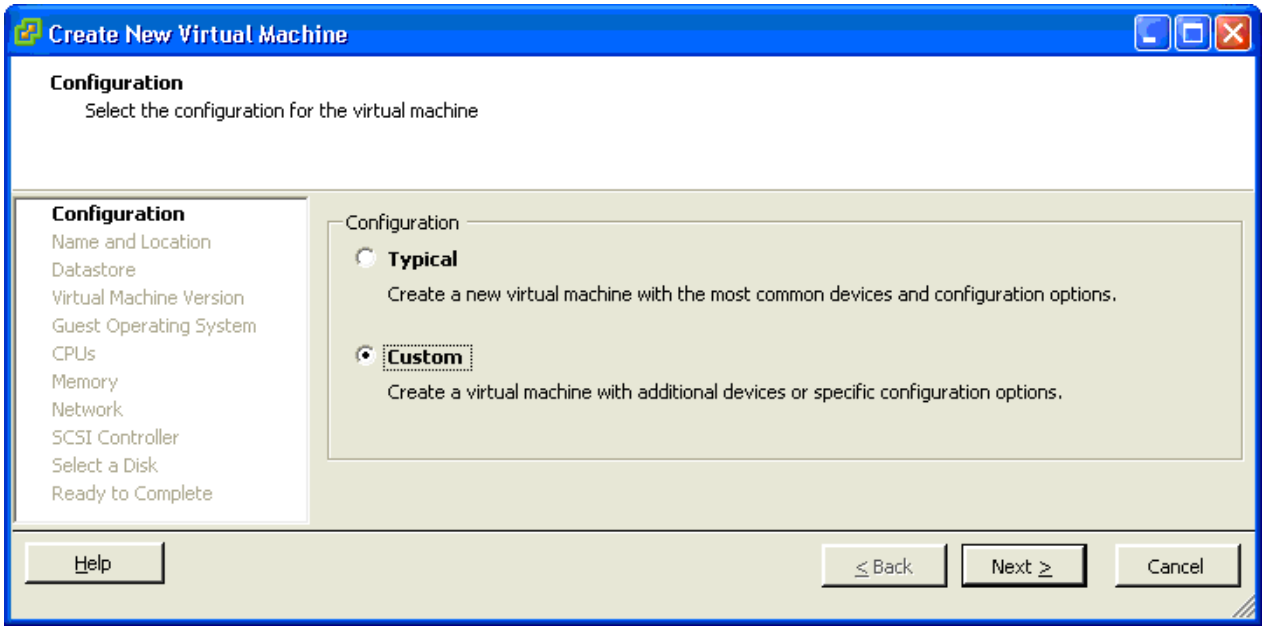
Access the **Create New Virtual Machine** wizard from the vSphere Client menu after selecting your Cluster by one of two methods:

- **Right click the cluster icon and select "New Virtual Machine"**
- **Or from the vSphere Client Toolbar, select File → New → Virtual Machine**

Note: These steps will be repeated for the creation of the second node as well. The first time through the procedure, conduct the steps indicated as "step 1" wherever specified. When conducting the steps the second time around for Node 2, follow the steps indicated as "step 2" wherever specified.

Starting from the initial Create New Virtual Machine Wizard screen the following are the steps to configure the system:

1. **Configuration**: Select **Custom configuration**, then select **Next**.



2. **Name and Location:** Enter the name for the new virtual machine

   a) **step 1:** Enter `Node1`, then select **Next**.

   b) **step 2:** Enter `Node2`, then select **Next**.

   Note: “Node1” or “Node2” are user defined names.

3. **Datastore:** Select a data store with sufficient data size for the machine (see: Section 4.3.1, “Virtualization — Overview”, on page 171). After selecting the datastore size, select **Next**.

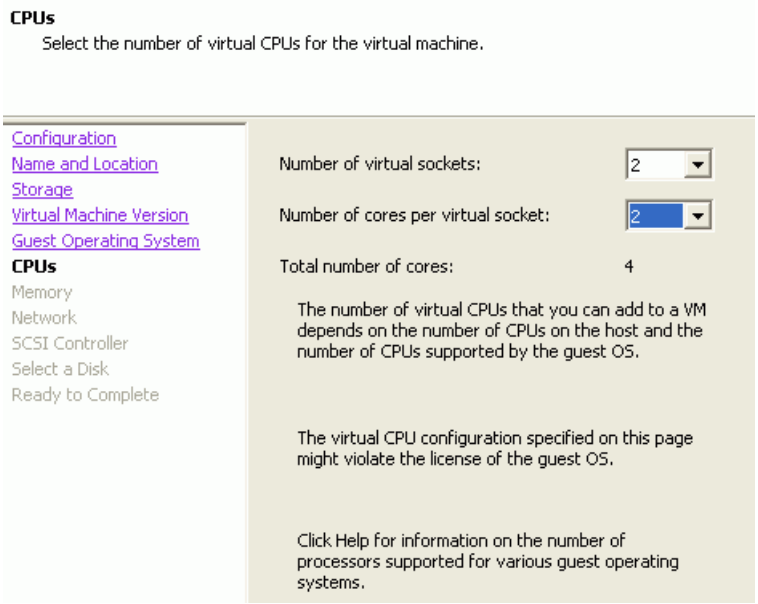
4. **Virtual Machine Version:** Select virtual machine version 8, then select **Next**.
5. **Guest Operating System:** Select **Linux** and version **SUSE Linux Enterprise 15 (64 bit)**. The OpenScape Voice Image is built with SLES 15 (64 bit). Select **Next**.

Note: Settings are based on values from the latest document *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide*, Virtual Machine Computer (minimum) Requirements for OpenScape Voice with OpenScape UC Suite for this release.

Note: For OpenScape Voice it is recommended to use SLES 15. For compatibility with VM Hardware Version, follow the link https://kb.vmware.com/kb/2007240. For OSV compatibility with ESXi please check chapter **Support VMware vSphere Versions** in the latest *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide*.

---

6. **CPUs:** Enter 4 for the number of virtual processors, then select **Next**. (Example below is for Version 8.)



Note: A 4 vCPU VM is configured with 2 virtual sockets and 2 cores per virtual socket, while an 8 vCPU VM is configured with 2 virtual sockets and 4 cores per virtual socket.

Note: Licensing for VMware is the responsibility of the customer.

---

7. **Memory**: Set the memory size to 9 GB for a virtual Duplex deployment or 10 GB for a virtual Integrated Simplex deployment, then select **Next**.
8. **Network choices:**

   Duplex: Select 4 Network adapters (NICs). Select the following choices from the NIC drop down lists as indicated below;

   a) step 1

   – NIC1 – admin_primary

   – NIC2 – signaling_primary

   – NIC3 – billing_primary

   – NIC4 – cross_connect_primary

   b) step 2

   – NIC1 – admin_secondary

   – NIC2 – signaling_ secondary

– NIC3 – billing_secondary

– NIC4 – cross_connect_secondary

Simplex: For an Integrated Simplex Virtual Machine there is no cross connect switch but the four NICs must be created. Examples of a one port and three port simplex virtual machine mapping are provided.

Integrated Simplex VM with All Subnets Shared (1 port) configuration example:

– NIC1 - admin_primary

– NIC2 - unused2

– NIC3 - unused2

– NIC4 - unused3

Integrated Simplex VM with Separate Subnets (3 port) configuration example:

– NIC1 - admin_primary

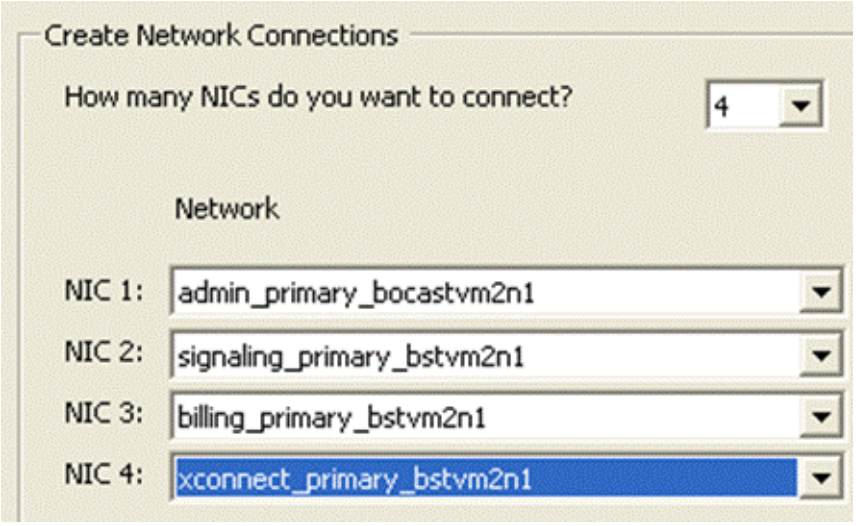
– NIC2 - signaling_primary

– NIC3 - billing_primary

– NIC4 - unused3

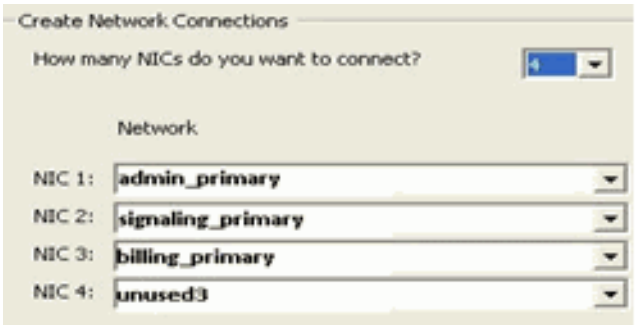
9. The order of the Network adapter to Network label is important and must match the order shown in the screenshot below **for all VMware installations**. After verifying the NIC configuration select **Next**.

   Duplex:



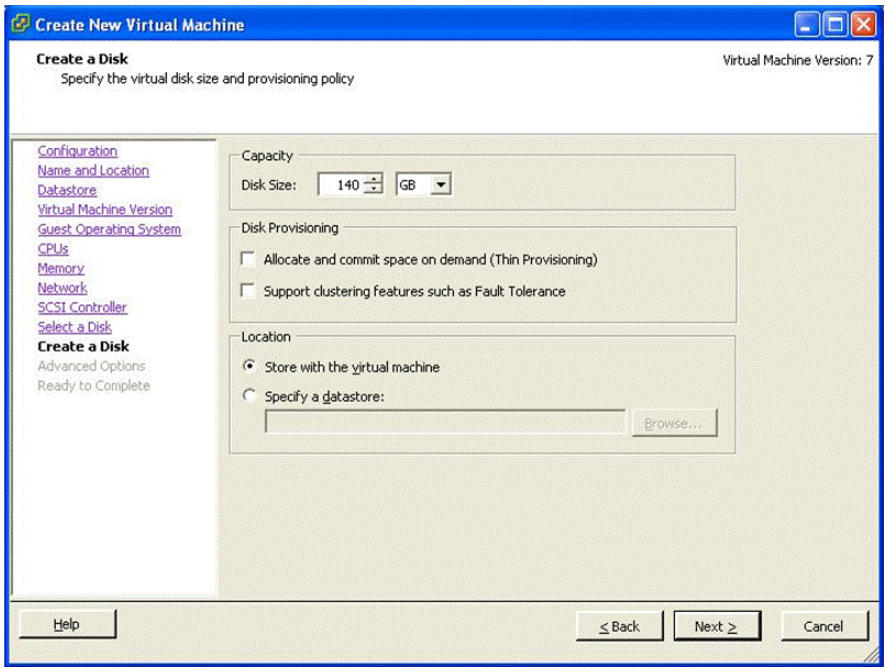
Simplex VM with Separate Subnets (3 port) configuration example:

Note: A 'not used' VMNIC ports should be labeled as such. For example, a Simplex VM with the All Subnets shared (1 port) configuration could label NIC2 'unused1' (VMNIC1), NIC3 'unused2' (VMNIC3) and NIC4 'unused3' (VMNIC3).



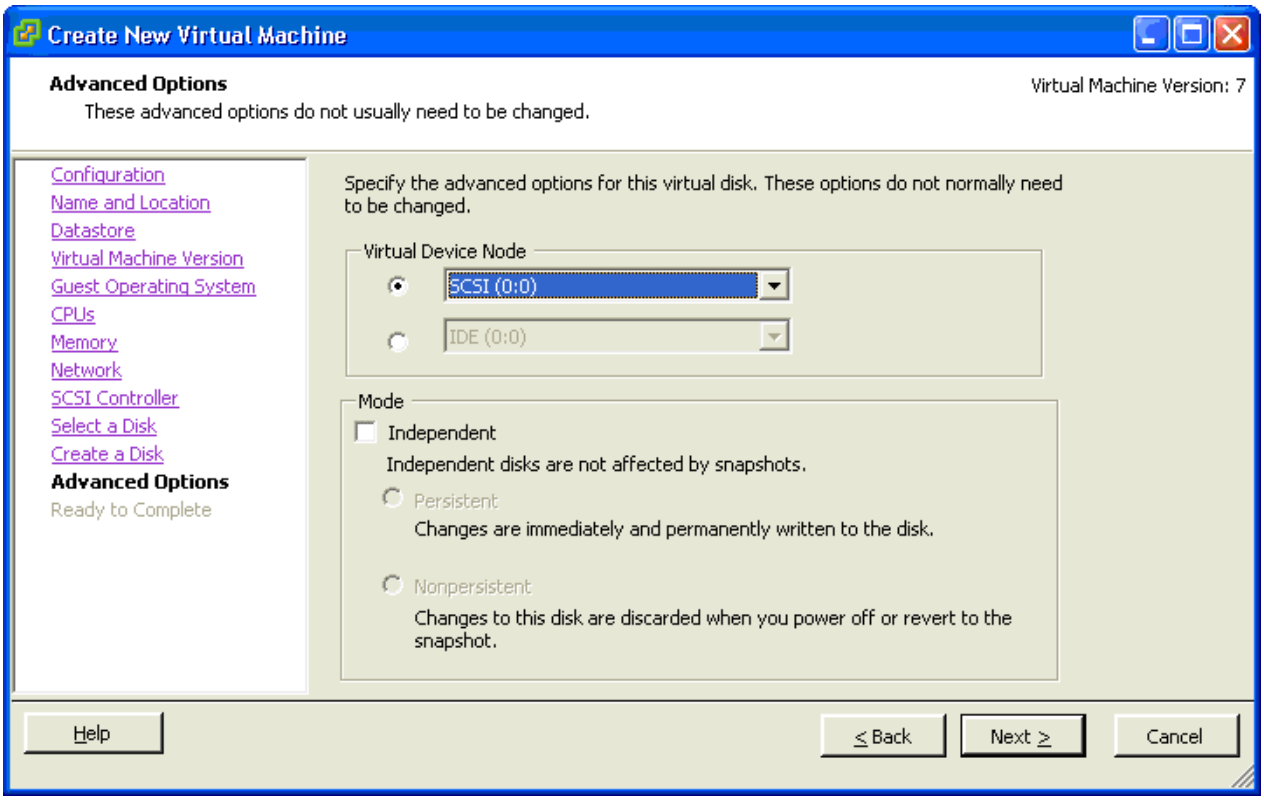
10. **SCSI Controller:** use defaults, select **Next**.

11. **Select a Disk:** Select **Create a new virtual disk**. Select **Next**. The **Create a Disk** window appears:



- **Create a Disk:** For the Capacity parameter select a Disk Size of **140 GB**
- Use the default selections for the remaining choices.

12. Select **Next**. The **Advanced Options** window appears.



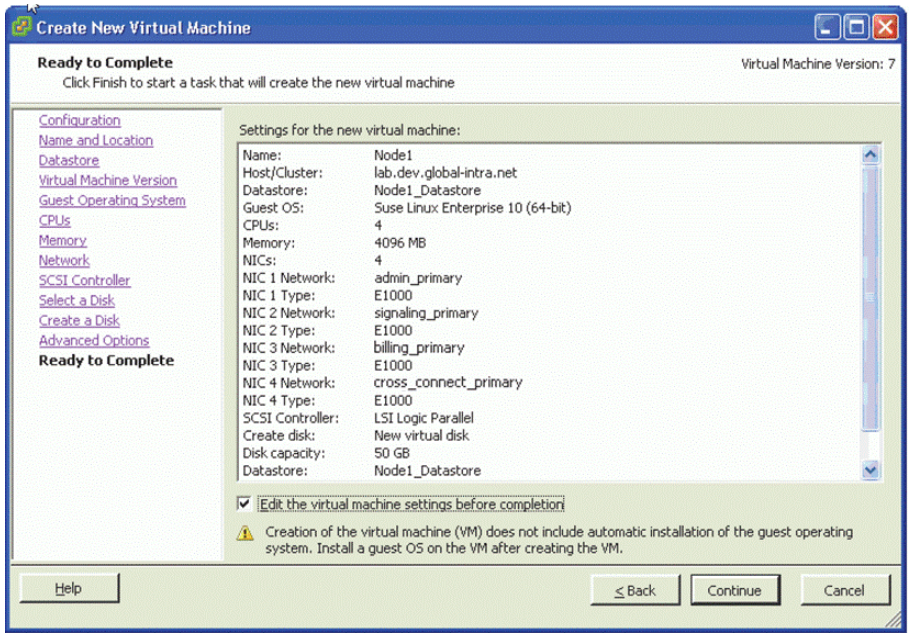
Note: The Virtual disk mode setting "Independent" disallows the creation of Snapshots of a virtual machine. For a customer environment, it is recommended the Mode settings are NOT selected. This is the default configuration.

Mode Independent Persistent will leave changes permanently written to disk.

Mode Independent Non-persistent writes data to disk but the data will be eliminated on restart (good for a training or demo environment).

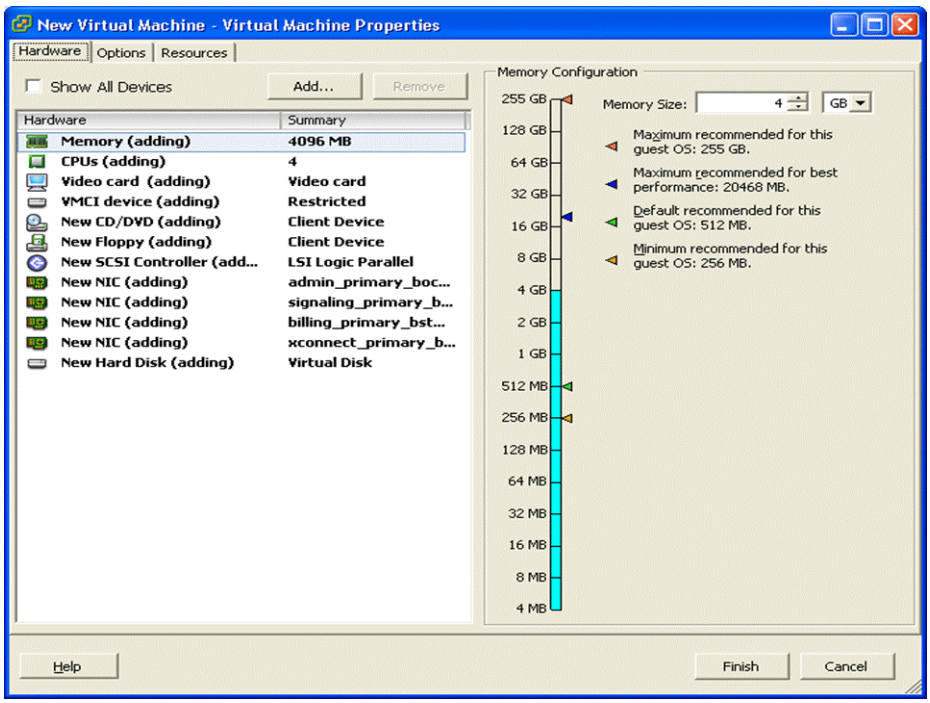
- **Advanced Options:** use the default values.

13. Select **Next**. The **Ready to Complete** window appears.



- **Ready to Complete**: The configuration summary of the new virtual machine is displayed.
- Check the “Edit the virtual machine settings before completion” checkbox as shown.

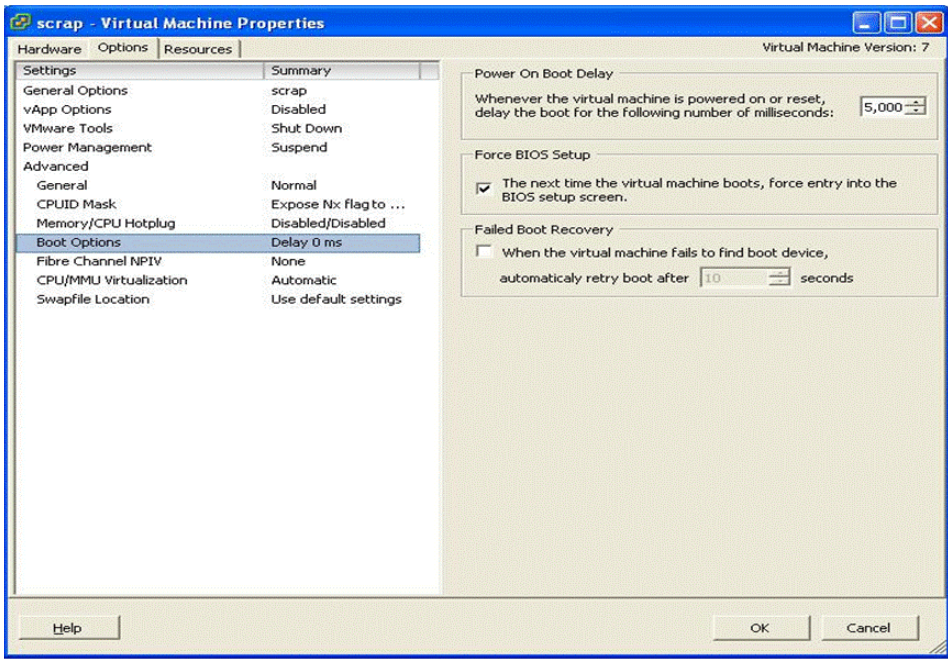
14. Select **Continue**. The **Virtual Machine Properties** window appears.



- Select the **Hardware** tab.
- In the **Hardware** tab, select **New CD/DVD**
  - Select **Datastore ISO File** and browse to the previously downloaded OpenScape Voice ISO image to be installed.
  - Select the **Connect at power on** checkbox under **Device Status**.
  - Change the Virtual Device Node to IDE (0:0)

15. Virtual Machines will use the 'Advanced Locking Identification' (ALI) concept for licensing. Note that more information regarding the ALI can be found in Section 20.2, “Virtual OSV Server”. There is a link back to this page at the end of Appendix 20.

16. Select the **Options** tab.



- In the **Options** tab select **Boot Options**.
- Set **Power-on Boot Delay** to 5000
- Check the **Force BIOS Setup** checkbox

17. Select the **Resources** tab.

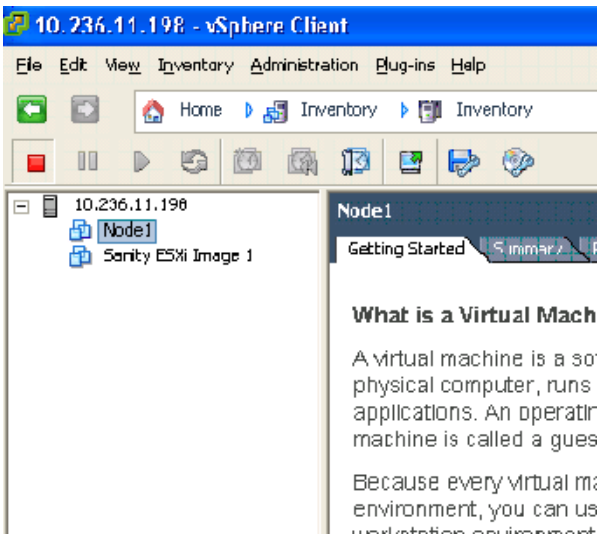
    - In the **Resources** tab select **CPU**.

    Note: Settings are based on values from the latest document *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide*, Virtual Machine Computer (minimum) Requirements for OpenScape Voice with OpenScape UC Suite for this release.

18. In the **Resources** tab, select **Memory**.

    Note: Settings are based on values from the latest document *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide*, Virtual Machine Computer (minimum) Requirements for OpenScape Voice with OpenScape UC Suite for this release.

19. Click **Finish** to create the new VM. VMs will appear on the left hand side of the vSphere Client dialog, e.g., Node 1.



20. For Duplex Virtual Machines, repeat the steps of Sect. 4.3.6.3 following "**step 2 on page 209**" wherever specified in order to create the Node2 VM.

    This completes the VMware Guest preparation for an Integrated Simplex VM.

    If you plan to use an ISO for the installation node.cfg please review **Section 4.3.6.5, "Adding a CD/DVD Drive to the Virtual Machine", on page 223** (if you have not already done so). After reviewing **Sect. 4.3.6.5 proceed to Section 4.3.6.6, "Loading the Image on the VMware Guest Machine", on page 229.**

4.3.6.4 Preparation of the VMware Guest Machines - Two Physical Server Solution

In order to save space and not repeat the equivalent steps from Section 4.3.6.3, "Preparation of the VMware Guest Machines - One Physical Server Solution", setup we will only specify the differences, that must be conducted in order to create the 2 Physical Server Solutions VM nodes, here.

The first time through Section 4.3.6.3, you will create Node1 and second time through, Node2 will be created. Please follow the step specified as “step 1” wherever indicated first time through and the step specified as “step 2” second time through the procedure.

Attention: Your settings should be based on values from the latest document *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide*.

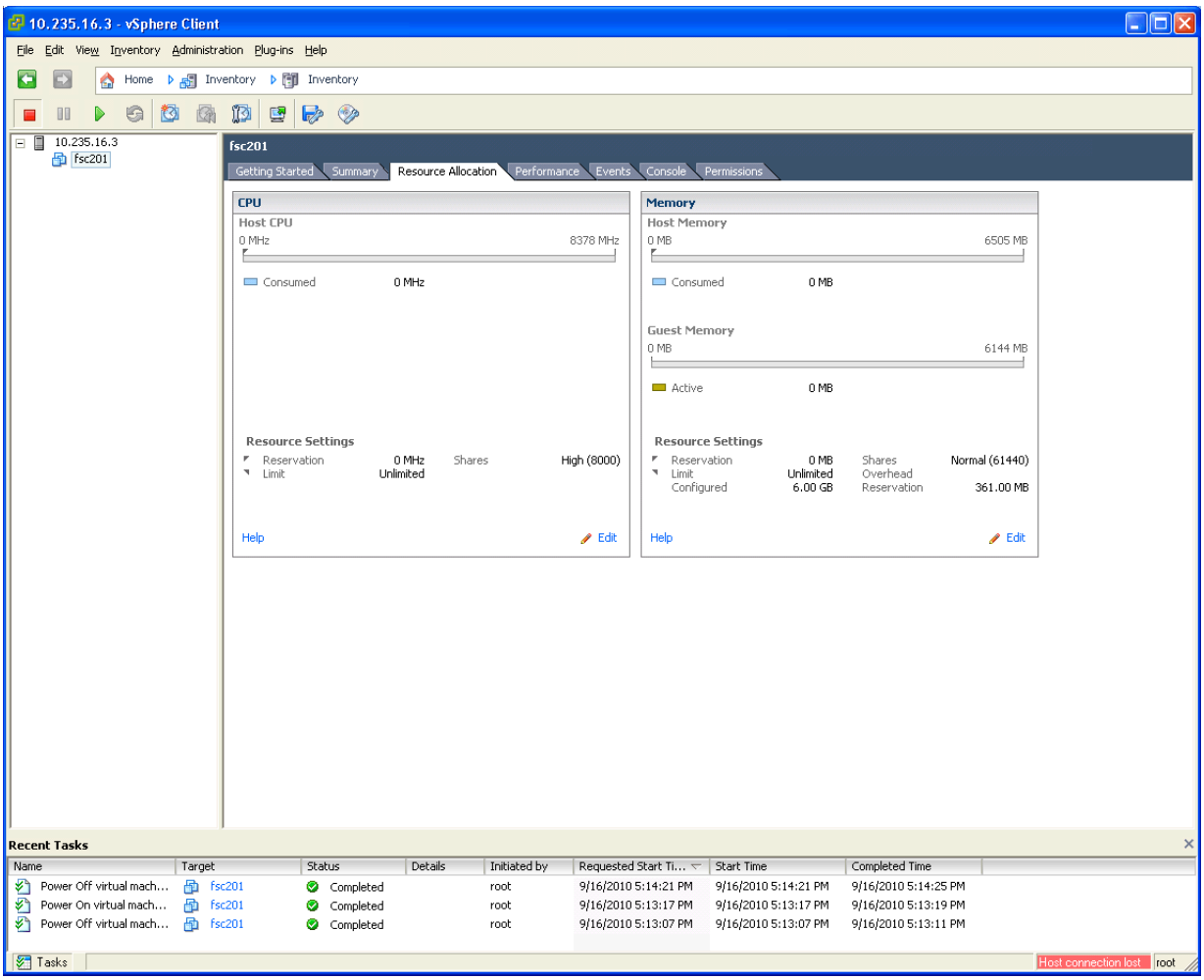
4.3.6.5 Adding a CD/DVD Drive to the Virtual Machine

This section can be employed to make a node.cfg ISO file available on a virtual CD/DVD device. Section 4.3.6.3, “Preparation of the VMware Guest Machines - One Physical Server Solution”, step 14 on page 218, provides instruction to add a virtual CD/DVD device for the OpenScape Voice iso file. If you are following the Installation and Upgrades Guide, Section 4.3.6.3, “Preparation of the VMware Guest Machines - One Physical Server Solution”, step 14 on page 218 should already be complete.

Attention: The VM OSV node must be powered down. This procedure must be completed on both nodes of a duplex system.

---

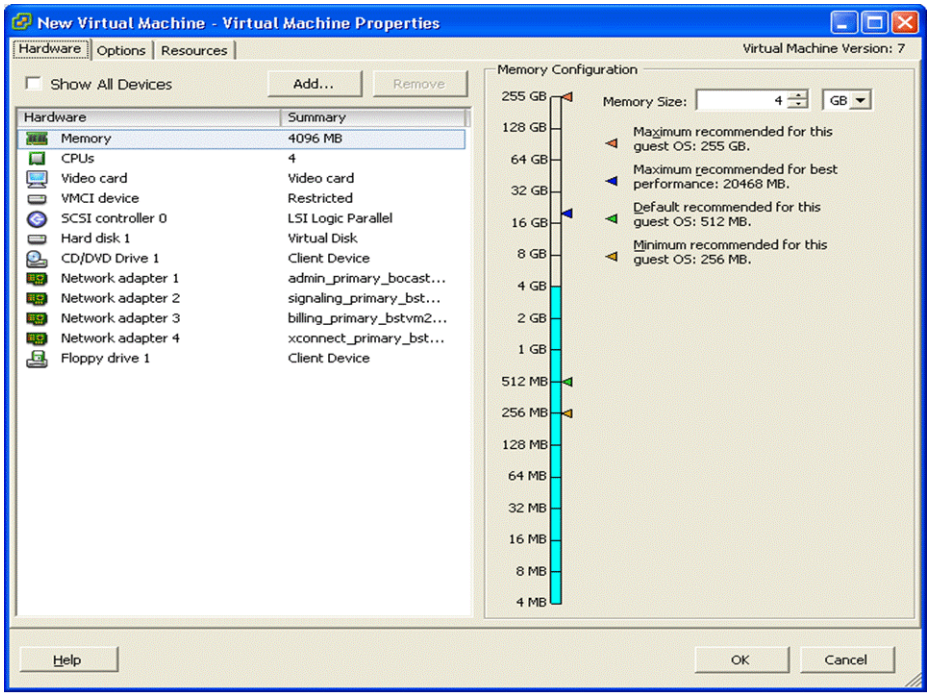
1. Access the vSphere client.



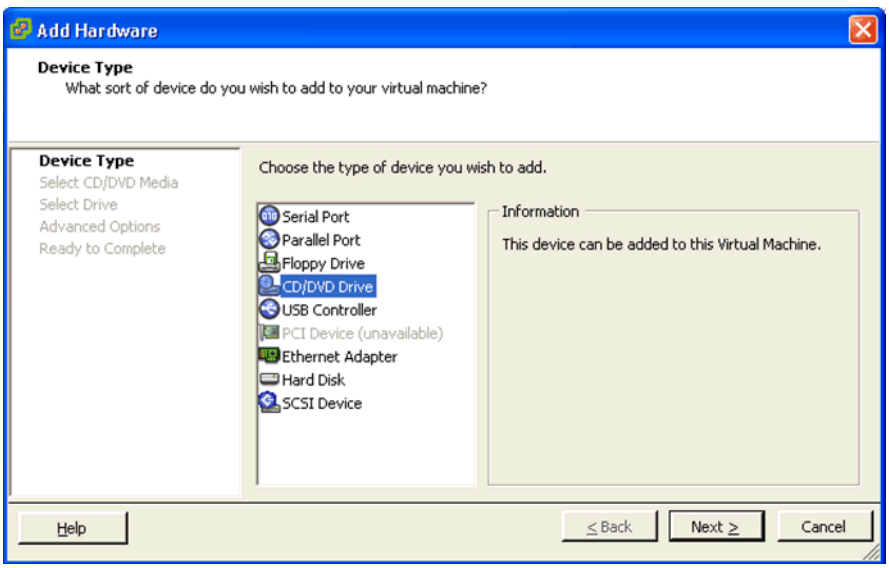
- Select the appropriate node.
- Select the **Resource Allocation** tab.

- Select **Edit** in the CPU (or Memory) window.

2. The **Virtual Machine Properties** window is displayed, select the **Add** button.



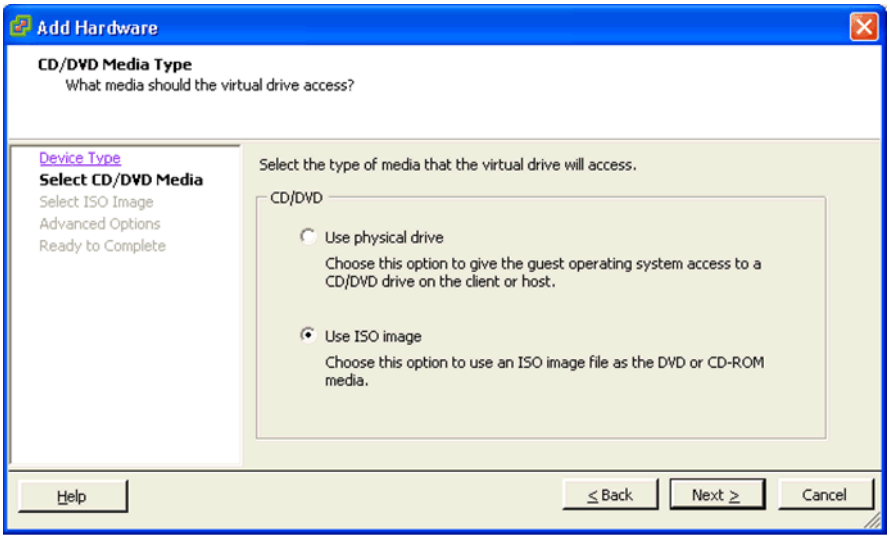
3. The **Add Hardware Device Type** window is presented.



On the **Add Hardware Device Type** window select/highlight **CD/DVD Drive**.

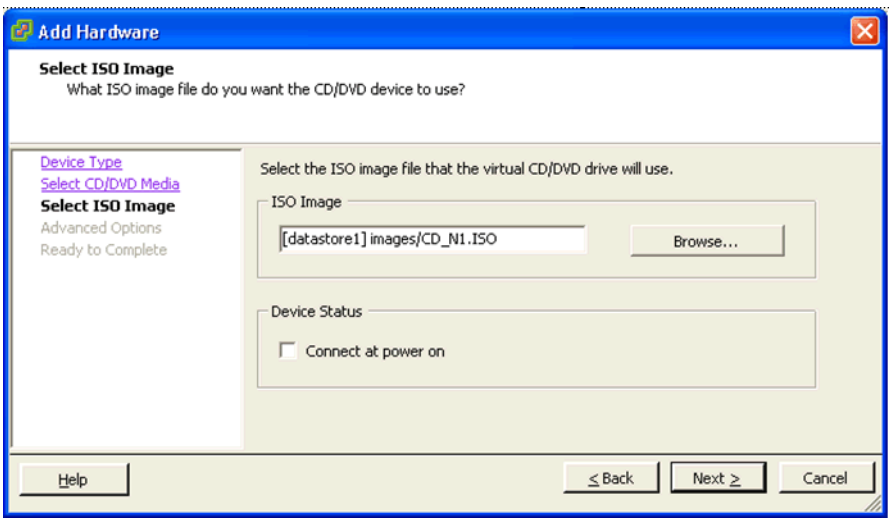
4. Select the **Next** button.

   The **Add Hardware CD/DVD Media Type** window is presented;



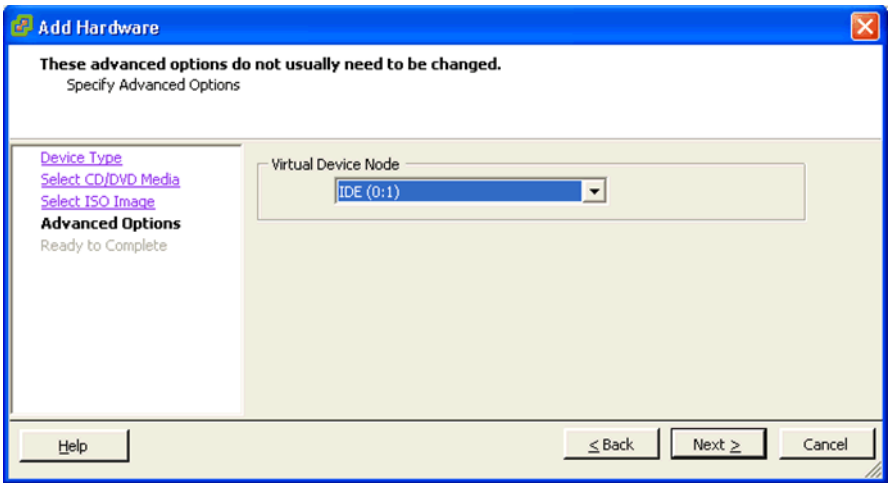
   Select the **Use ISO image radio** button.

5. Select the **Next** button. The **Add Hardware Select ISO Image** window is presented;



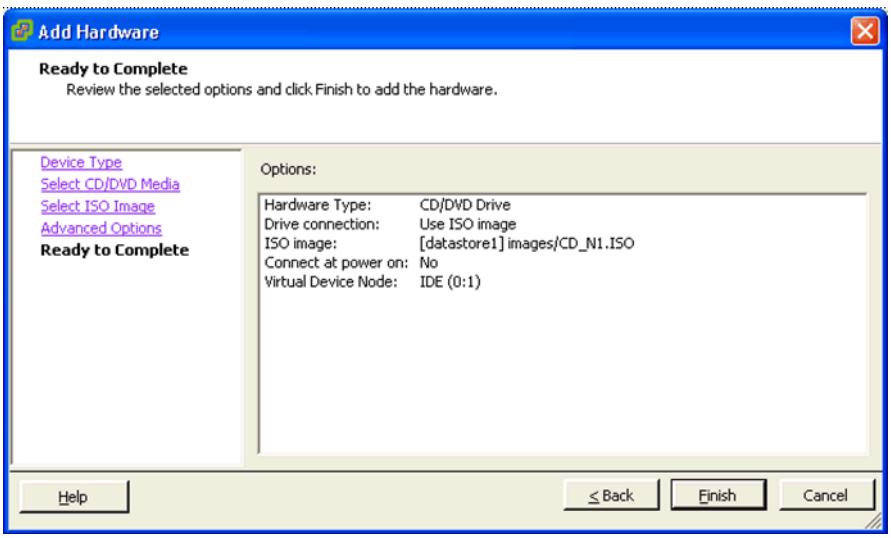
   - Browse to and select the appropriate ISO image for this activity.
   - **Do NOT select the “Connect at power on” radio button**.

6. Select the **Next** button. The **Add Hardware Specify Advanced Options** window is presented;



The expected value of "**Virtual Device Node**" is IDE (0:1). Typically this is the default value.

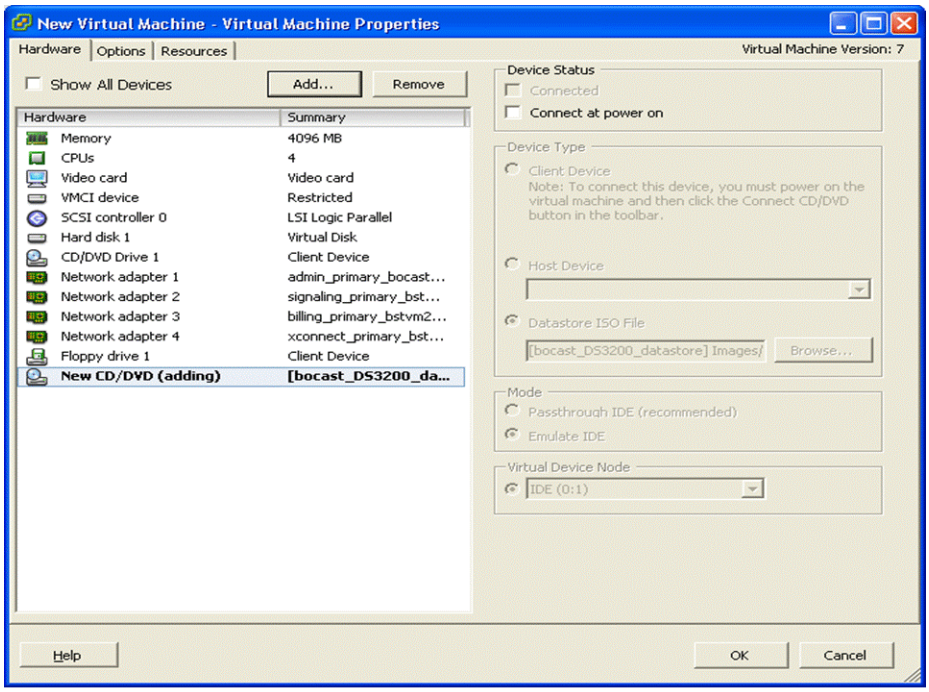
7. Select the **Next** button. The **Add Hardware Ready to Complete** window is presented;



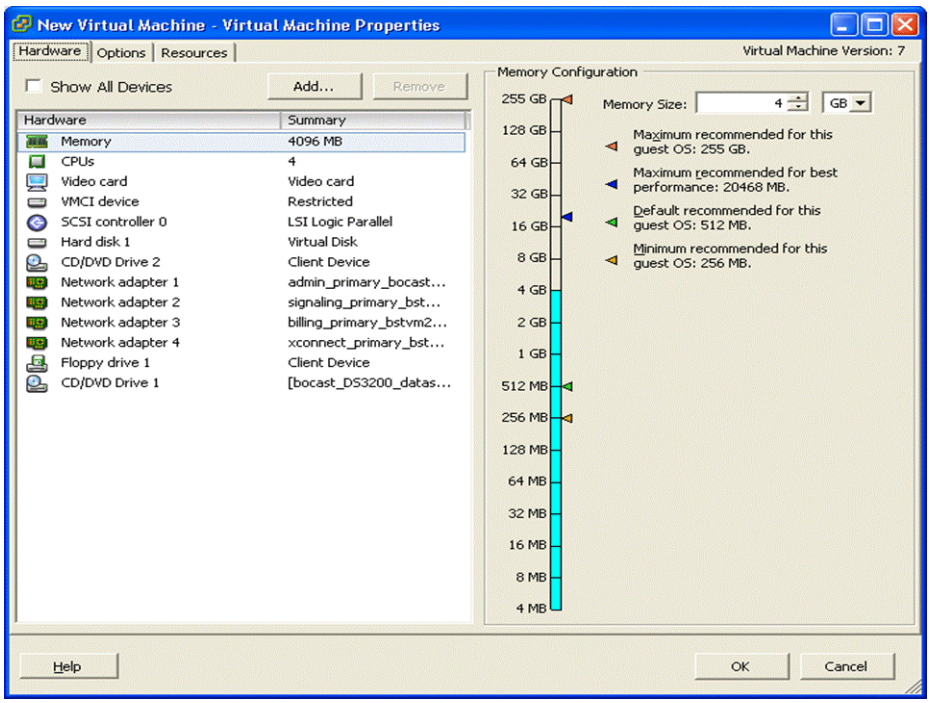
- Verify the options settings are listed correctly. Refer to the snapshot above.
- If any options are different than those presented here, use the **Back** button to update that option accordingly and then return to this page. It is a good practice to verify the options once more (the best check is a double check).

8. After verifying the options are correct, select the **Finish** button. The **Virtual Machine Properties** window is presented. The 'new' CD/DVD should now be present in the Hardware list.

   Select the **OK** button.



9. If you return to the vSphere top level and select **Edit** in the CPU (or Memory) window, the Virtual Machine properties are displayed as:



Attention: This procedure must be completed on both nodes of a duplex system.

Note: This link will take you to: step d on page 736 in Section 24.2, “Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)”.

Note: This link will take you to: Section 24.3, “Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration”, on page 738.

4.3.6.6 Loading the Image on the VMware Guest Machine

Follow the instructions described in Section 4.2.3.3, “Virtual systems via Virtual CD/DVD”

4.3.6.7 Virtual Machine Post Installation Best Practices

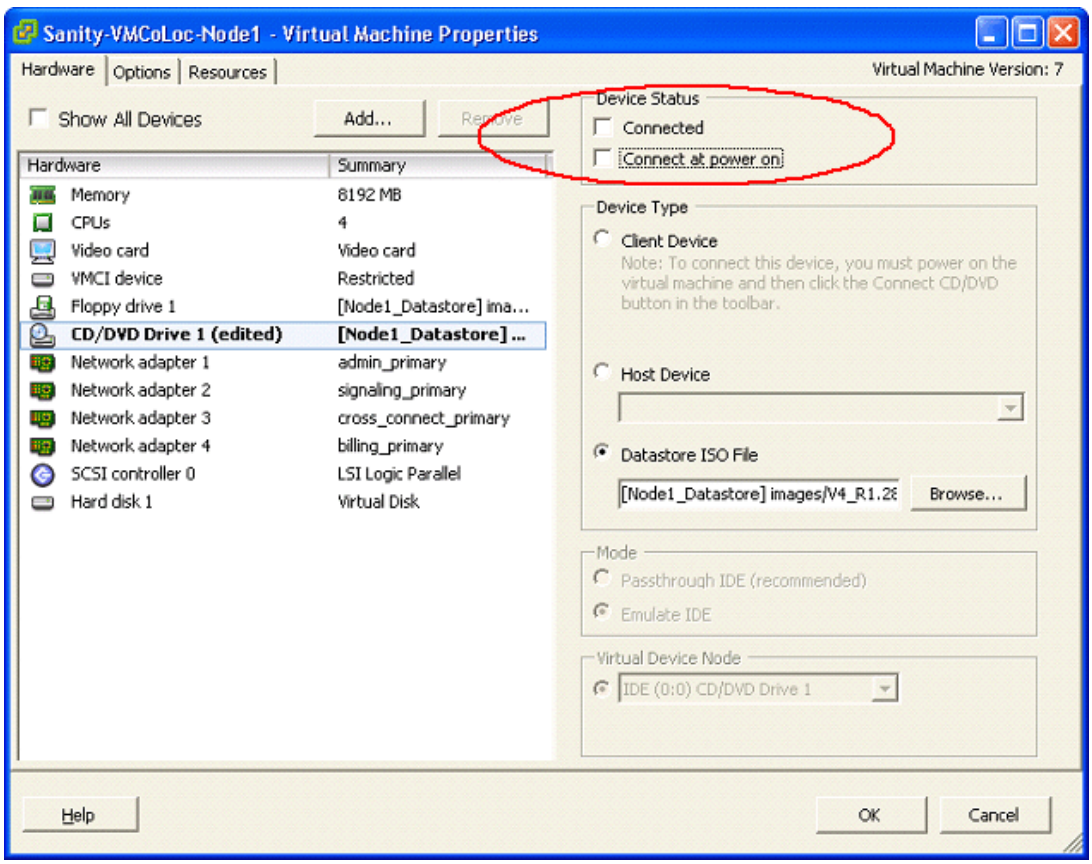
Increasing Node Boot-Up Speed

After the installation completes, several steps can be taken to speed up the Node Boot-Up time if the servers were ever rebooted.

1. Disconnect the CD/DVD device and prevent it from connecting during boot.

   a) First click the nodes Edit Virtual Machine Settings and select the **CD/DVD Drive** where the Image ISO was connected.

   b) Uncheck the **Connected** and **Connect at power on** checkboxes inside device status.



2. Select the **Options** tab.

a) Select **Advanced**, **Boot Options**.

b) Set the **Power-on Boot Delay** time value to **1000**.

3. Click the **OK** button.
4. Repeat steps 1 through 3 on the other node.
5. On the OpenScape Voice Installation Checklist, in Section 2.2.4, “OpenScape Voice Installation Checklist”, on page 30, initial step 8 on page 32 and proceed to step 9 on page 33. Perform the tasks required for your installation environment.

4.3.7 Create a Virtual Machine in Proxmox

Note: The instructions of this chapter apply to Duplex and Integrated Simplex OSV VM Guest preparation. Sections of this chapter with headings such as "Duplex" or "Simplex", describe different configuration settings based on the VM system being prepared. Choose the appropriate section for your VM deployment.

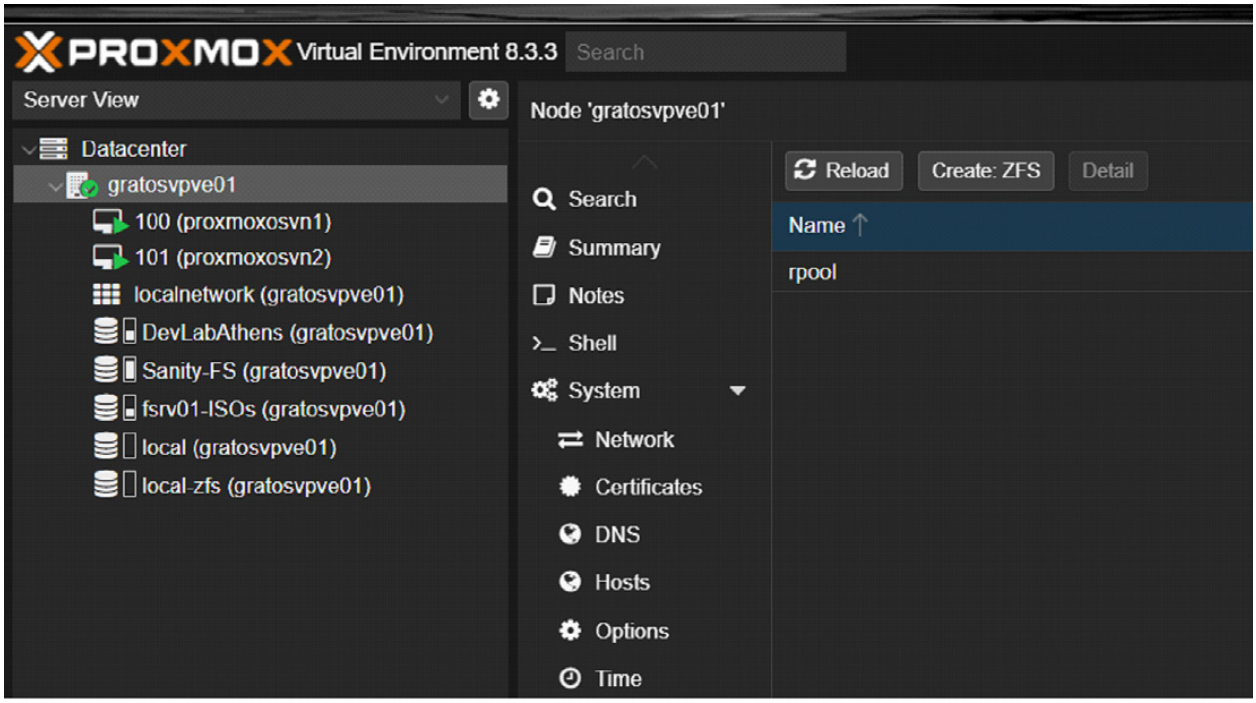
Attention: The values configured in the following steps are presented as examples. These values may require adjustment based on a site's particular installation environment. The *OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide* document, lists the configuration parameters needed to configure each OpenScape Voice node.

Attention: Some settings in the following steps are mandatory: The virtual disk drive should be set to SCSI 0:0 and the D/DVD Virtual Device Node should be set to IDE (0:0).

Attention: Default values should be used during the configuration process unless specified otherwise. Using other than the default values may result in unexpected behavior.

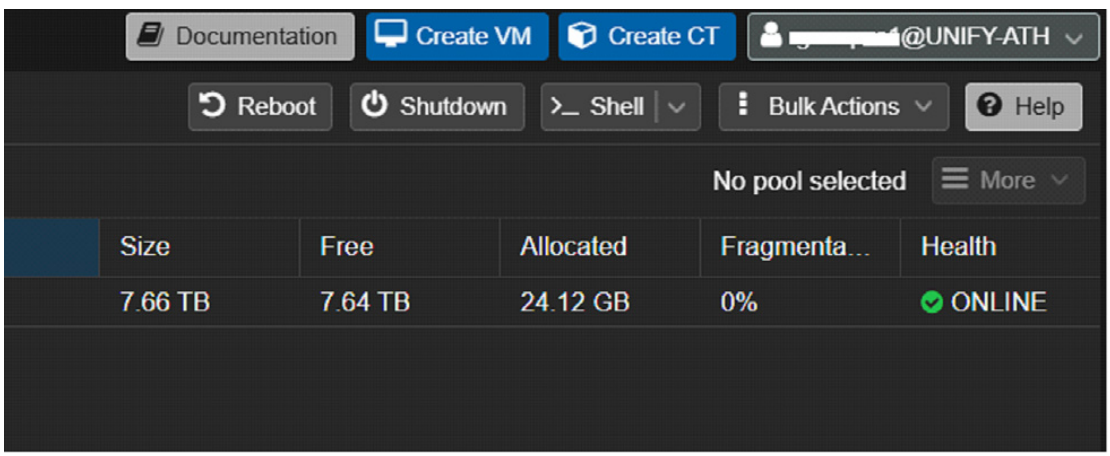
The **Create New Virtual Machine** wizard is used to configure the virtualized OSV installations. This procedure assumes that the Datacenter and Cluster are already configured.

Run the Proxmox user interface and select your cluster (the cluster element is highlighted in the following figure).



1. Access the **Create VM** wizard from the Proxmox UI (PVE) menu after selecting your cluster by one of two methods:

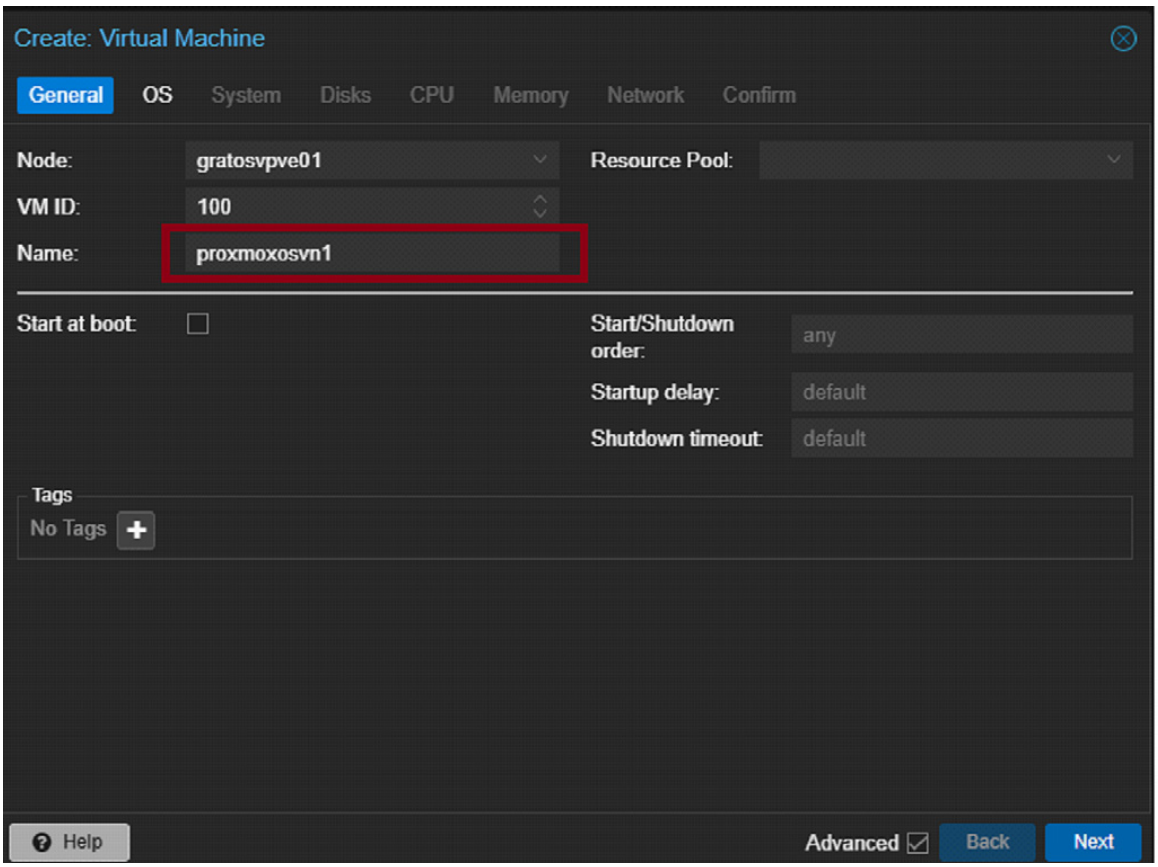
- Right click the cluster icon and select **Create VM**
- Click the **Create VM** button on the top right corner.



Note: These steps are repeated for the creation of the second node. The first time through the procedure, conduct the steps indicated as "step 1" wherever specified. When conducting the steps the second time around for Node 2, follow the steps indicated as "step 2" wherever specified.

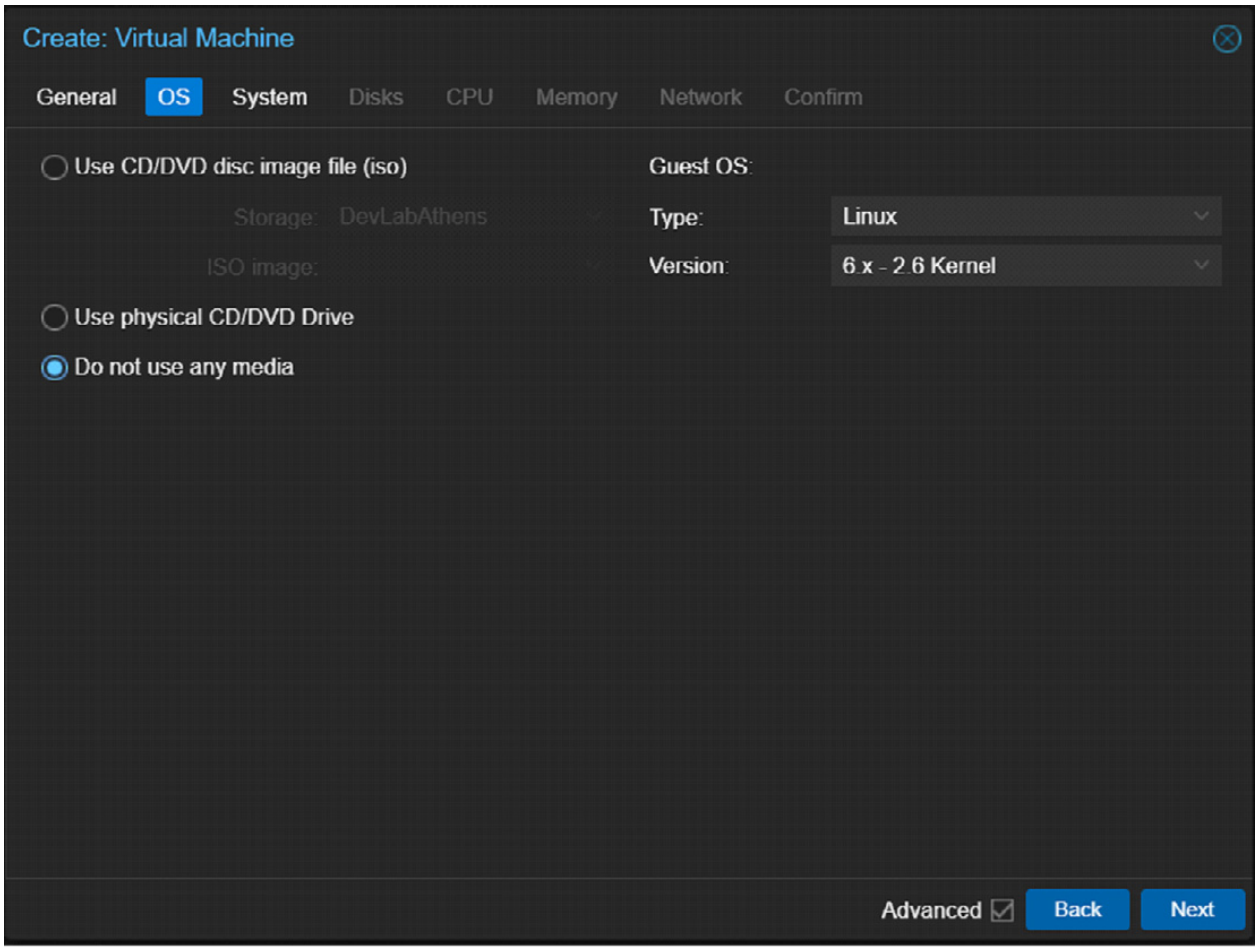
2. In **General** tab you need to enter a Virtual Machine Name.

Keep in mind that some special characters (like underscore) are not allowed by Proxmox. The values of **Node** and **VM ID** fields are assigned automatically, no changes are needed. Also check the **Advanced** box to be able to see additional options.

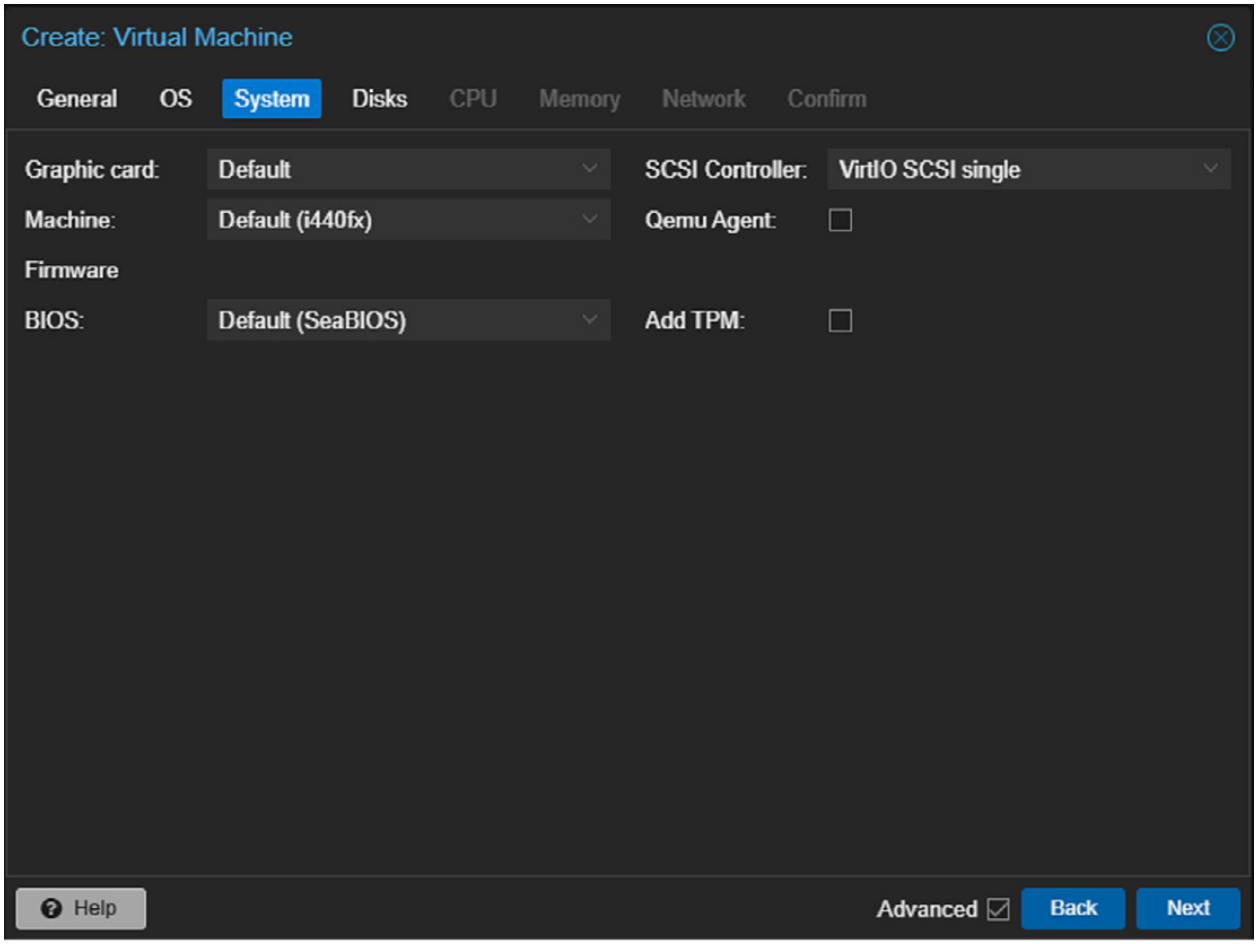


3. In **OS** tab, select **Do not use any media**. The installation will be done at the end, after creating the machine and the custom OpenScape Voice ISO.

The value of **Guest OS** field is by default (and should be left) as Linux.

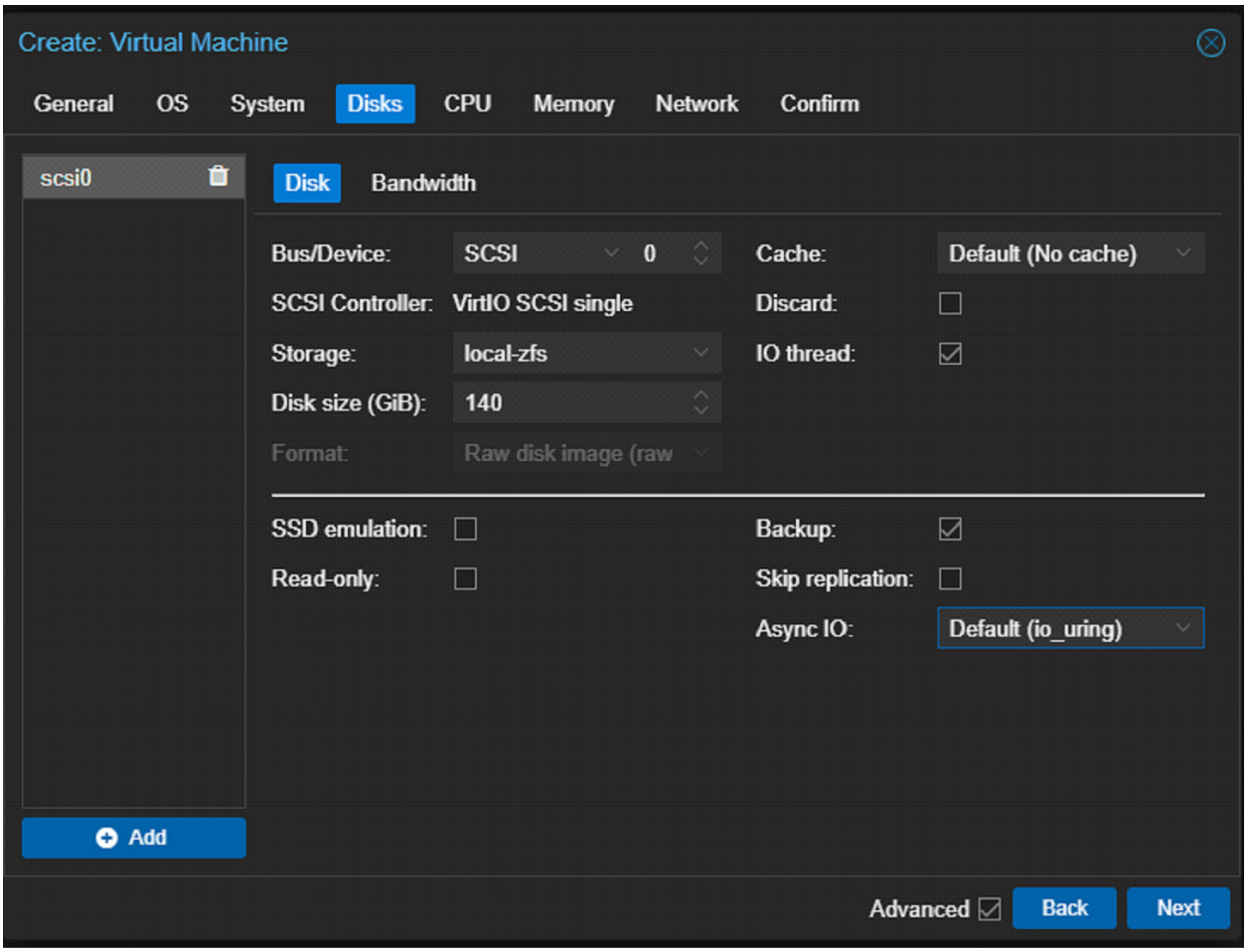


4. In **System** tab, in the **BIOS** field the pre-configured value is **Default SeaBIOS**. Do not change this as UEFI installation is not supported by OpenScape Voice. The **SCSI Controller** field should be also left in the default value **VirtIO SCSI single**.

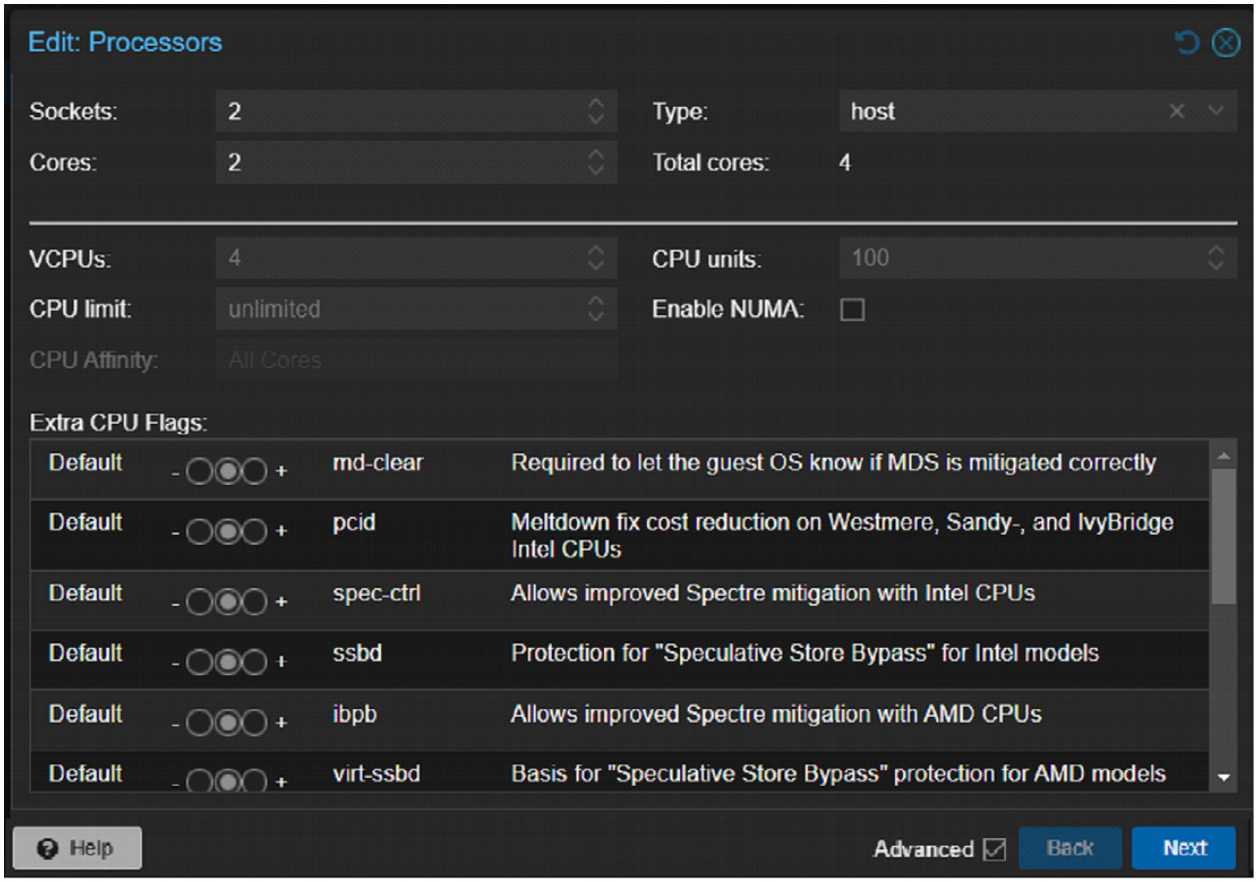


5. In **Disks** tab, select the required value for **Storage** (if more options are available, depending on the Proxmox Cluster configuration) and select the **Disk size (GiB)** based on the values in the *OpenScape Virtual Machine Resourcing and Configuration Guide*.

Keep in mind that KVM hypervisors calculate the disk and memory size in GiB.



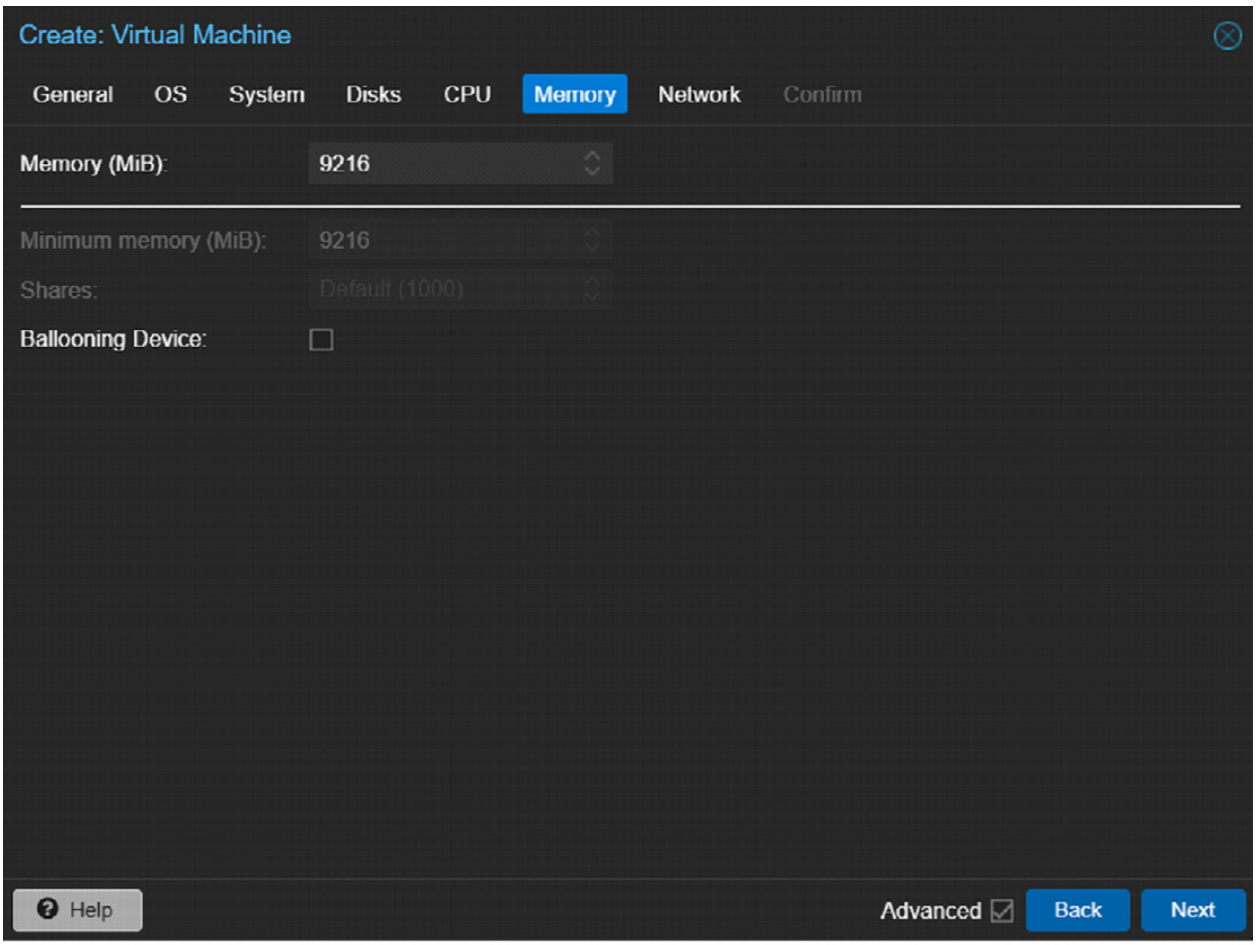
6. In **CPU** tab, select the number of CPUs according to the values provided in the *OpenScape Virtual Machine Resourcing and Configuration Guide*.



Note: A 4 vCPU VM is configured with 2 virtual sockets and 2 cores per virtual socket, while an 8 vCPU VM is configured with 2 virtual sockets and 4 cores per virtual socket.

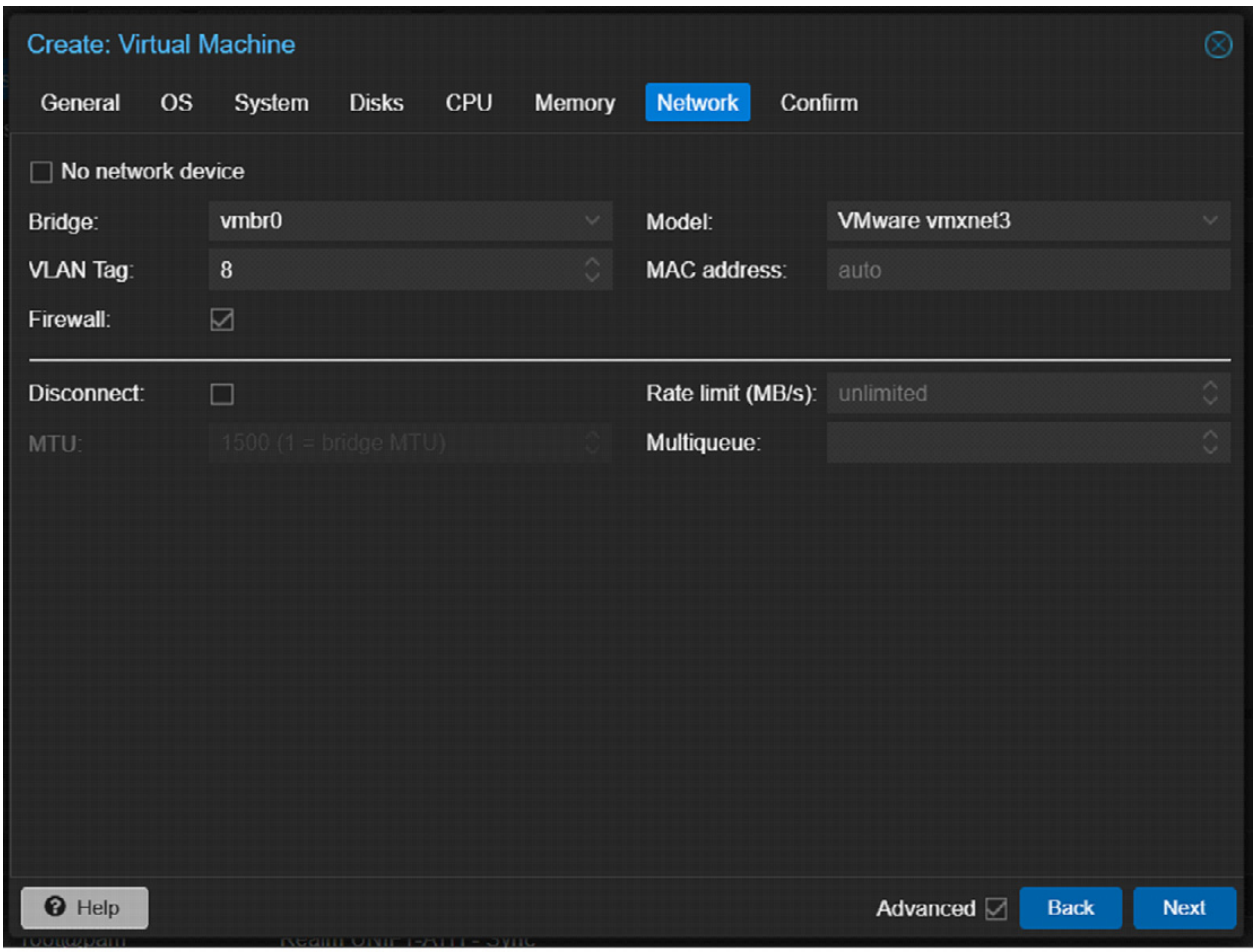
For optimal performance, change the value **Type** field to **host**. Do this only if all the CPUs from the cluster servers are identical, to avoid possible problems in case of Virtual Machine migration between servers.

7. In the **Memory** tab, set the value of Memory (MiB) to **9 GiB** for a virtual **Duplex** deployment or **10 GiB** for a virtual **Integrated Simplex** deployment. Disable the **Ballooning Device** checkbox so that the memory is reserved and not dynamically changed by the guest machine.



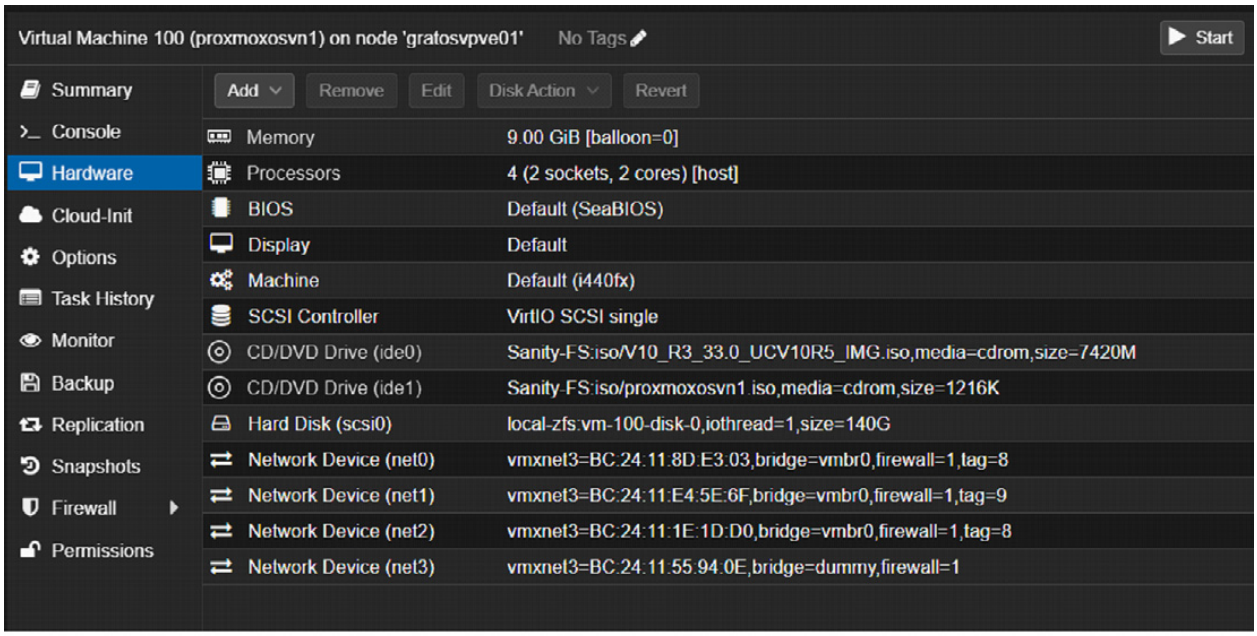
8. In the **Network** tab, you can configure 1 NIC. The Proxmox Virtual Machine creation wizard only allows adding 1 NIC. The value of **Model** field should be set to **VMware vmxnet3**.

Depending on the instructions provided in the *OpenScape Virtual Machine Resourcing and Configuration Guide*, more Network cards can be added after the Virtual Machine is created.



9. Once the Virtual Machine is created, you can add/change the hardware in the **Hardware** menu.

- From here you can add the remaining NIC cards according to your implementation.
- You can add the required CD/DVD Drives and mount/unmount the ISO images needed for the installation.



4.3.7.1 Network choices

Duplex

Select 4 Network adapters (NICs). Select the following choices from the NIC drop down lists as indicated below;

a) **step 1 (Node 1)**

- NIC1 - admin_primary

- NIC2 - signaling_primary

- NIC3 - billing_primary

- NIC4 - cross_connect_primary

b) **step 2 (Node 2)**

- NIC1 - admin_secondary

- NIC2 - signaling_ secondary

- NIC3 - billing_secondary

- NIC4 - cross_connect_secondary

Simplex

For an Integrated Simplex Virtual Machine there is no cross connect switch but the four NICs must be created. Examples of a one port and three port simplex virtual machine mapping are provided.

Integrated Simplex VM with All Subnets Shared (1 port) configuration example:

- NIC1 - admin_primary

- NIC2 - unused2

- NIC3 - unused2

- NIC4 - unused3

Integrated Simplex VM with Separate Subnets (3 port) configuration example:

- NIC1 - admin_primary

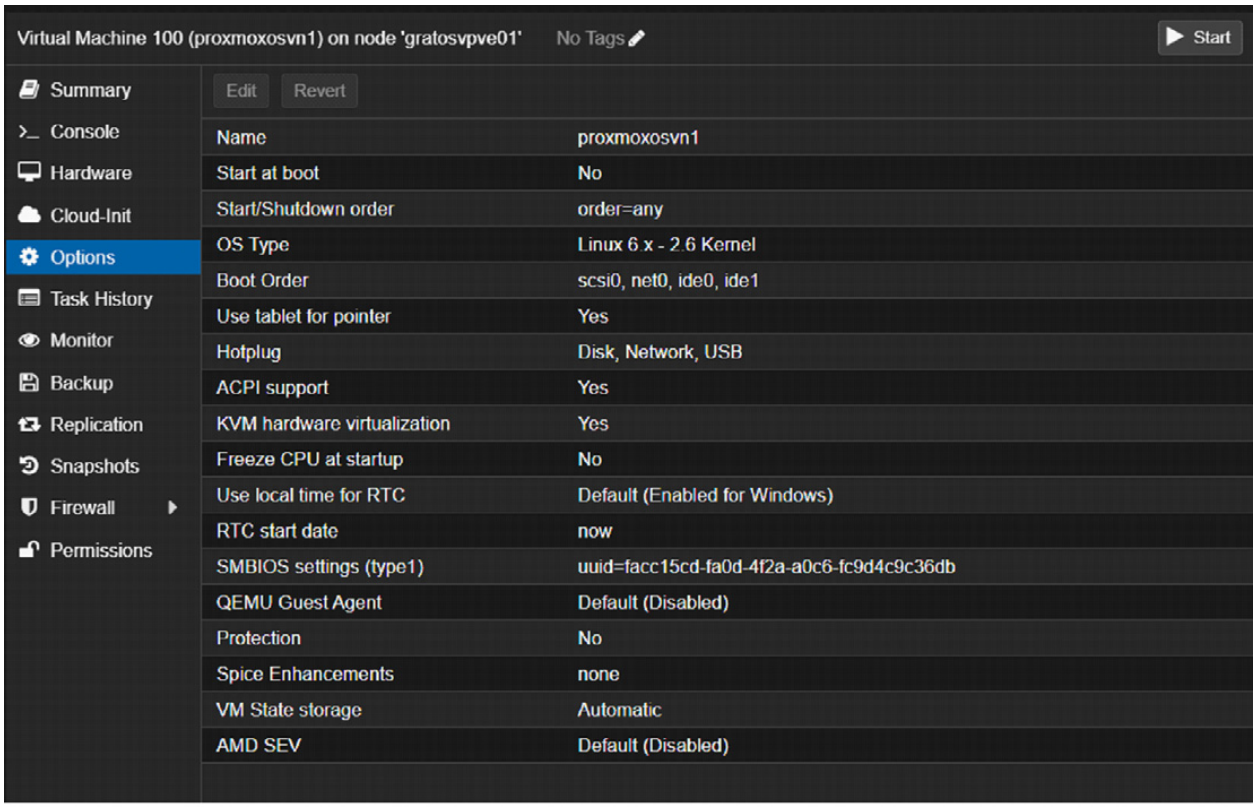
- NIC2 - signaling_primary

- NIC3 - billing_primary

- NIC4 - unused3

The order of the Network adapter to Network label is important and must match the order shown in the image below **for all Virtual installations**. The above example refers to a solution where Admin-Billing are shared and all the rest networks separated.

10. From the **Options** menu you can change the **Boot Order**.



4.3.7.2 Adding a CD/DVD Drive to the Virtual Machine

This section can be employed to make a *node.cfg* ISO file available on a virtual CD/DVD device.

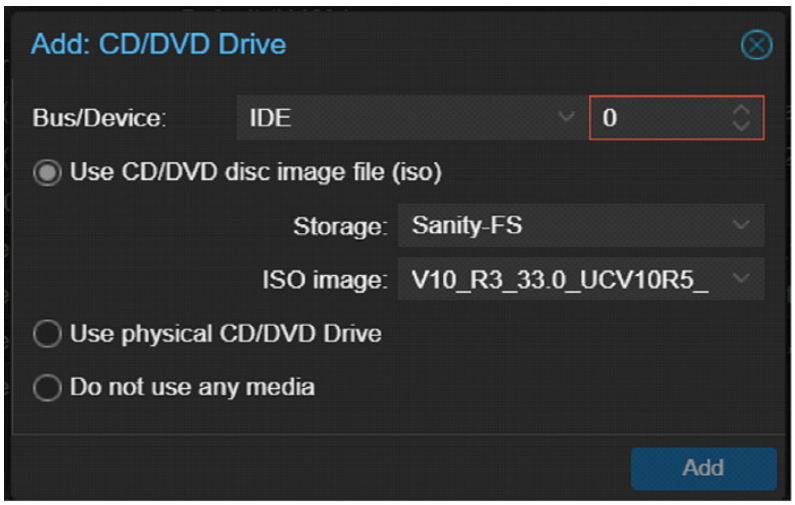
Attention: The VM OSV node must be powered down. This process has to be completed on both nodes of a duplex system.

---

1. Access the Proxmox GUI and perform the following actions:

- Select the appropriate node
- Select Hardware
- Click the **Add** button and select CD/DVD Drive

2. In the **Add: CD/DVD Drive** window do the following:



3. Set the **Bus/Device** to **IDE 0**

- Choose the radio button **Use CD/DVD disk image file (iso)**
- In **Storage** choose your datastore where you have uploaded your OSV ISO image
- In **ISO image** browse and select the proper ISO image for that activity
- Click **Add** to finish this activity.

The 'new' CD/DVD should now be present in the Hardware list.

4.3.7.3 Installing the OpenScape Voice

Once the virtual machine is created, with the required Openscape Voice ISO file and the node.cfg iso file mounted, you can start the Virtual machine of each node and proceed with the OSV installation through the console.

4.3.8 Create a Virtual Machine in Hyper-V

Note: These instructions apply to Duplex and Integrated Simplex OSV VM Guest preparation. Some of the steps have different headings like "**Duplex**:" and "**Simplex**:" depending on the VM system being prepared. Choose the selections listed for your VM deployment.

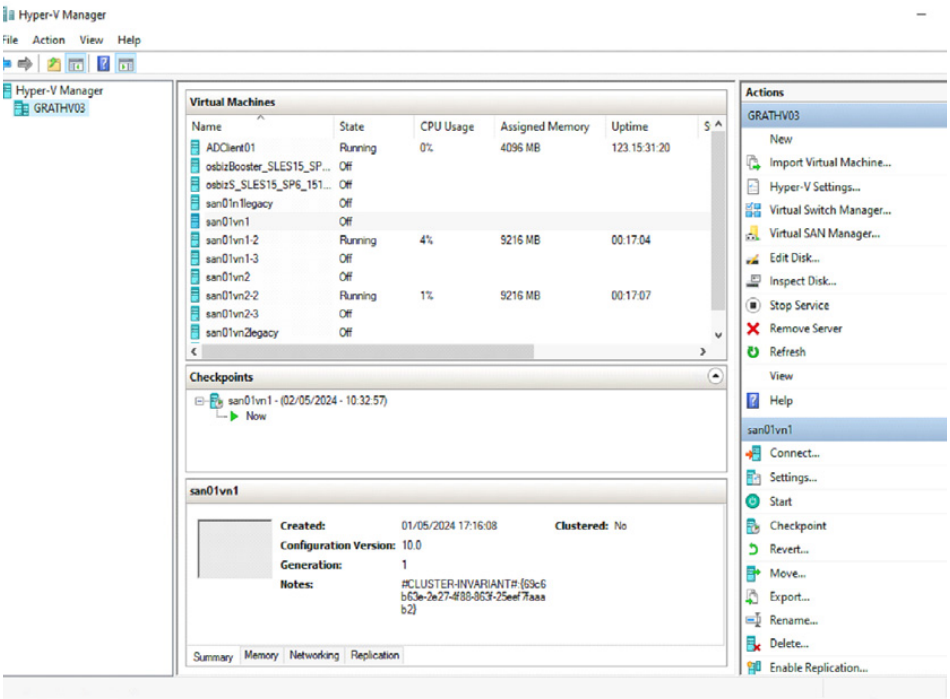
Attention: The following values are presented as examples only. The values may require adjustment based on a site's particular installation environment. Document OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide lists the configuration parameters needed to configure each OpenScape Voice node.

Attention: Mandatory settings for these steps in this section.
- The virtual disk drive should be set to IDE 0:0 in step 12.
- The CD/DVD Virtual Device Node should be set to IDE (1:0) in step 15.

Attention: Default values should be used during the configuration process unless specified otherwise. **Using other than the default values may result in unexpected behavior.**

The New Virtual Machine wizard will be used to configure the virtualized OSV installations. This procedure assumes that the Datacenter and Cluster are already configured.

Select your server in Hyper-V Manager (the server element is highlighted in the following figure.)

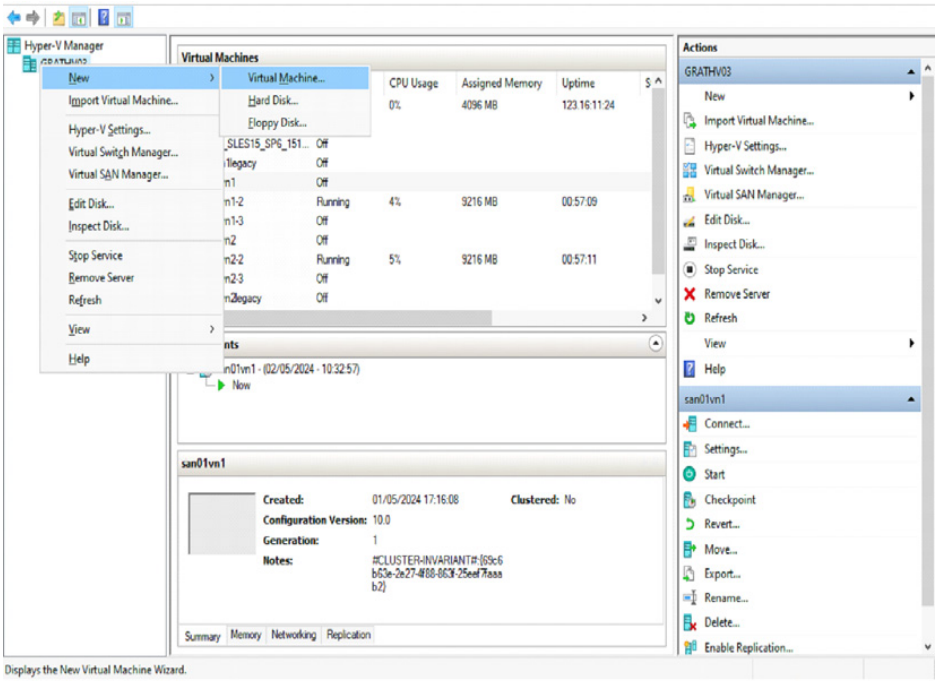


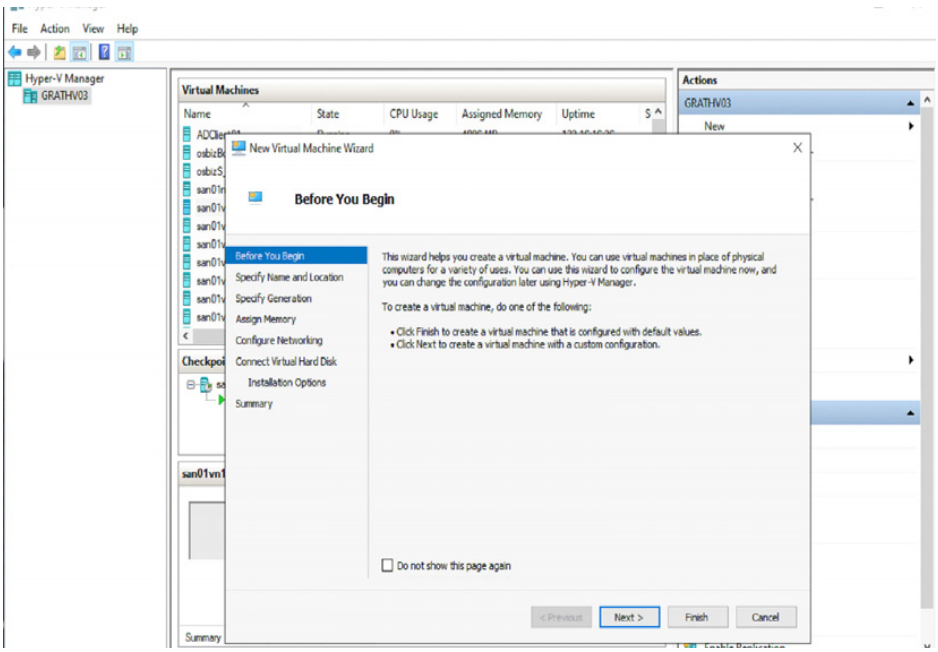
1.Access the **New Virtual Machine** wizard from the HyperV Manager after selecting your server by one of following methods:

- Right click the server icon and select New -> "Virtual Machine"

- Click Action Menu -> New -> "Virtual Machine"

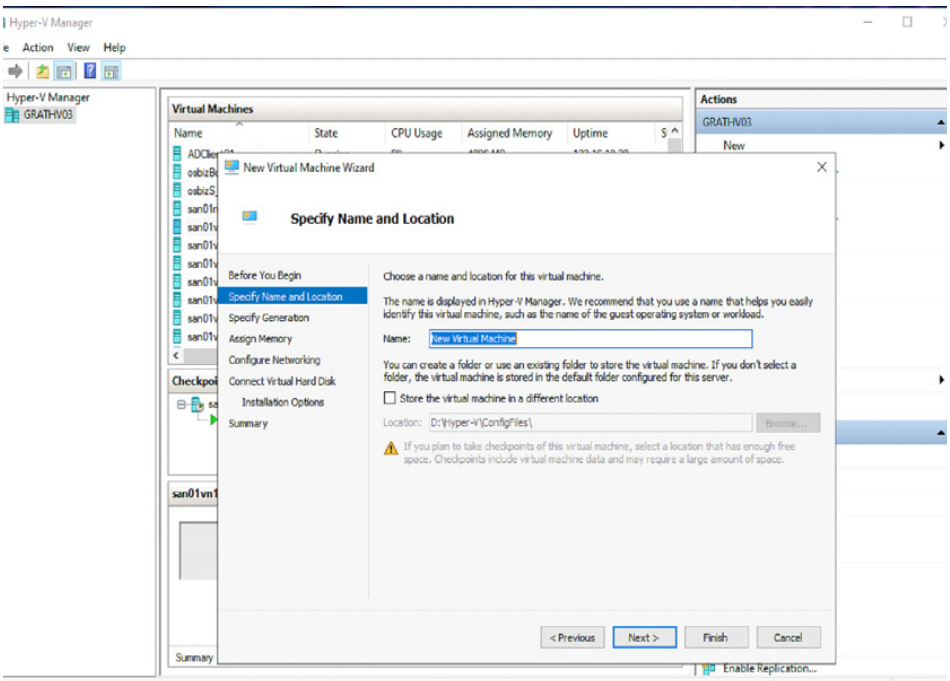
- Click on the right Actions pane -> New -> "Virtual Machine"



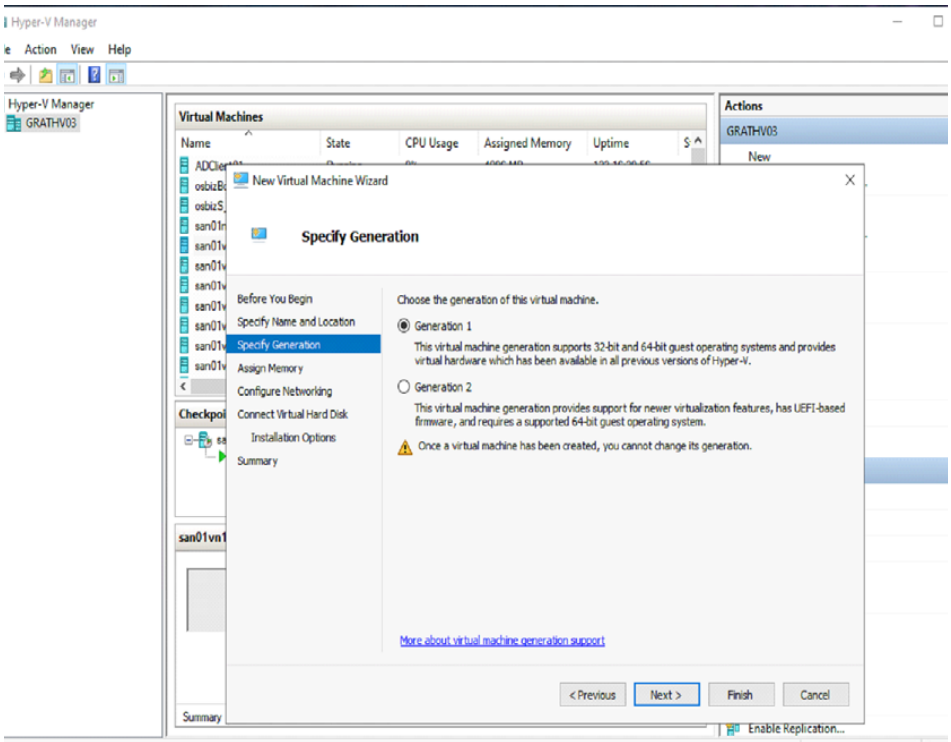


Note: These steps will be repeated for the creation of the second node as well. The first time through the procedure, conduct the steps indicated as "step 1" wherever specified. When conducting the steps the second time around for Node 2, follow the steps indicated as "step 2" wherever specified.

2. In **Specify Name and Location** screen Configure a VM name and select your location depending on the Hyper-V configuration.

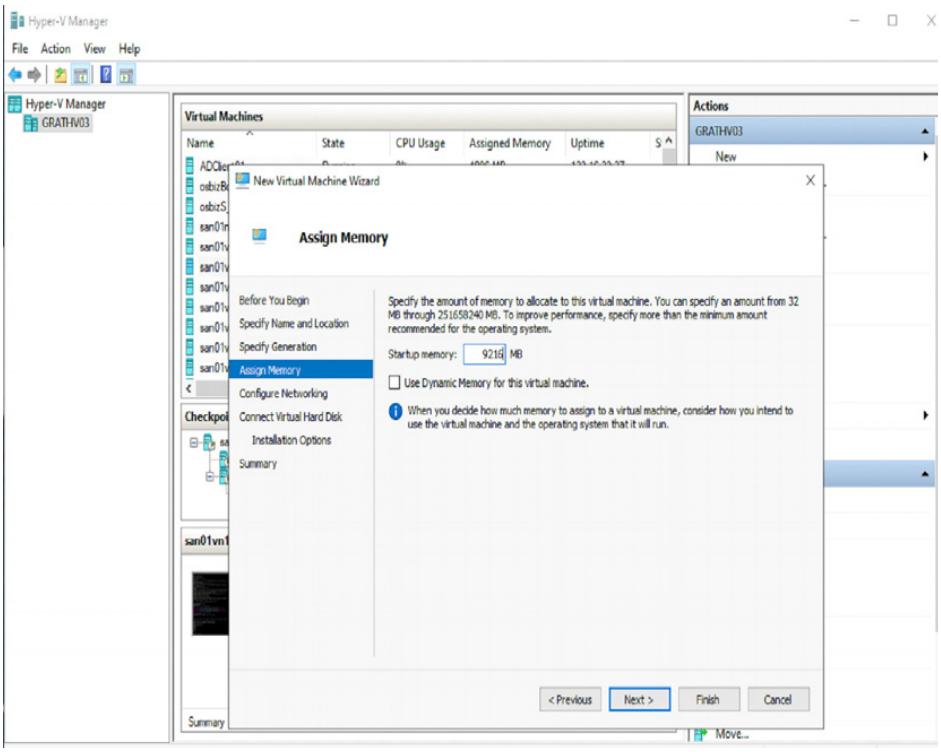


3.In **Specify Generation** screen, select **Generation 1** as OpenScape Voice uses legacy BIOS.



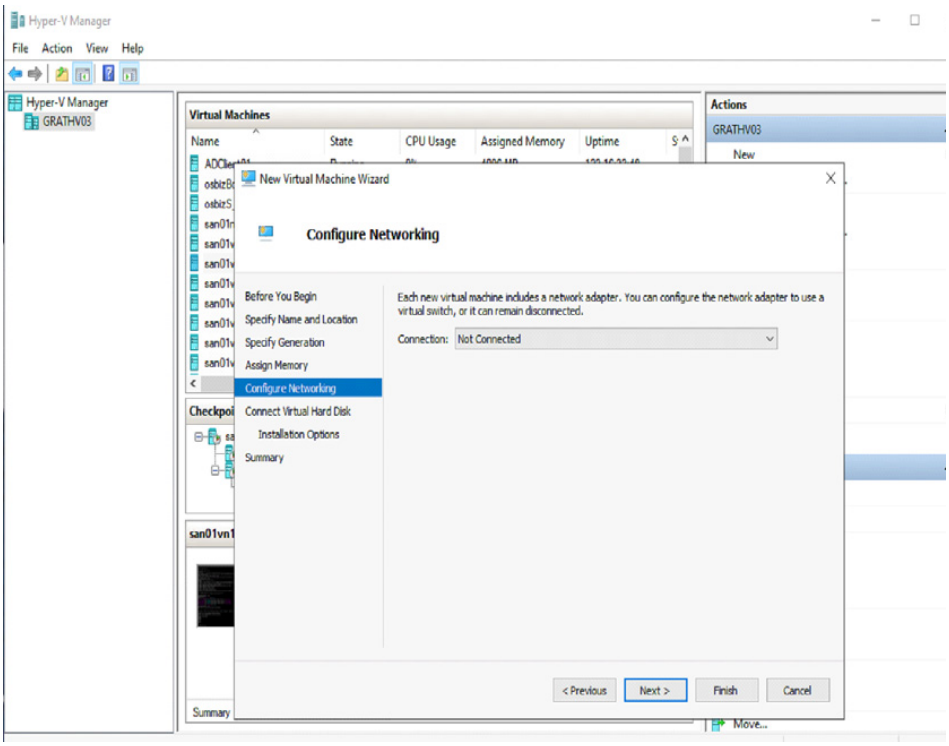
4.In **Assign Memory** screen, Configure the VM RAM memory according to the values indicated in the OpenScape Virtual Machine Resourcing and Configuration Guide.

Note: Do not check the box to use the Dynamic Memory for OpenScape Voice.

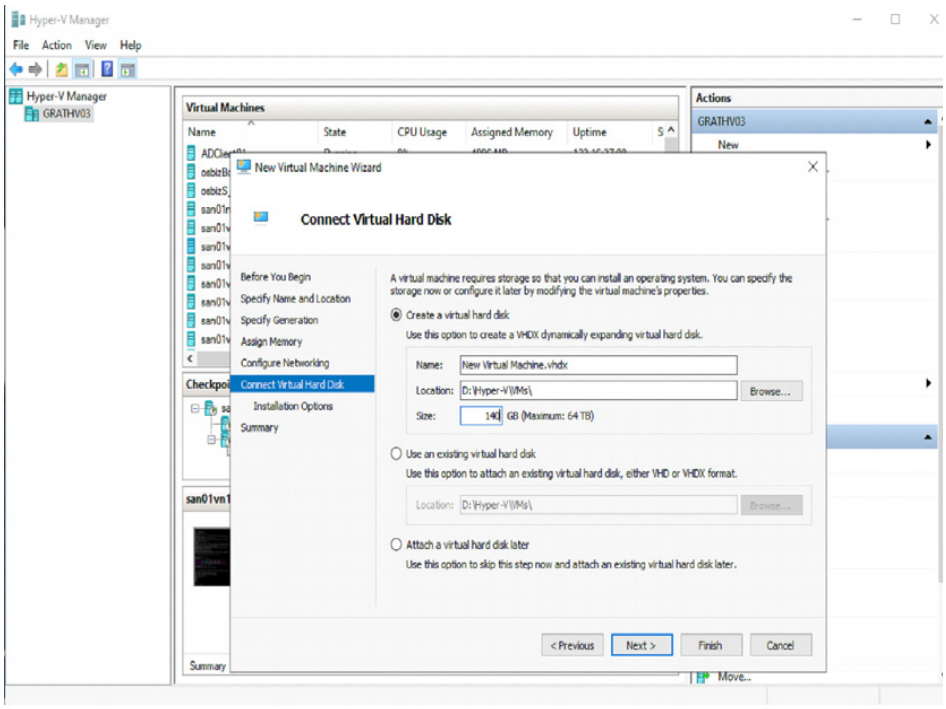


5.In **Configure Networking** tab, leave the Default selection as during the VM creation wizard you can only add 1 NIC (not Legacy) and you will have to come back to this menu after the VM creation. Depending on the needs described in the OpenScape Virtual Machine Resourcing and Configuration Guide, more Network cards can be added after the Virtual Machine is created.

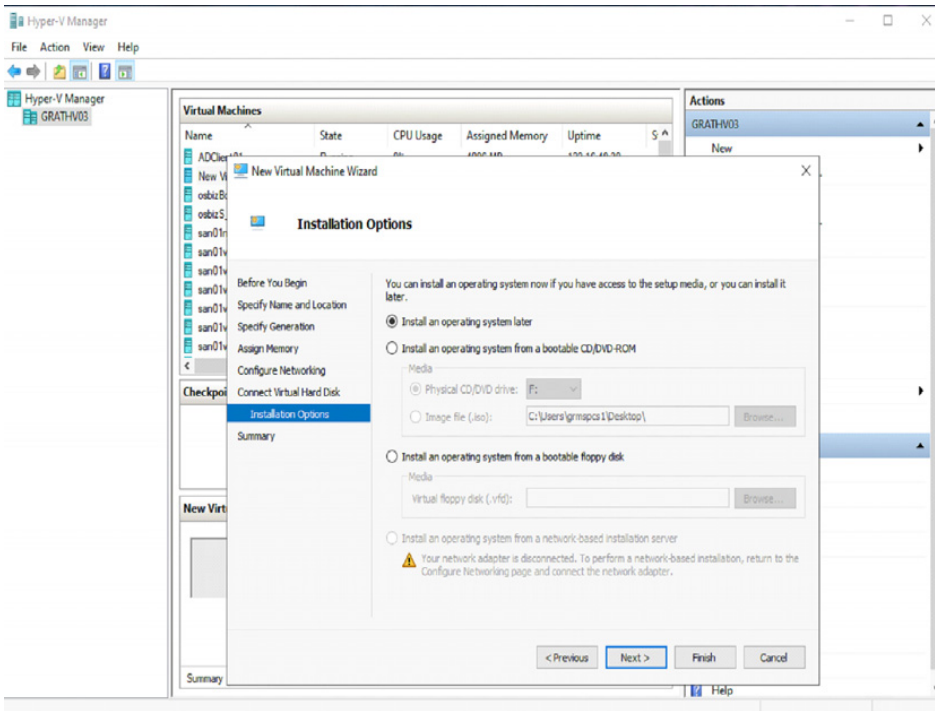
Note: In all the network interfaces shared (Admin, Signaling, Billing, Interconnection) solution where only 1 NIC is needed the native **Network Adapter** can be used. In all the other solutions where more than 2 NICs are needed only the **Legacy Network Adapter** type is supported.



6.In **Connect Virtual Hard Disk** screen, assign a virtual disk size according to the OpenScape Virtual Machine Resourcing and Configuration Guide.



7a) In **Installation Options** screen, leave the default Install an operating system later, as you will need to add another drive to attach the node.cfg as well.



7b. Once the Virtual Machine is created, go to **Settings** to **finish** (or adjust) further **settings**:

8. In **Add Hardware** screen you can add additional NIC cards (or other hardware)

Note: Choose **Legacy Network Adapter** if more than 1 NICs are needed and the default Network Adapter created during the New Virtual Machine wizard must be removed.

Network choices:

Duplex: Select 4 Network adapters (NICs). Select the following choices from the NIC drop down lists as indicated below;

a) step 1

- NIC1 - admin_primary

- NIC2 - signaling_primary

- NIC3 - billing_primary

- NIC4 - cross_connect_primary

b) step 2

- NIC1 - admin_secondary

- NIC2 - signaling_ secondary

- NIC3 - billing_secondary

- NIC4 - cross_connect_secondary

Simplex: For an Integrated Simplex Virtual Machine there is no cross connect switch but the four NICs must be created. Examples of a one port and three port simplex virtual machine mapping are provided.

Integrated Simplex VM with All Subnets Shared (1 port) configuration example:

- NIC1 - admin_primary

- NIC2 - unused2

- NIC3 - unused2

- NIC4 - unused3

Integrated Simplex VM with Separate Subnets (3 port) configuration example:

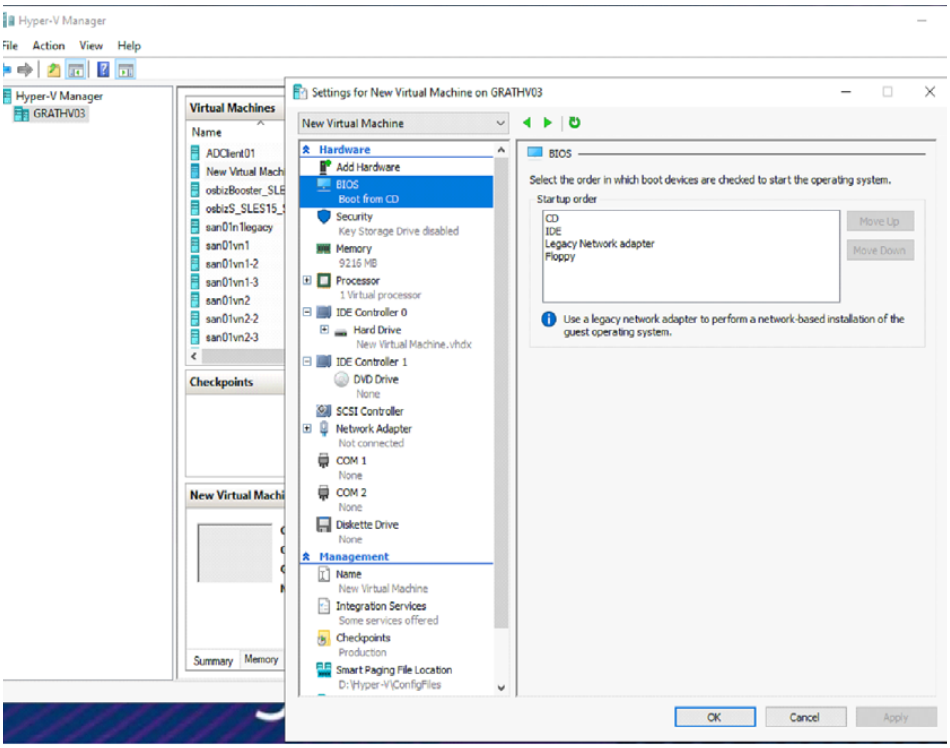
- NIC1 - admin_primary

- NIC2 - signaling_primary

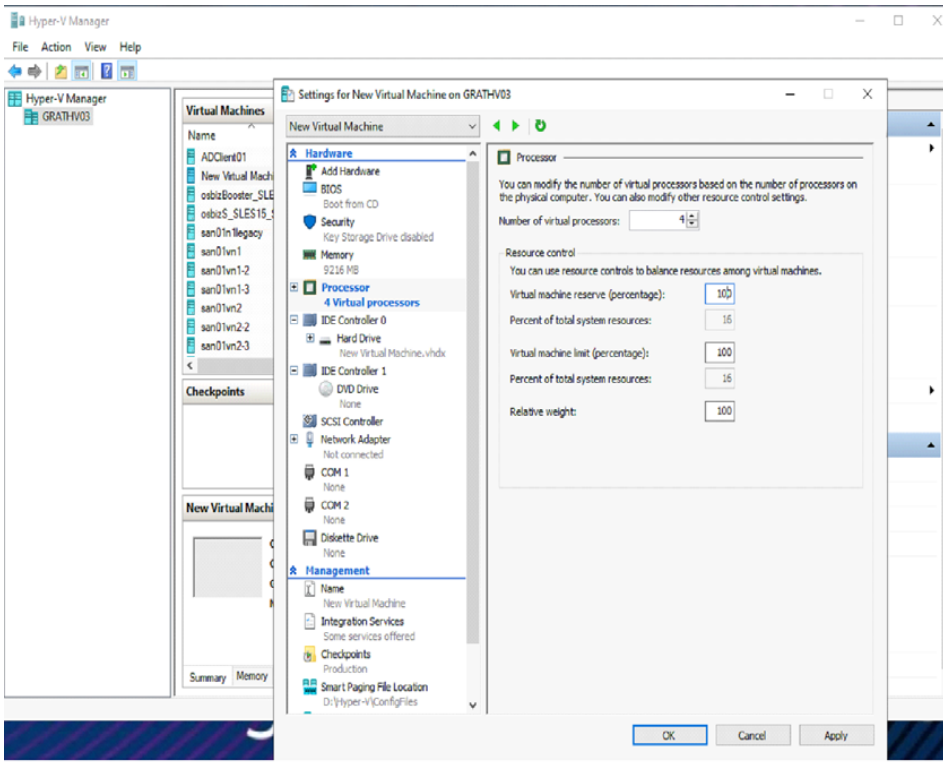
- NIC3 - billing_primary

- NIC4 - unused3

9.In **BIOS** menu you can change the Boot Order.



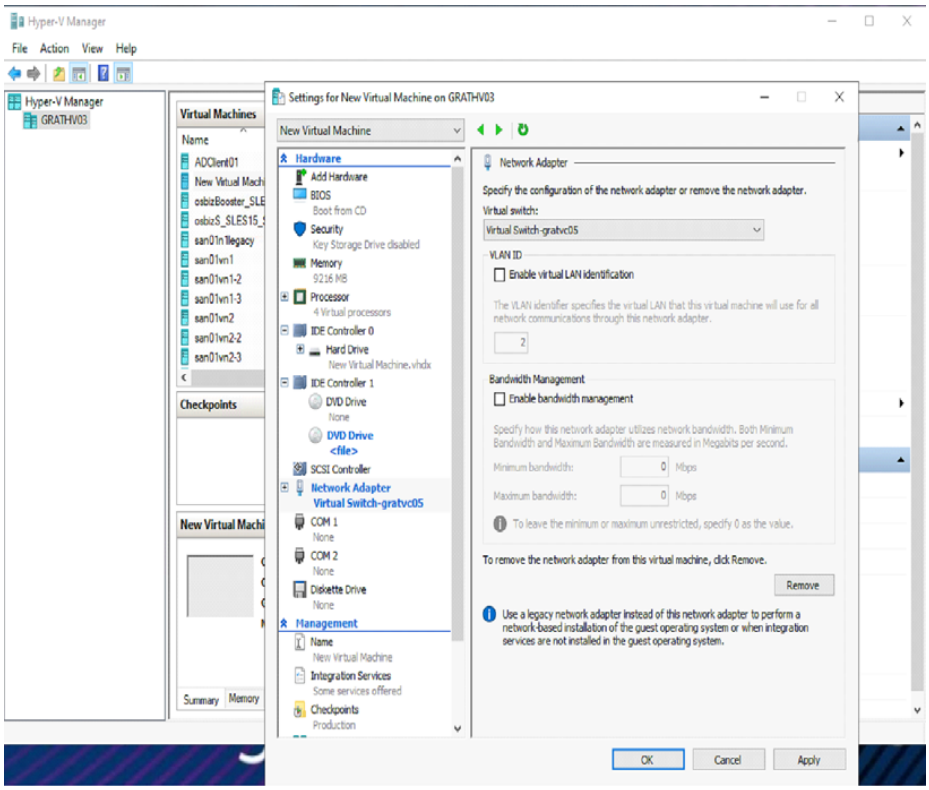
10.In **Processor** menu select the number of CPU threads according to the OpenScape Virtual Machine Resourcing and Configuration Guide. Also set the **Virtual Machine reserve (percentage)** to **100**.

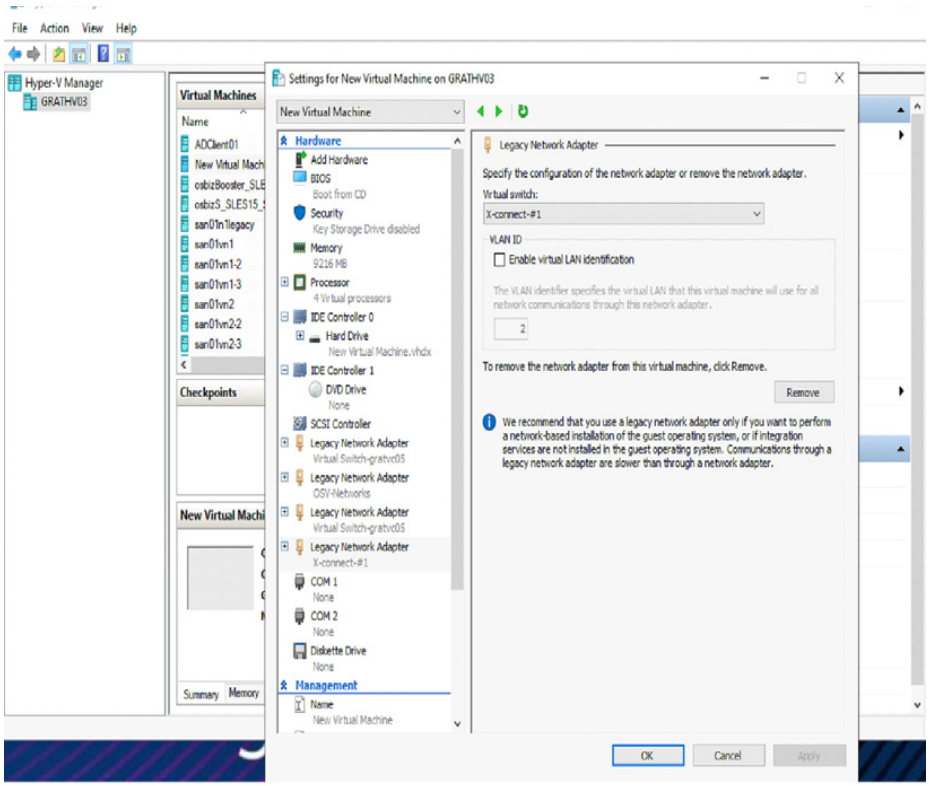


11.Remove the existed **SCSI Controller** by selecting it and click **Remove** and **Apply**

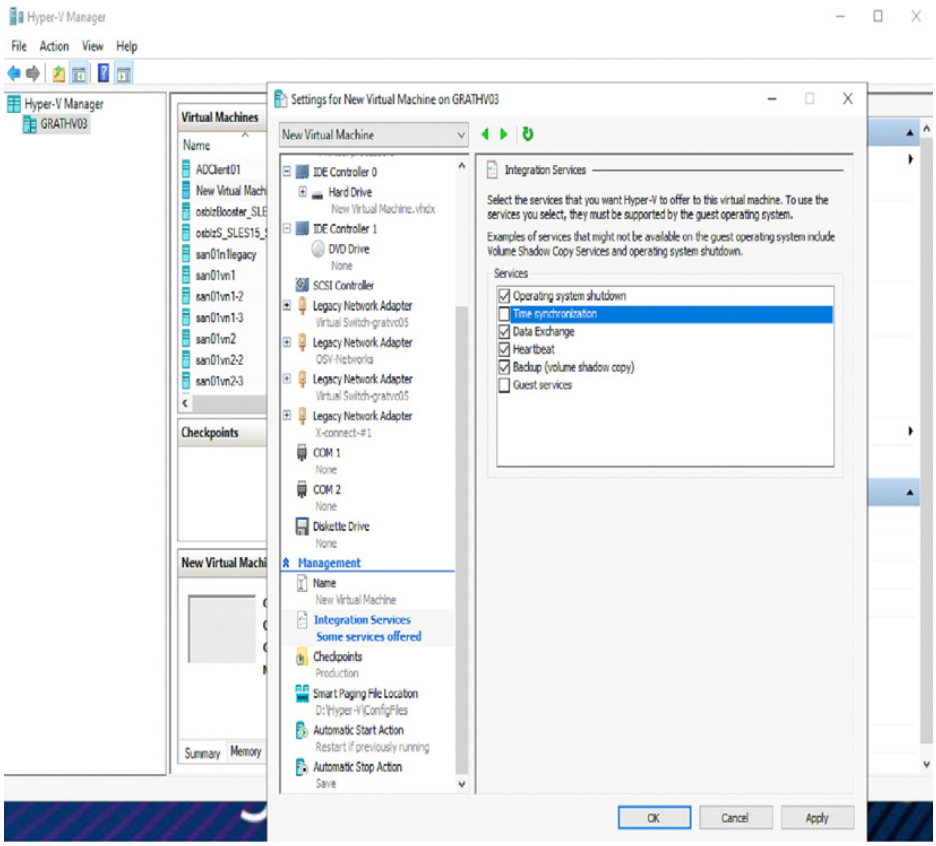
12.In **Network Adapter** menu you select the appropriate Virtual Switch for each network interface.

Note: If you are installing the OSV with all the interfaces shared, 1NIC implementation then you can use the existed network adapter and only assign the proper **Virtual switch** and **Enable virtual LAN identification** as needed. If you are using more that 2 NICs then you must remove the existed Network Adapter and then add the needed NICs as Legacy Network Adapters.

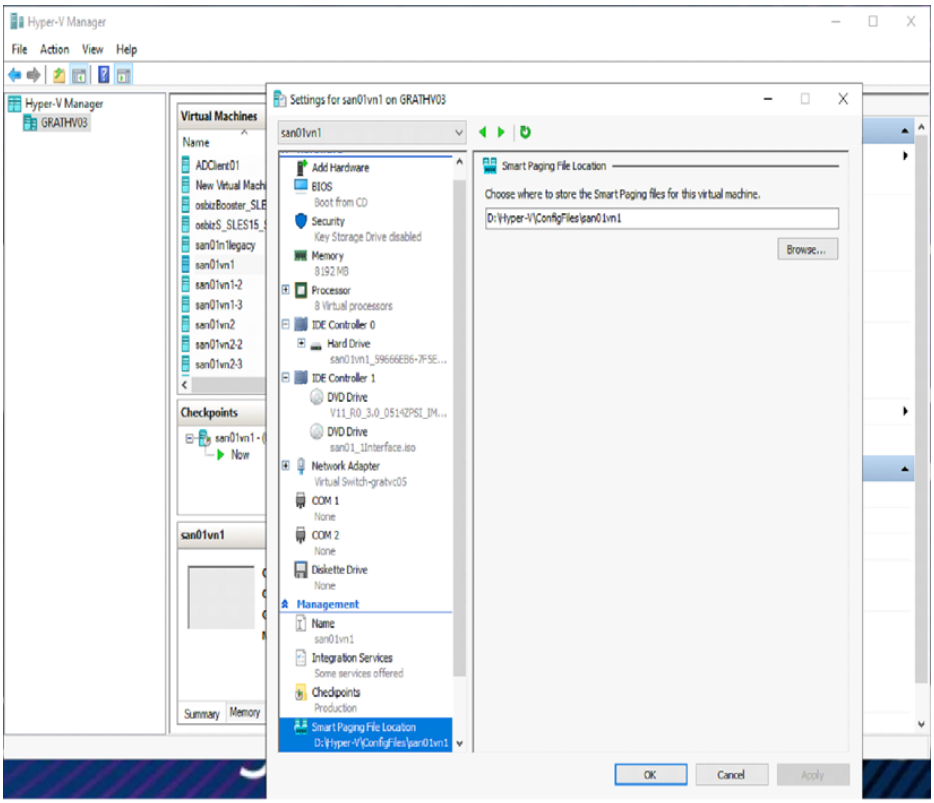

Hyper-V Manager
File Action View Help
Hyper-V Manager
GRATHV03
Virtual Machines
Name
ADClient01
New Virtual Machi
osbizBooster_SLE
osbizS_SLES15_
san01n1legacy
san01vn1
san01vn1-2
san01vn1-3
san01vn2
san01vn2-2
san01vn2-3
Checkpoints
New Virtual Machi
Summary
Memory
Settings for New Virtual Machine on GRATHV03
New Virtual Machine
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
9216 MB
Processor
4 Virtual processors
IDE Controller 0
Hard Drive
New Virtual Machine.vhdx
IDE Controller 1
DVD Drive
None
DVD Drive
<file>
SCSI Controller
Network Adapter
Virtual Switch-gratvc05
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
New Virtual Machine
Integration Services
Some services offered
Checkpoints
Production
Network Adapter
Specify the configuration of the network adapter or remove the network adapter.
Virtual switch:
Virtual Switch-gratvc05
VLAN ID
Enable virtual LAN identification
The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.
2
Bandwidth Management
Enable bandwidth management
Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.
Minimum bandwidth:
0
Mbps
Maximum bandwidth:
0
Mbps
To leave the minimum or maximum unrestricted, specify 0 as the value.
To remove the network adapter from this virtual machine, click Remove.
Remove
Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.
OK
Cancel
Apply


File Action View Help
Hyper-V Manager
GRATHV03
Virtual Machines
Name
ADClient01
New Virtual Machi
osbizBooster_SLE
osbizS_SLES15_
san01n1legacy
san01vn1
san01vn1-2
san01vn1-3
san01vn2
san01vn2-2
san01vn2-3
Checkpoints
New Virtual Machi
Summary
Memory
Settings for New Virtual Machine on GRATHV03
New Virtual Machine
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
9216 MB
Processor
4 Virtual processors
IDE Controller 0
Hard Drive
New Virtual Machine.vhdx
IDE Controller 1
DVD Drive
None
SCSI Controller
Legacy Network Adapter
Virtual Switch-gratvc05
Legacy Network Adapter
OSV-Networks
Legacy Network Adapter
Virtual Switch-gratvc05
Legacy Network Adapter
X-connect-#1
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
New Virtual Machine
Legacy Network Adapter
Specify the configuration of the network adapter or remove the network adapter.
Virtual switch:
X-connect-#1
VLAN ID
Enable virtual LAN identification
The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.
2
To remove the network adapter from this virtual machine, click Remove.
Remove
We recommend that you use a legacy network adapter only if you want to perform a network-based installation of the guest operating system, or if integration services are not installed in the guest operating system. Communications through a legacy network adapter are slower than through a network adapter.
OK
Cancel
Apply

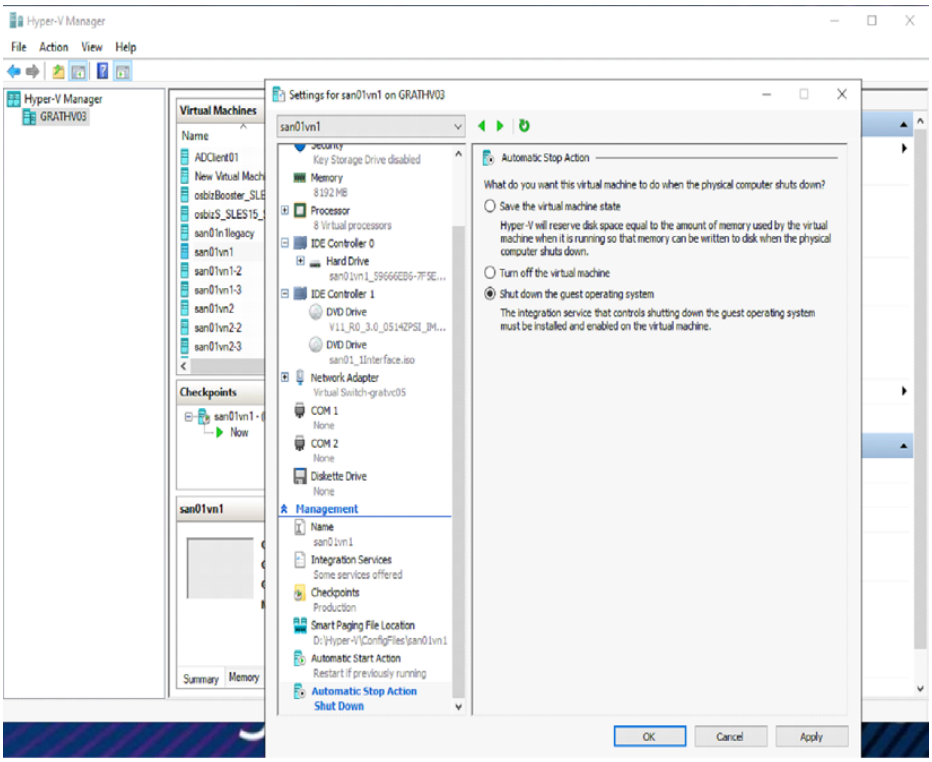
13.In **Integration Services** disable (uncheck) **Time Synchronization**



14.In **Smart Paging File Location** browse and select the previously created VM folder (if not already configured)



15.In **Automatic Stop Action** enable (check) **Shutdown the guest operating system**



4.3.8.1 Adding a CD/DVD Drive to the Virtual Machine

This section can be employed to make a node.cfg ISO file available on a virtual CD/DVD device.

Attention: The VM OSV node must be powered down. This procedure must be completed on both nodes of a duplex system.

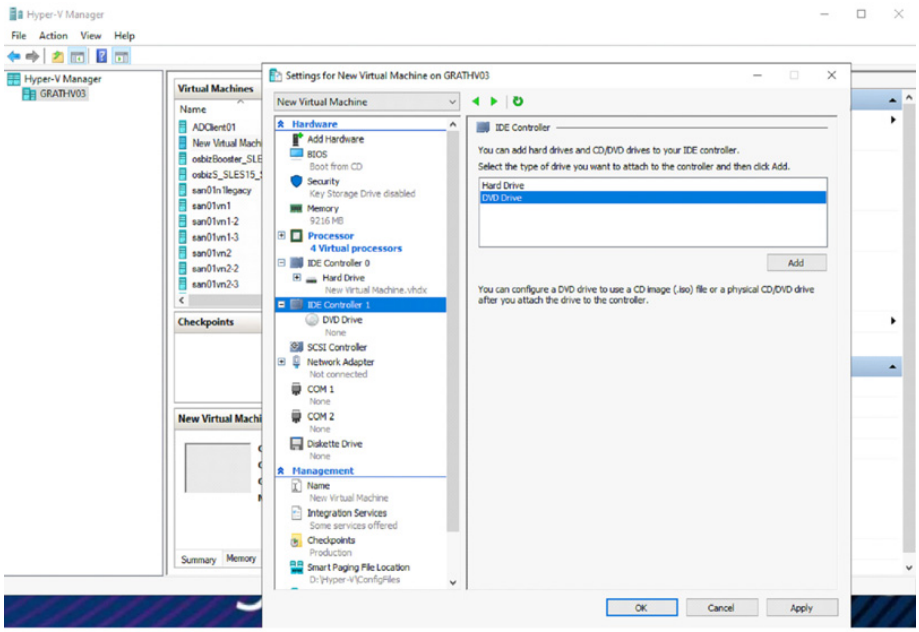
---

1. Access the HyperV manager GUI

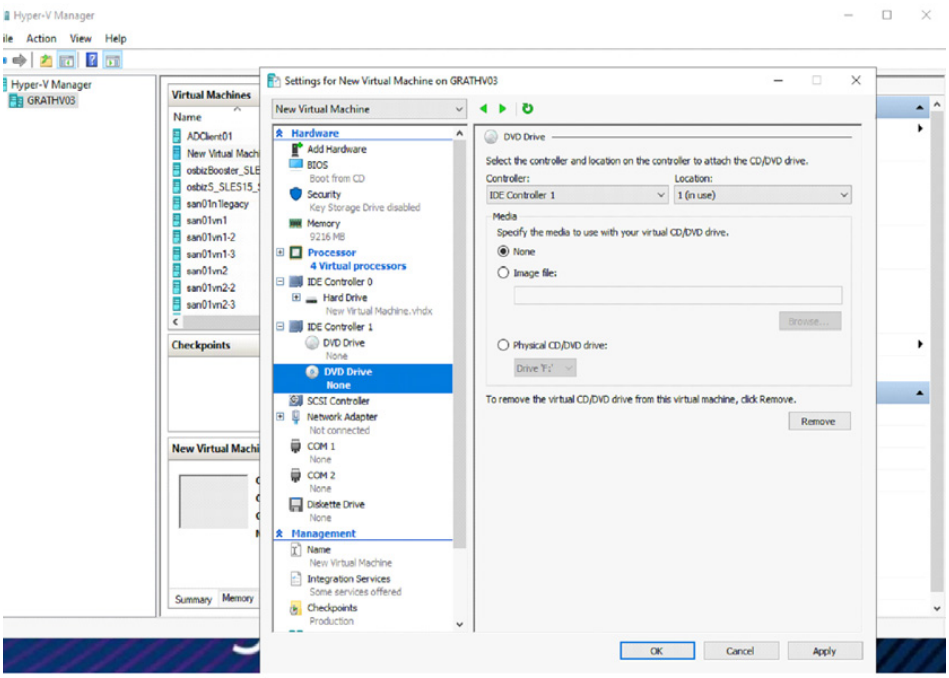
Select the appropriate node

Select **Settings**

Click on **IDE Controller 1**, select **DVD Drive** and **Add**



2.The **DVD Drive** window is presented

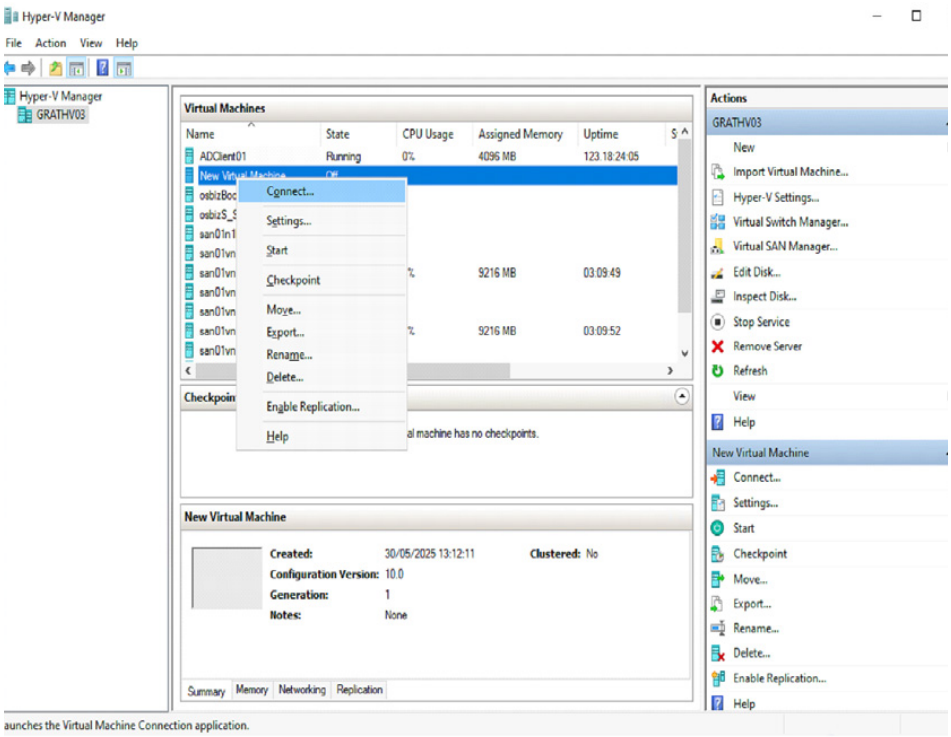


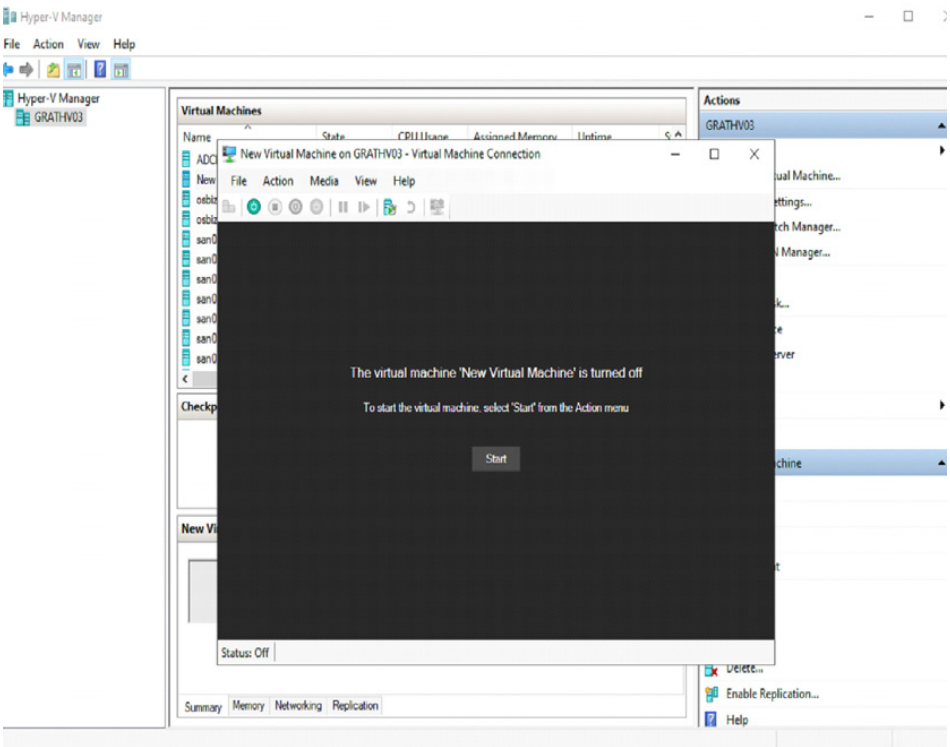
3.Navigate through the 2 DVD drives and assign the proper ISO Files by Browsing them from Storage and click **Apply**. If you would like to use a network datastore where you have uploaded your iso images you should have added it as a Network location to your Windows server.

4.This section can be also employed to make a node.cfg ISO file available on a virtual CD/DVD device.

4.3.8.2 Installing the OpenScape Voice

Once the virtual machine is created, with the required Openscape Voice iso file and the node.cfg iso file mounted you can connect to the Virtual machine console of each node and proceed with the OSV installation through the Console.




Hyper-V Manager
File Action View Help
Hyper-V Manager
GRATHV03
Virtual Machines
Name
New Virtual Machine on GRATHV03 - Virtual Machine Connection
File Action Media View Help
The virtual machine 'New Virtual Machine' is turned off
To start the virtual machine, select 'Start' from the Action menu
Start
Status: Off
Summary Memory Networking Replication
Actions
GRATHV03
Enable Replication...
Help

4.3.9 Migration from VMWare to Hyper-V

Prerequisites

- Ensure all requirements described in the following chapter *HDD preparations for Hyper-V*, are achieved.

To be able to migrate from VMWare to Hyper-V there are several options.

The tested tool is Starwind V2V converter (tested version is V9.0.1.444).

A precondition is that the Windows PC, where the tool runs, should be configured in the same domain as the Hyper-V cluster.

Please refer to the Starwind V2V documentation for installation and configuration details.

4.3.9.1 HDD preparations for Hyper-V

HDD preparation for SLES 12 UC deployments

For a SLES 12 Virtual Machine, to ensure that the required drivers for Hyper-V are included in the *initrd* during the migration from ESXi to Hyper-V, perform the steps below while the VM is still running on the ESXi host. These steps will update the *initrd* configuration to include the necessary Hyper-V drivers:

1) Modify the *initrd* configuration to include Hyper-V drivers:

Edit or create the */etc/sysconfig/kernel* file and modify the *INITRD_MODULES* line to include the following Hyper-V drivers:

```
bash

sed -i "/^INITRD_MODULES/s/\"$/ hv_vmbus hv_netvsc

hv_storvsc\"/" /etc/sysconfig/kernel
```

2) Rebuild the *initramfs*:

Run the following command to regenerate the *initrd* with the updated configuration:

```
bash

mkinitrd
```

This will regenerate the *initrd* image to include the Hyper-V drivers necessary for migration to Hyper-V.

HDD preparation for SLES 15 UC deployments

For an SLES 15 virtual machine, to ensure that the required drivers for Hyper-V are included in the *initrd* during migration from ESXi to Hyper-V, perform the steps below while the VM is still running on the ESXi host. These steps update the *initrd* configuration to include the necessary Hyper-V drivers:

1) Modify the *dracut* configuration to include Hyper-V drivers:

Edit or create the /*etc/dracut.conf.d/90-hyperv.conf* file and add the following lines:

```
bash

echo "add_drivers=\"hv_vmbus hv_netvsc hv_storvsc\"" >

/etc/dracut.conf.d/90-hyperv.conf
```

2) Rebuild the *initramfs* using *dracut*:

Run the following command to regenerate the *initrd* with the updated configuration:

```
bash

dracut –force
```

This will regenerate the *initrd* image to include the Hyper-V drivers necessary for migration to Hyper-V.

After executing these steps, you can proceed with migrating the virtual machine to Hyper-V.

4.3.10 Migration from VMWare to Proxmox

Prerequisites

- Ensure all requirements described in *HDD preparations for Proxmox* on the following chapter, are achieved.

In newer versions (tested in 8.3.0), Proxmox includes an integrated tool that enables the direct import of virtual machines from VMware.

For detailed instructions on configuring the import wizard for VMware migration, please refer to the Proxmox documentation.

- The minimum OpenScape Voice version that can be migrated from VMWare to Proxmox is V10_R3.34.0

After the import, the Virtual machine will require the Network settings to be adapted (eg. assign the vlan to the NIC), as the wizard only imports the NIC cards, not the NIC configuration.

4.3.10.1 HDD preparations for Proxmox

HDD preparation for SLES 12 UC deployments

To ensure that the necessary drivers for Proxmox are included in the *initrd* during the migration of an SLES 12 virtual machine from ESXi to Proxmox, execute the following commands while the VM is still running on the ESXi host.

These commands will update the *initrd* configuration to include the required *virtio* drivers:

1) Modify the *INITRD_MODULES* configuration to include the *virtio* drivers:

Edit the */etc/dracut.conf.d/90-virtio.conf* file (create it if it does not exist) and add the following lines:

```
bash

sed -i "/^INITRD_MODULES/s/\"$/ virtio_pci virtio_blk

 virtio_scsi\"/"

/etc/sysconfig/kernel
```

2) Rebuild the *initrd* to include the updated configuration:

Run the following command to regenerate the initrd with the updated configuration:

```
bash

mkinitrd
```

After executing these commands, proceed with the migration of the virtual machine to Proxmox.

HDD preparation for SLES 15 UC deployments

For an SLES 15 virtual machine, to ensure that the required drivers for Proxmox are included in the initrd during migration from ESXi to Proxmox, perform the following steps while the VM is still running on the ESXi host. These steps will update the *initrd* configuration to include the necessary virtio drivers:

1) Modify the dracut configuration to include virtio drivers:

Edit the */etc/dracut.conf.d/90-virtio.conf* file (create it if it does not exist) and add the following lines:

```
bash

echo "add_drivers+=\"virtio_pci virtio_blk virtio_scsi\"" > /etc/
dracut.conf.d/90-virtio.conf
```

2) Rebuild the `initramfs` using *dracut*:

Run the following command to regenerate the `initrd` with the updated configuration:

```
bash

dracut –f
```

This will regenerate the `initrd` image to include the virtio drivers necessary for Proxmox.

After executing these steps, you can proceed with migrating the virtual machine to Proxmox.

4.3.11 Create a Virtual Machine in Nutanix and install OpenScape Voice

Attention: The values configured in the following steps are presented as examples. These values may require adjustment based on a site's particular installation environment. The OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide document lists the configuration parameters needed to configure each OpenScape Voice node.

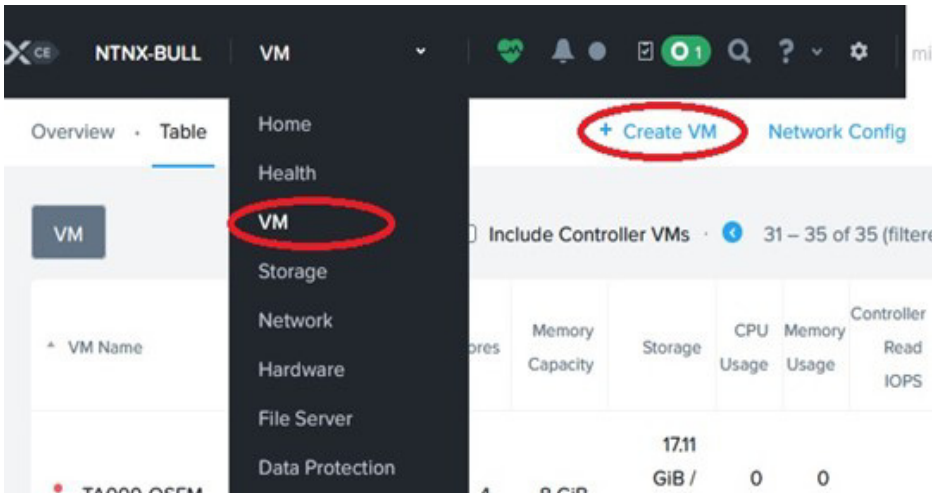
Attention: Some settings in the following steps are mandatory: The virtual disk drive should be set to **SCSI** and the CD/DVD Virtual Device Node should be set to **IDE.**

Attention: Default values should be used during the configuration process unless specified otherwise. Using other than the default values may result in unexpected behavior.

The machine dimensioning should be done based on the values in the OpenScape Virtual Machine Resourcing and Configuration Guide.

The **Create New Virtual Machine** wizard is used to configure virtualized OSV installations. This procedure assumes that the Datacenter and Cluster are already configured and that the prerequisites described in Chapter "Section 4.3.3, “Virtual Machine Guidelines”, are met (installation and configuration ISOs created).

1. In the Nutanix user interface access the VM menu and select **Create VM** from the top-right corner



2. In the new window, select a **Name** and the **Timezone** for the VM.

Note: The VM name is independent of the Hostname. Only letters, numbers, hyphens (-), and underscores (_) are allowed in VM names. Do **not** use spaces, dots, or other special characters.

---

3. In the **Compute Details** section, configure the following:

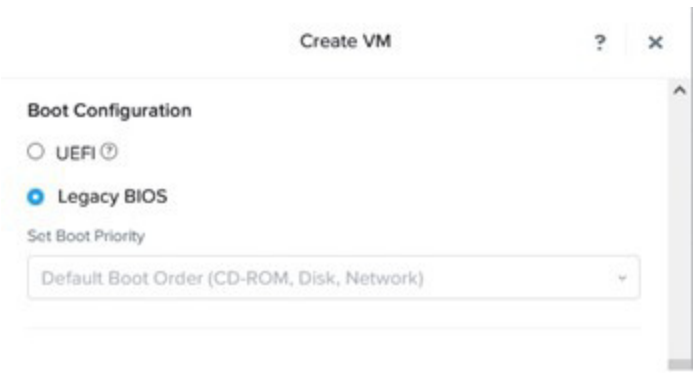
   1. The number of vCPUs
   2. The number of Cores per vCPU
   3. The required RAM

Note: All values should be configured according to OSV Virtual Machine Resourcing and Configuration Guide.

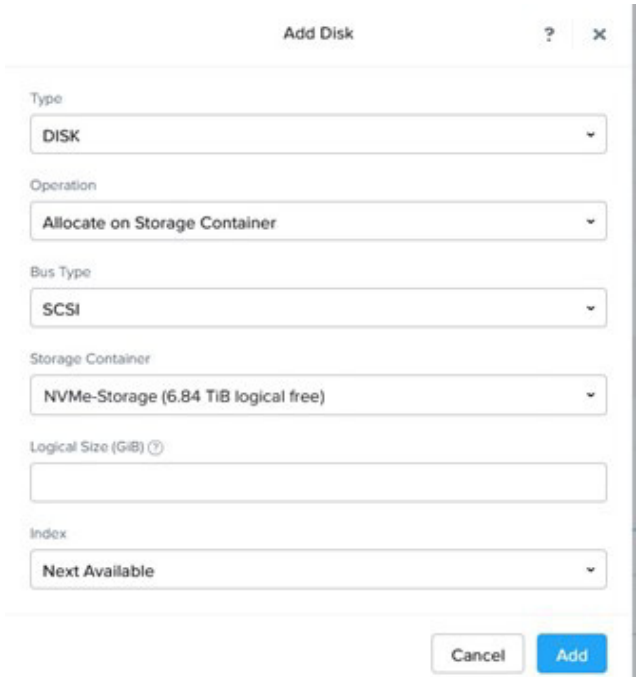
Note: Use a single socket configuration where possible for optimal performance. This means: 1 vCPU and desired number of Cores per vCPU. KVM hypervisors calculate the disk and memory size in GiB instead of GB.

---

4. In the **Boot Configuration,** you must select **Legacy BIOS** since OpenScape Voice does not support UEFI installation.

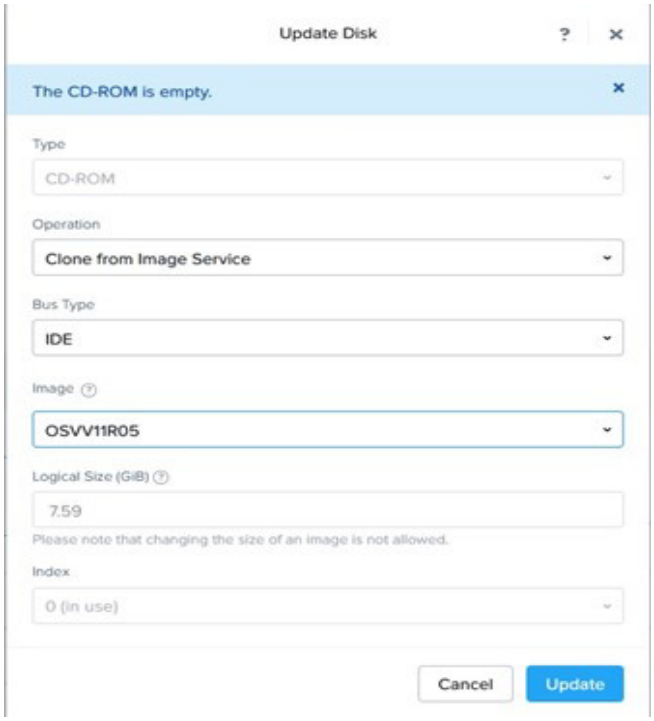


5. In the **Disks** section, click **Add New Disk**.



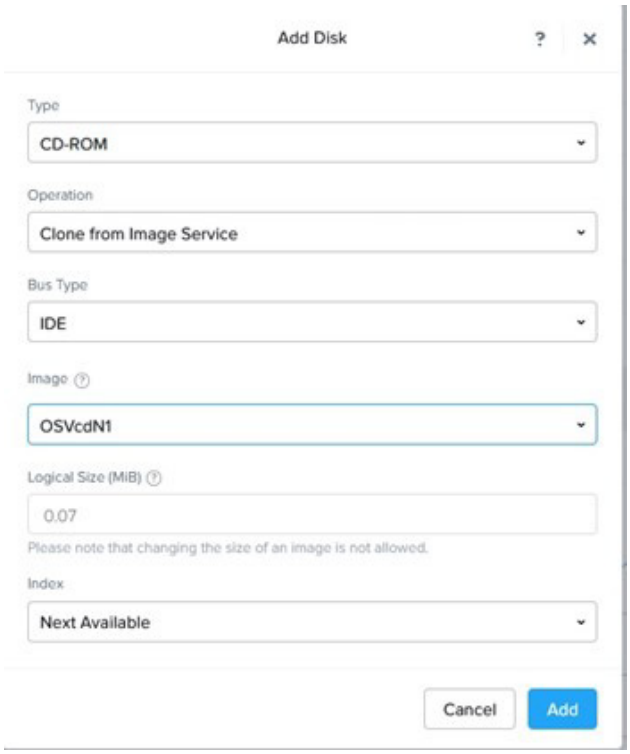
   1. From the **Type** drop-down menu, select **DISK**.
   2. From the **Operation** drop-down menu, select **Allocate on Storage Container.**
   3. From the **Bus Type** drop-down menu, select **SCSI**.
   4. From the **Storage Container** drop-down menu, select the available Storage Container.
   5. Configure the **Logical Size** according to the OpenScape Virtual Machine Resourcing and Configuration Guide.
   6. Click **Add**.

6. Mount the OSV installation ISO:



1. To mount the OSV installation ISO, click the edit icon to edit the CD-ROM entry.
2. From the **Operation** drop-down menu, select **Clone from Image Service**.
3. From the **Bus Type** drop-down menu, select **IDE**.
4. From the **Image** drop-down menu, select the previously created and uploaded OSV installation ISO image.
5. Click **Update**.

7. Add the second CD-ROM and mount the ISO previously uploaded to the Nutanix datastore, which contains all required files, including the *node.cfg* file, as well as any patch sets and license files.



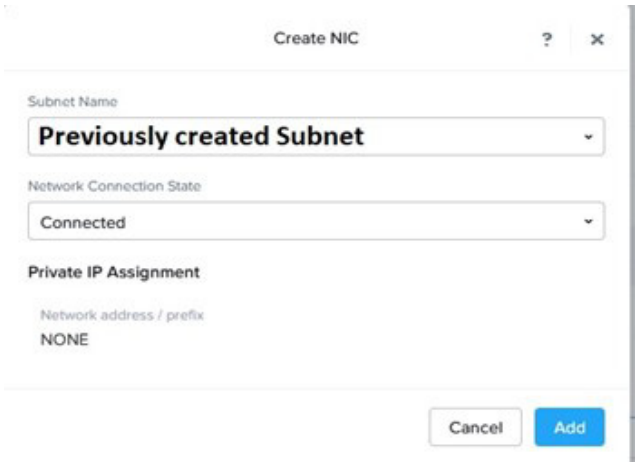
1. From the **Type** drop-down menu, select **CD-ROM**.

Note: For details, please check Section 4.3.4, “Creating a Virtual Machine Node.cfg File”. Mounting the ISO files can also be done after VM is created.

---

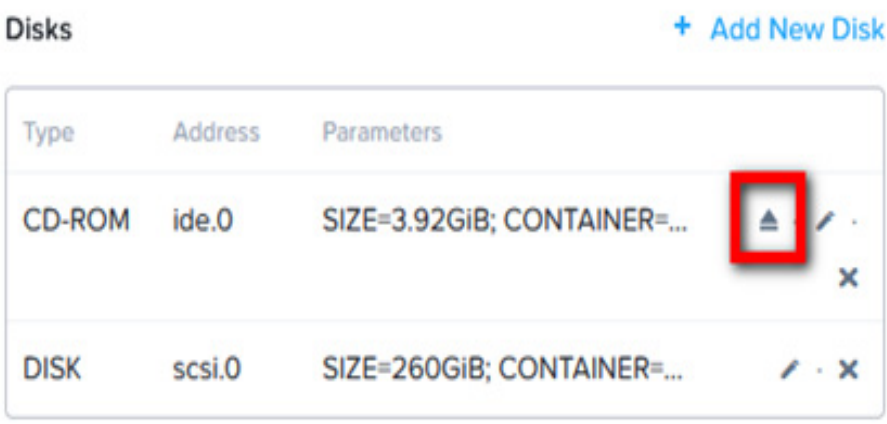
2. Click **Add.**

8. In the **Network Adapters (NIC)** section, add the VM NICs and select the appropriate (previously created) subnets according to the OSV networking requirements.

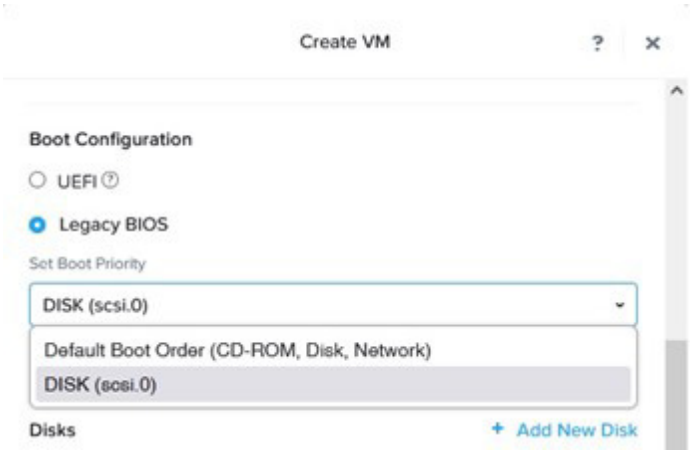


Note: Repeat the procedure for all required network interfaces, according to the **OpenScape Virtual Machine Resourcing and Configuration** Guide.

9. For duplex installations, repeat the procedure for the second node.
10. Once the Virtual Machine is created, you can change the hardware settings/ mount ISO files by right-clicking the **VM** and selecting **Update**.
11. Start the created VM with the OpenScape Voice and node.cfg ISOs mounted and proceed with the OSV installation through the console: right-click the VM and select **Launch Console**.
12. After the installation is complete, make sure to unmount the ISO images by selecting the **Eject** option: right-click the VM name, select **Update**, and go to the **Disks** section.



13. To improve boot time, adjust the boot order accordingly:



4.3.12 Migration from VMWare to Nutanix

Nutanix offers the **Nutanix Move** integrated tool for VM migration.

For detailed instructions on configuring the import wizard for VMware migration, please refer to the Nutanix documentation.

The minimum OpenScape Voice version that can be migrated from VMWare to Nutanix is **V11 R0.4**

Prerequisites

Before the actual migration, the following steps must be taken:

For a SLES 15 virtual machine, ensure that the required drivers are included in the Linux `initrd` before migrating from ESXi to Nutanix.

To do this, update the `initrd` configuration to include the necessary **virtio** drivers while the VM is still running on the ESXi host.

Login as "root" via ESXi console and modify the **dracut** configuration to include **virtio** drivers:

3. Edit the `/etc/dracut.conf.d/90-virtio.conf` file (if it does not exist, create it) and add the following lines:

bashecho "add_drivers=\"virtio_pci virtio_blk

virtio_scsi\"" >

/etc/dracut.conf.d/90-virtio.conf

2) Rebuild the `initramfs` using **dracut**:

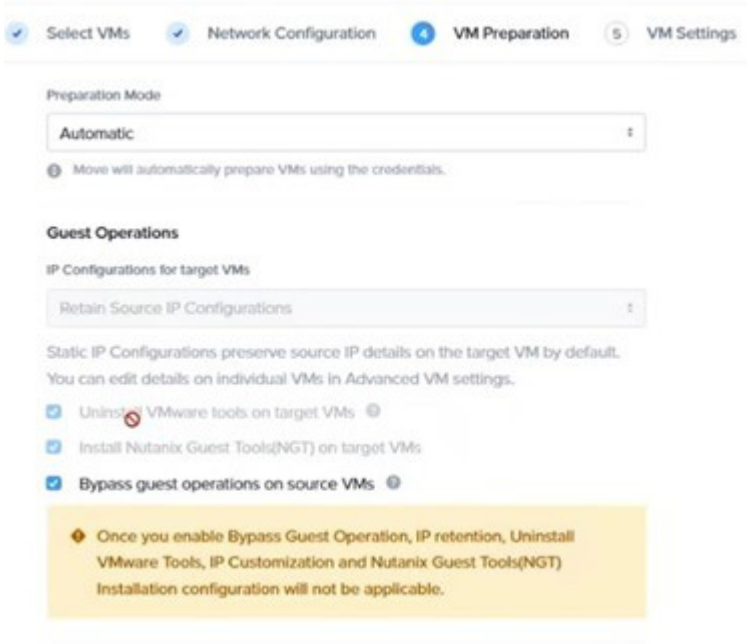
Run the following command to regenerate the `initrd` with the updated configuration:

bash

dracut --force

This will regenerate the `initrd` image to include the **virtio** drivers necessary for Nutanix.

Note: Since the VM preparation was performed manually in the previous step, during Nutanix Move procedure, on the **VM preparation** tab, in the **Guest Operations** section, select the **Bypass guest operations on source VMs** option.



4.4 Post Software Installation Activities

Note: The following activities should have been addressed by following Table 1, "OpenScape Voice Installation Checklist". It is a good practice to review Section 4.4 to ensure your installation is complete.

Note: It is recommended that any USB drive(s) used during an OpenScape Voice Installation procedure be removed from the server(s) at this time.

4.4.1 Profiles of Users root and srx

The active login profiles for users root and srx should not be modified. The OSV has functionality to protect the OSV login profiles for those two users from unauthorized changes. This is because alteration of these profiles typically causes issues to components that automatically login to the OSV nodes in order to perform various actions (e.g. NCPE/EZ-IP, Assistant etc).

There have been cases where a customer has modified the root or srx active login profiles to either gather or display system information during user login. The modification caused problems to components that login automatically as mentioned above. It should be noted that users root and srx are intended for OSV specific activities only; any user-initiated activities are to be done via the sysad user.

Attention: Root access is disabled for remote access by default.

The Pluggable Authentication Module (PAM) now compares the active login profile with the default login profile for user *root* or srx upon login. In case of a mismatch, the active login profile is overwritten with the default login profile. The PAM module also generates a major alarm followed by a matching clear alarm.

The active login profile files that are checked by the PAM module are the following:

1. `/root/.profile`
2. `/unisphere/srx3000/srx/.profile`
3. `/unisphere/srx3000/srx/.kshrc`
4. `/unisphere/srx3000/srx/.myrc`

4.4.2 Verify Remote Access for srx Account in a Standard Duplex

---

Attention: This section only applies to a standard duplex OSV system.

On each node of a duplex OpenScape Voice system, edit the

`/etc/security/access.conf`

file to permit access by the CMP as user *srx*.

For example, in the access.conf file, change this:

-:srx:ALL EXCEPT LOCAL <list of exception IP addresses which should be the nodes, the console, and ttys>

To this:

-:srx:ALL EXCEPT LOCAL<**FQDN of external (offboard) CMP** > <**IP address of external (offboard) CMP and** <list of original exception IP addresses which should be the nodes, the console, and ttys>

For example:

-:srx:ALL EXCEPT LOCAL **Ast247.site 10.235.200.247** bocastress1a bocastress1a_cip0 srxl70a_cip0 bocastress1b bocastress1b_cip0 srxl70b_cip0 console localhost tty1 tty2 tty3 tty4 tty5 tty6 clusternode1-priv clusternode2-priv

To obtain the IP address of the CMP, execute the following command from the OSV node:

```
# grep -i superuserip /etc/hiq8000/node.cfg
```

To obtain the FQDN of the CMP, execute the following command from the OSV node:

```
# nslookup <ip_address_of_CMP>
```

If the command above does not return an FQDN string for the CMP, then check with your network administrator. The network administrator can run the following command on the **offboard CMP server** to obtain the FQDN used during the CMP installation:

```
# cat /etc/hosts
```

An example of a truncated output:

```
:     :           :      :
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
10.235.200.247  Ast247.site  Ast247
```

You must ensure that there is an entry in each node's /etc/hosts file that maps the CMP FQDN to the CMP IP address. In the following example, the CMP FQDN is cmp49.mitel.stlab.com:

```
##############################################
# Please add new hosts under this line#
##############################################
165.218.177.242   cmp49.mitel.stlab.com   cmp49
```

If there is no entry for the CMP under the banner, add the CMP IP address and FQDN as the last line under the banner of the `/etc/hosts` file of each node.

With this configuration, the OSV will permit an external (offboard) CMP to connect to the OSV nodes using the CMP FQDN or IP address.

Note: Follow this link to return to Section 2.6, “Creating a Node.cfg File”, step Section 2.6.4.2, “Assistant/CMP”, on page 61.

Note: Follow this link to return to Section 5.2.6.7, “Remote Access for srx Account”, on page 337.

Note: Follow this link to return to Section 8.4.8, “Verify Presence of IP Address and FQDN of External CMP”, on page 467.

Note: Follow this link to return to Section 9.2, “Create the Node.cfg for the Target System”, step 3 "From the NCPE GUI:" substep f on page 547.

Note: Follow this link to return to Section 9.9, “Create the Node.cfg for the Target System (Source system = Low Cost)”, on page 557, step 3 on page 559.

4.4.3 Changing the User ID and Password for the IMM/ iRMC/BMC Account

The password of the maintenance controller is no longer listed in clear text. Because of this security enhancement the steps to update the maintenance controller user ID and password have changed. It is recommended the steps of this procedure be followed to change the User ID and Password for the IMM/ iRMC Account.

Change the default user ID (USERID) and password (PASSW0RD, the "0" character is the number zero) for the account as detailed below in steps 1 through 6.

Please review this section in its entirety before performing the procedure. After updating the IMM/iRMC user ID and/or password be sure to execute step 6 (to verify the shutdown agent functionality).

Note: Please note that the Virtual OSV has no maintenance controller interfaces (RSA, IMM, iRMC, VMK).

Attention: Regarding the Lenovo SR530 Server, the required settings at the steps of changing the default user ID and password should be in accordance with the Global Settings of the BMC Configuration for Users.

1. Log in as user *root*.
2. The *sa_ipmi.cfg* file will be read to update the maintenance controller user ID. Edit the sa_ipmi configuration file (*/etc/opt/SMAW/SMAWhaext/sa_ipmi.cfg*) to update the default user ID. Change only the user ID. The password will be updated in a following step. It is recommended these user ID guidelines be followed;
   - The user ID should contain a minimum of 5 alphanumeric characters.
   - The user ID can contain a maximum of 15 alphanumeric characters.
   - **The following words should NOT be user IDs:**
     - immroot
     - nobody
     - ldap
     - lighttpd
     - sshd
     - daemon
     - immftp

   The following example shows the *sa_ipmi.cfg* file default user ID (USERID) **BEFORE** the update:

```
# cat /etc/opt/SMAW/SMAWhaext/sa_ipmi.cfg
TestLocalStatus
encryptedPassword true
useCycle
retryPonCnt 2
fsc201 10.235.16.20:USERID:DUMMY cycle
fsc202 10.235.16.21:USERID:DUMMY cycle
root@fsc201:[/log] #124
#
```

The following example shows the *sa_ipmi.cfg* file **AFTER** the user ID was updated to NEWUSER:

```
# cat /etc/opt/SMAW/SMAWhaext/sa_ipmi.cfg
TestLocalStatus
encryptedPassword true
useCycle
retryPonCnt 2
fsc201 10.235.16.20:NEWUSER:DUMMY cycle
fsc202 10.235.16.21:NEWUSER:DUMMY cycle
root@fsc201:[~] #88
#
```

Attention: Be sure to edit the *sa_ipmi.cfg* file on both nodes in a redundant system.

Attention: In the next step the maintenance controller password is updated. The password information should be updated for each node entry in the *sa_ipmi.cfg* file. **Be sure to update the password information on both nodes in a redundant system.**

---

3. Update the maintenance controller password. It is recommended these password guidelines be followed;

   - A password should contain a minimum of 5 characters, one of which must be a nonalphabetic character.
   - A password can contain a maximum of 15 characters, one of which must be a nonalphabetic character.
   - A password **should NOT** contain the following characters;
     - **> (greater than sign)**
     - **< (less than sign)**
     - **"" (double quote)**

- **/ (forward slash)**
- **¥ (Yen sign)**
- **= (equals sign)**
- **! (exclamation point)**
- **? (Question mark)**
- **; (semi colon)**
- **, (comma)**
- **& (ampersand)**
- **$ (dollar sign)**
- **@ (at sign)**
- **# (hash)**
- **((parentheses)**
- **) (parentheses)**
- **’ (apostrophe)**
- ( ) **(space)**
- **` (Backtick - grave accent symbol)**
- **% (percent)**
- **+ (plus sign)**
- **[(square brackets)**
- **] (square brackets)**
- **{ (curly brackets)**
- **} (curly brackets)**
- **^ (Circumflex - caret)**
- **- (minus)**
- *** (Asterisk)**

The syntax of the command to update the maintenance controller password follows;

 # echo '<new_password>' | /opt/SMAW/SMAWhaext/bin/saCrypt -w <node_name>

In the following example the maintenance controller password is updated to NEWPSWD. It is necessary to update the password for each node entry of the *sa_ipmi.cfg* file (fsc201 and fsc202).

 # echo 'NEWPSW1' | /opt/SMAW/SMAWhaext/bin/saCrypt -w fsc201
 # echo 'NEWPSW2' | /opt/SMAW/SMAWhaext/bin/saCrypt -w fsc202

Attention: Regarding the Lenovo SR530 Server, the required settings at the steps of changing the default user ID and password should be in accordance with the Global Settings of the BMC Configuration for Users.

Attention: Be sure to update the password information on both nodes in a redundant system.

---

4. The user ID and password changes are updated to the maintenance controller with the *rsaConfig* tool. It is recommended the following syntax be used (the -v option provides a verbose output);

   # /unisphere/srx3000/callp/bin/rsaConfig -v

Attention: Be sure to execute the command on both nodes in a redundant system.

Note: There is a delay of approximately 90 second between the:
"Connected via IPMI device driver (KCS interface)" output
and the next IMM response:
"[set IMM.AuthorityLevel.2 Custom]".

```
[set IMM.RemoteConsolePriv.2 Yes]
IMM.RemoteConsolePriv.2=Yes

[set IMM.RemoteConsoleDiskPriv.2 Yes]
IMM.RemoteConsoleDiskPriv.2=Yes

[set IMM.RemotePowerPriv.2 Yes]
IMM.RemotePowerPriv.2=Yes

[set IMM.ClearEventLogPriv.2 Yes]
IMM.ClearEventLogPriv.2=Yes

[set IMM.BasicAdapterConfigPriv.2 No]
IMM.BasicAdapterConfigPriv.2=No

[set IMM.AdapterConfigNetworkSecurityPriv.2 No]
IMM.AdapterConfigNetworkSecurityPriv.2=No

[set IMM.AdvancedAdapterConfigPriv.2 No]
IMM.AdvancedAdapterConfigPriv.2=No

Beginning intermediate batch update.
Waiting for command completion status.
Command completed successfully.
Completed intermediate batch update.
Batch mode competed successfully.
root@bocast4b:[/unisphere/srx3000/callp/bin] #387
#
```

Attention: Be sure to execute the command on both nodes in a redundant system.

c) The following log **example** is from a Lenovo SR530 server:

```
# /unisphere/srx3000/callp/bin/rsaConfig -v
Host name for this node is: sr530n2
hardware platform is SR530
admin_interface = 'bond0'
Retrieving rsa configuration for node 2
rsa_enabled = 'YES'
Found IPMI parameters for this node
Username from SA_ipmi = USERID
IP address from SA_ipmi = 10.9.0.143
hardware platform is SR530
Successfully retrieved Username for user 2
Successfully retrieved MAC address

platform type=SR530, user number=2, access level=4 channel number=1

BMC Configuration Data
Network Data:
 Interface IP Address:    10.9.0.143
```

```
 Network Mask:            255.255.255.224
 Default Gateway Address: 10.9.0.129
 MAC address:             08:94:EF:6C:0B:B7

Login Data:
User Name: USERID
Username is already set correctly
Successfully set User Enable
Successfully set IP address for channel 1
Successfully set IP Netmask for channel 1
Successfully set Default Gateway for channel 1
Successfully set IP source for channel 1
Successfully retrieved Username for user 3
Configuring separate user account for the OSV Assistant
Username is already set correctly
Successfully set Password for user 3
Successfully set User Enable
Configuring user account privileges using the ASU utility
Lenovo Advanced Settings Utility version 10.4.94M
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2017 All Rights Reserved
Batch mode start.
Connected via IPMI device driver (KCS interface)
[set IMM.AuthorityLevel.2 Custom]
IMM.AuthorityLevel.2=Custom

[set IMM.UserAccountManagementPriv.2 No]
IMM.UserAccountManagementPriv.2=No

[set IMM.RemoteConsolePriv.2 Yes]
IMM.RemoteConsolePriv.2=Yes

[set IMM.RemoteConsoleDiskPriv.2 Yes]
IMM.RemoteConsoleDiskPriv.2=Yes

[set IMM.RemotePowerPriv.2 Yes]
IMM.RemotePowerPriv.2=Yes

[set IMM.ClearEventLogPriv.2 Yes]
```

```
IMM.ClearEventLogPriv.2=Yes

[set IMM.BasicAdapterConfigPriv.2 No]
IMM.BasicAdapterConfigPriv.2=No

[set IMM.AdapterConfigNetworkSecurityPriv.2 No]
IMM.AdapterConfigNetworkSecurityPriv.2=No

[set IMM.AdvancedAdapterConfigPriv.2 No]
IMM.AdvancedAdapterConfigPriv.2=No

Beginning intermediate batch update.
Waiting for command completion status.
Command completed successfully.
Completed intermediate batch update.
Batch mode completed successfully.
Created Assistant user configuration file /etc/opt/SMAW/SMAWhaext/
mctl_ipmi.cfg
```

Attention: If the next output displayed is "*ERROR*, it failed to set the BMC User 2 Password: IPMI Command Error, result=0, cc=0xD5. In that case, the BMC Global Settings and the password settings mentioned in the steps under Chapter 4, “Changing the User ID and Password for the IMM/iRMC/BMC Account” have not been configured as required.

d) The following log example is from a Lenovo SR630 V2 server

```
root@SR630 V2n1:[~] #1042
# /unisphere/srx3000/callp/bin/rsaConfig -v
Host name for this node is: SR630 V2n1
hardware platform is SR630 V2
Retrieving rsa configuration for node 1
admin_interface = 'bond0'
rsa_enabled = 'YES'
Found IPMI parameters for this node
Username from SA_ipmi = USERID
IP address from SA_ipmi = 10.0.23.10
hardware platform is SR630 V2
```

```
Successfully retrieved Username for user 2
Successfully retrieved MAC address

platform type=SR630 V2, user number=2, access level=4 channel number=1

BMC Configuration Data
Network Data:
 Interface IP Address:    10.0.23.10
 Network Mask:            255.255.255.224
 Default Gateway Address: 10.0.23.1
 MAC address:             38:68:DD:93:6B:99

Login Data:
 User Name: USERID
Username is already set correctly
Successfully set Password for user 2
Successfully set User Access for channel 1 to 4
Successfully set User Enable
Successfully set IP address for channel 1
Successfully set IP Netmask for channel 1
Successfully set Default Gateway for channel 1
Successfully set IP source for channel 1
Successfully retrieved Username for user 3
Configuring separate user account for the OSV Assistant
Username is already set correctly
Successfully set Password for user 3
Successfully set User Enable
Configuring user account privileges using the ASU utility
Lenovo Advanced Settings Utility version 10.4.94M
Licensed Materials - Property of Lenovo
```

(C) Copyright Lenovo Corp. 2007-2017 All Rights Reserved

Batch mode start.

Connected via IPMI device driver (KCS interface)

[set IMM.AuthorityRoleName.4 Custom]

IMM.AuthorityRoleName.4=Custom

[set IMM.AuthorityRolePriv.4 custom:rca|rcvma|pr|cel]

IMM.AuthorityRolePriv.4=custom:rca|rcvma|pr|cel

[set IMM.LoginRole.2 Custom]

IMM.LoginRole.2=Custom

Beginning intermediate batch update.

Waiting for command completion status.

Command completed successfully.

Completed intermediate batch update.

Batch mode completed successfully.

Created Assistant user configuration file /etc/opt/SMAW/SMAWhaext/mctl_ipmi.cfg

e) The following log example is from a Lenovo SR630 V3 server:

root@san03n1:[~] #307

/unisphere/srx3000/callp/bin/rsaConfig -v

Host name for this node is: san03n1

hardware platform is SR630V3

Retrieving rsa configuration for node 1

admin_interface = 'bond0'

rsa_enabled = 'YES'

Found IPMI parameters for this node

Username from SA_ipmi = USERID

IP address from SA_ipmi = 10.2.13.19

hardware platform is SR630V3

Successfully retrieved Username for user 2

Successfully retrieved MAC address

platform type=SR630V3, user number=2, access level=4 channel number=1

BMC Configuration Data

Network Data:

Interface IP Address: 10.2.13.19

Network Mask: 255.255.255.0

Default Gateway Address: 10.2.13.1

MAC address: C4:EF:BB:1B:77:33

Login Data:

User Name: USERID

Username is already set correctly

Successfully set Password for user 2

Successfully set User Access for channel 1 to 4

Successfully set User Enable

Successfully set IP address for channel 1

Successfully set IP Netmask for channel 1

Successfully set Default Gateway for channel 1

Successfully set IP source for channel 1

Successfully retrieved Username for user 3

Configuring separate user account for the OSV Assistant

Username is already set correctly

Successfully set Password for user 3

Successfully set User Enable

Configuring user account privileges using the ASU utility

Lenovo Advanced Settings Utility version 10.4.94M

Licensed Materials - Property of Lenovo

(C) Copyright Lenovo Corp. 2007-2017 All Rights Reserved

Batch mode start.

Connected via IPMI device driver (KCS interface)

[set IMM.AuthorityRoleName.4 Custom]

IMM.AuthorityRoleName.4=Custom

[set IMM.AuthorityRolePriv.4 custom:rca|rcvma|pr|cel]

IMM.AuthorityRolePriv.4=custom:rca|rcvma|pr|cel

[set IMM.LoginRole.2 Custom]

IMM.LoginRole.2=Custom

Beginning intermediate batch update.

Waiting for command completion status.

Command completed successfully.

Completed intermediate batch update.

Batch mode completed successfully.

Created Assistant user configuration file /etc/opt/SMAW/SMAWhaext/mctl_ipmi.cfg

5. The *rsaConfig* tool can be employed with a -l option (list) to list that nodes maintenance controller (BMC) configuration and verify the user ID and password combinations (of the maintenance controller and the Common Management Platform (CMP) Assistant). **If the configuration list is satisfactory proceed to step 6 (to verify the shutdown agent functionality**).

   Attention: Execute the command on both nodes in a redundant system.\

```
root@fsc201:[/etc/opt/SMAW/SMAWhaext] #140
# /unisphere/srx3000/callp/bin/rsaConfig -l

BMC Configuration Data
Network Data:
  Interface IP Address:    10.235.16.20
  Network Mask:            255.255.255.0
  Default Gateway Address: 10.235.16.1

Login Data:
  User Name: NEWUSER
  Successfully verified Password for User Name: NEWUSER
  Secondary User Name: OSVAssistant
  Successfully verified Password for User Name: OSVAssistant

root@fsc201:[/etc/opt/SMAW/SMAWhaext] #141
#
```

6. Verify the new configuration's functionality for both nodes. Refer to Section 6.8, “Verifying the Shutdown Agents Configuration”, on page 409.

Attention: Be sure to verify the configuration on both nodes in a redundant system.

4.4.4 Configuring the Ethernet NICs for Fixed Operation

By default, Ethernet NICs are set to auto-negotiate interface speed and mode.

If the customer’s LAN equipment does not support auto-negotiation, the Ethernet NICs have to be set to the interface speed and mode appropriate for the customer’s LAN.

Only the interfaces that are directly connected to the customer's LAN need to be changed.

The supported fixed operation speeds and modes are as follows:

- 100BaseTx-FD
- 1000BaseTx-FD

Attention: Only the 100 mb/sec interface can set auto-negotiate to "off" (neg=off), if desired by the customer. The 1000 mb/sec interface should always set auto-negotiate to "on" (neg=on).

Disable auto-negotiation and set the Ethernet NICs for fixed operation as follows:

1. Log in as *root*.
2. Create a Linux text file named “etherset” in the */etc/init.d* directory and enter the text as follows:

Note: This step employs the configuration of a duplex, co-located server as an example. Only the interfaces that are directly connected to the customer's LAN should be changed.

The Ethernet assignments for a duplex, co-located server follow. The Ethernet NICs that are used for the cluster interconnects do not need to be changed in a co-located configuration since the two OSV nodes are directly connected by cables. Those crossover cables are not connected to the customer's LAN.

Note: The cluster interconnects of a geo-separated configuration will be connected to the customer's LAN. In this scenario, the cluster interconnects should be included in the *etherset* file.

```
#!/bin/bash
### BEGIN INIT INFO
# Provides: etherset
# Required-Start: network
# Required-Stop:
# Default-Start: 3 5
# Default-Stop:
# Description: Configure the network interfaces
### END INIT INFO

echo “begin etherset”
ethtool -s eth0 speed 100 duplex full autoneg off
ifconfig eth0 up
ethtool -s eth1 speed 100 duplex full autoneg off
ifconfig eth1 up
ethtool -s eth2 speed 100 duplex full autoneg off
ifconfig eth2 up
ethtool -s eth4 speed 100 duplex full autoneg off
ifconfig eth4 up
ethtool -s eth5 speed 100 duplex full autoneg off
ifconfig eth5 up
ethtool -s eth6 speed 100 duplex full autoneg off
ifconfig eth6 up
echo “end etherset”
exit 0
```

In this example, the speed is set to 100, with full duplex operation, and auto negotiation turned off. For 1000BaseTx, specify speed 1000 and auto-negotiation must be turned on.

3. Set the Ethernet interfaces to the values specified in the *etherset* file with following commands:

cd /etc/init.d
chmod +x /etc/init.d/etherset
insserv etherset /etc/init.d/etherset
/etc/init.d/etherset

4. If applicable, repeat steps 1 on page 289 through 3 on the other node.
5. On the OpenScape Voice Installation Checklist, initial step 13 and proceed to step 14.

4.4.5 Checking Ethernet Port Assignments

Check the Ethernet port assignments as follows:

1. As *root*, issue the following command for each of the Ethernet interfaces (eth0 through eth2 for a single node system and eth0 through eth7 for a redundant system):

   ```
   ethtool <Ethernet interface>
   ```

   If you check a non-existent Ethernet interface, the following snapshot shows what is displayed:

   ```
   # ethtool eth3
   Settings for eth3:
   Cannot get device settings: No such device
   Cannot get wake-on-lan settings: No such device
   Cannot get message level: No such device
   Cannot get link status: No such device
   No data available
   ```

   The following examples show the information displayed for eth0 through eth7 on a redundant system. The eth0, eth1, and eth2 interfaces should be displayed for a single-node system.

Attention: steps 2 through 5 are intended for fresh installations of OpenScape Voice servers only. Service degradation will occur if these steps are performed on a live system.

---

2. Unplug an Ethernet connector and issue the ethtool command (specifying that interface). The display indicates which port (Link) was disconnected (**Link detected: no**).

   ```
   # ethtool <Ethernet interface>
   ```

   Note: Chapter 3 of this document contains “Connecting the Cables” information for each platform. Within these subsections are snapshots of the server backplane that will help in identifying the physical locations of the Ethernet interfaces.

   A console snapshot is provided as an example;

```
# ethtool eth7
Settings for eth7:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: Unknown! (65535)
        Duplex: Unknown! (255)
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: d
        Wake-on: d
        Current message level: 0x00000007 (7)
        Link detected: no
```

3. Restore the Ethernet connector and reissue the ethtool command to verify the Link was reactivated (**Link detected: yes**).
4. Repeat steps 3 and 4 on all the Ethernet ports on this node.
5. If applicable, repeat steps 1 through 4 on the other node.
6. On the OpenScape Voice Installation Checklist, initial step 14 and proceed to step 15.

4.4.6 Testing the KVM/Mouse Combination

If the equipment for OpenScape Voice includes a KVM, the KVM/mouse combination must be tested for compatibility.

When the KVM is not switched to a server/node, it must simulate the connection. If a different signature is generated on the simulation, the server/node requests clarification of the type of mouse in use.

Some combinations of KVM switches and mice are not 100% compatible. Failure to have a correctly working KVM/mouse combination will cause the server to hang (waiting for operator input) during a reboot.

Test the KVM as follows:

1. Select the test node with the KVM and log in as *root*.
2. Run `hwbootscan`. It should produce no output.
3. Switch the KVM to another position.
4. Remotely log in to the test node as user *sysad* and then switch to user *root* using the switch user (**su -**) command.
5. Run `hwbootscan`. It should produce no output.

   If a menu is displayed to select a mouse, perform the following steps:

   a) When prompted, select the mouse type, and select **ACCEPT**.

   b) Switch the KVM back to the test node.

   c) Run `hwbootscan`. It should produce no output.
6. Repeat this procedure on the other node.
7. On the OpenScape Voice Installation Checklist, initial step 15 and proceed to step 16.

4.4.7 SNMP Community Names on OpenScape Voice

Note: Any alphanumeric character and ONLY the following special characters are allowed for the SNMP community string:

! (exclamation mark)
(hash mark)
% (per cent)
* (asterisk)
+ (plus)
- (hyphen)
. (period or full stop)
: (colon or full colon)
= (equals)
? (question mark)
@ (at)
[(open or left bracket)
] (close or right bracket)
^ (caret)
_ (underscore)
{ (open or left parenthesis)
} (close or right parenthesis)
~ (tilde)

4.4.7.1 Changing the Community String for the Emanate Master Agent

---

Note: To change the SNMP community name string to meet site security requirements, it is strongly recommended that you contact your next level of support before attempting the following procedures."

Note: Avoid using any UNIX special characters (e.g., ampersand (&), semi colon (;), etc.) when changing the SNMP community string as these characters may cause translation errors.

You can change community strings with the use of Cli. In order to use startCli, follow the procedure below:

1. Login to CLI as: **sysad**

   Node1:/home/sysad (62> **startCli**

2. Navigate to menu 6 > 1 > 9 > 2

3. Change the read-only/read-write community strings as shown below:

```
SNMP Management (methods):

        Display SNMP Configuration.....................1
        Modify SNMP Configuration......................2

        Return.................................99

        Selection (default: 1): 2

        *** Modify SNMP community String ***

        Enter Read-only SNMP community String: <Any ASCII
string (max length: 64)> (default: SENread):
        Enter Read-write SNMP community String: <Any ASCII
string (max length: 64)> (default: SENSnmp):

        Do you want to execute this action? <y/n> (default:
yes):
        Checking connection with grd404n1.
        Checking connection with grd404n2.
        Backing up original configuration file.
```

```
Copying new configuration file to grd404n1.
Copying new configuration file to grd404n2.
Please wait. Applying new configuration on grd404n1.
Please wait. Applying new configuration on grd404n2.
Validating new configuration
Done.
```

4. Navigate to menu 6 > 1 > 9 > 2 to display the SNMP configuration for verification purposes.

Here is a link back to Section 17.3.1.1.

5 Installing the OpenScape Applications

The following documents (available on Mitel Doc Center) will be referenced in this section:

Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section "Installing and Configuring the Computer and Operating System".

OpenScape UC Application V10 Configuration and Administration.

OpenScape UC Application V11, ISO Installation and Upgrade, Installation Guide

OpenScape UC Application V11, Configuration and Administration, Administrator Documentation

OpenScape Common Management Platform V10, Administration, Administrator Documentation, the subsection titled "Software Activation (User Interface Patching)"

For media server announcement and treatments, refer to *OpenScape Voice V11 Administration, Administrator Documentation*, the section titled *Media Services*.

For media server hardware requirements, refer to *OpenScape Media Server Vx Administrator Documentation* (where *x* is the software release version).

5.1 Installation Overview

This chapter provides a guideline for installing the OpenScape Applications (OpenScape Voice Assistant, OpenScape Media Server, Deployment Service [DLS], and OpenScape UC Application).

To execute the steps described in this section, you need to know which deployment scenario you want to use.

Deployment Scenarios:

The Applications deployment scenarios are:

- Integrated Simplex
- Standard Duplex -small deployment
- Standard Duplex - large deployment
- Standard Duplex - very large deployment
- Media Server Standalone
- Multiple Communication Server Administration (no UC capability)

This document contains the installation and update procedures of OpenScape UC Applications for the following deployment scenarios:

- Integrated simplex
- Media server Standalone
- Multiple Communication Server

Note: Information for installing the OpenScape UC Application separately (apart from the normal OpenScape Voice installation) is included in the *OpenScape UC Application V10, Installation Instructions, Installation Guide.* There the installation procedures for standard duplex - small deployment and the standard duplex - large deployment are described.

The OpenScape Applications are installed:

- Internally on the integrated simplex.

  Note: On a integrated system the Applications are installed as part of the OpenScape Voice Image installation. Use the OpenScape Voice V11 Reference Image USB stick that contains the node.cfg file to install the OpenScape Applications onto the OpenScape Voice node. Integrated systems response files are built automatically as part of the installation process. Response files no longer need to be generated for images and are not required on USB sticks. If a response file is found on the USB stick that file will take precedence over the file that is automatically generated via the Image installation. Refer to Section 4.2, “Installation via DVD”, on page 231 for more details on the installation procedure.

- Externally on an applications server for the standard duplex.

The Applications installation process follows this general outline:

1. Configure the installation with the response file (knut.responsefile.txt). A sample of the response file is copied from the setup file (OpenScapeUcSuiteApps-Repository-<version>.iso) OpenScapeUcSuiteApps-Repository-<version>.iso for the OpenScape UC Application to the respective computer and edited. **Remember that response files no longer need to be generated for integrated systems and are not required on USB sticks.**
2. Transfer the “response” files (or file) to the USB stick that contains the node.cfg file for an integrated system if needed or to the external applications server for a standard duplex system.

3. Installation

Attention: For offboard (external) Applications servers the OpenScape UC Application components are installed by osc-setup (NOT zypper or yast). Only use zypper or yast to install the osc-setup RPM package.

For information on Media Server Standalone, secured for JITC deployment, see Section 5.2.4, “Updating using the CMP (UI Patching) instead of osc-setup”

For information on Multiple Communication Server Admin Secure, secured for JITC deployment - see Section 5.2.6, “Installation/Update Instructions for Multiple Communications Server Admin deployment”.

5.1.1 Prerequisites

The installer needs *root* access or administrator rights on the SLES operating system of the machine on which the OpenScape Applications will be installed.

For a standard duplex system:

- OpenScape Voice software must be installed. Refer to Chapter 2, “Preparing for the Installation”, Chapter 3, “Installing the Hardware Platform”, and Chapter 4, “Installing the OpenScape Voice Reference Image” for information.
- The minimum patch level for OpenScape Voice must be installed to ensure compatibility with the OpenScape Applications.

  Refer to the OpenScape Applications release note to confirm the minimum patch level for OpenScape Voice. The minimum patch level in the release note supersedes the patch level specified here.
- A currently supported external applications server or a customer-provided external applications server with the appropriate SLES OS and service pack level (that meets or exceeds the requirements described in Section 5.1.2, “External (Offboard) Applications Server Hardware Requirements”, on page 298) must be available for installation of the OpenScape Applications.

For more information on the OpenScape Applications, refer to the release notes.

5.1.2 External (Offboard) Applications Server Hardware Requirements

---

Attention: When using syncUC with the "Multiple Communication Admin Server" or "Media Server Standalone" Applications deployments; the recommended disk sizing is 2 x 300GB in RAID-1 configuration.

For more information regarding syncUC, refer to Section 5.2.16, “syncUC”, on page 365.

Customer-provided hardware for an external applications server (i.e., Media Server Standalone and the Multiple Communications Server deployments) must meet or exceed the specifications described here:

For media server announcement and treatments, refer to *OpenScape Voice V11 Administration, Administrator Documentation*, the section titled *Media Services.*

For media server hardware requirements, refer to *OpenScape Media Server Vx Administrator Documentation* (where *x is the software release version*).

For Prefix Access Code (PAC) information, refer to Section 14.2, “How to Add/ Delete Default PACs for Vertical Services”, on page 598.

Multiple Communications Server deployments must meet or exceed the specifications described in the UC documentation.

5.2 Installation Instructions for Applications Servers

Note: Information for installing the OpenScape UC Application separately (apart from the normal OpenScape Voice installation) is included in the *OpenScape UC Application V10, Installation Instructions, Installation Guide*. There, the installation procedures for standard duplex – small deployment and the standard duplex – large deployment are described.

Note: The Deployment Service (DLS) component might not be supported on the external applications server due to sizing limitations. A separate server running Microsoft Windows might be required for the DLS component. Please review the DLS release notes for sizing limitations when DLS is installed as a component of the external applications server.

5.2.1 SLES Partitioning and Installation on the External Applications Server

The instructions for the SLES partitioning and installation of the appropriate SLES distribution onto customer provided hardware are provided in;

Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section “Installing and Configuring the Computer and Operating System”.

It is recommended that this section be reviewed in its entirety before partitioning the server and installing the appropriate SLES OS and service pack level.

5.2.2 External Applications Server Port List

To harden the operating system of the external OpenScape Applications server, activate the Linux Firewall (using YaST) or use firewall in the network infrastructure to block all ports not listed in Table 16. Access the external applications server firewall port table as follows:

1. Click **Yast**, **Security and Users**, **Firewall**, **Allowed Services**, and **Advanced**.
2. Update the port data to the firewall as specified in Table 16 on page 300.
3. When you are finished updating the port data, click **Advanced**, **Next**, and **Accept**.

Table 16 lists all the ports that should not be blocked. During installation of the OpenScape Applications these ports are required incoming.

Port	Protocol	Description
25	TCP	For SMTP groupware integration
443	TCP	HTTPS for browser access to Common Management Platform
483	TCP	Office Communicator connection
4444	TCP	OpenScape User Management Access (optional)
4708	TCP	SOAP communication to Shared Services. Required for OpenScape RichClient using HTTP.
4709	TCP	SOAP communication to Shared Services. Required for OpenScape RichClient using HTTPS.
4710	TCP	Osgi communication
4711	TCP	Osgi communication via TLS
7778	TCP	XML asynchronous events for WebClient
7788	TCP	XMLS secure for WebClient
7789	TCP	HTTP access to OpenScape WebClient
7800	TCP	Application discovery (optional; required for distributed installations)
8443	TCP	HTTPS access to OpenScape WebClient
8787	TCP	Communication from XPressions
8818	TCP	Communication (HTTPS) to CLM
8819	TCP	Communication (HTTP) to CLM
10001	TCP	Communication from XPressions
16760	TCP	Solid database connection
61616	TCP	Symphonia events
UDP Protocol Ports		
161	UDP	SNMP Get and Set Requests (optional, only required for communication to SNMP management systems, for example: OpenScape Voice Fault Management)
162	UDP	Retrieve alarms via SNMP traps.
2427	UDP	MGCP protocol of the external OpenScape Media Server
5004:5008	UDP	RTP (voice) payload for the external OpenScape Media Server
5060:5061	UDP	SIP signaling for the external OpenScape Media Server
20000:21000 (see Note)	UDP	RTP (voice) payload for the external OpenScape Media Server.
45566	UDP	Symphonia Multicast Discovery

Table 16 Port List for the External OpenScape Applications

5.2.3 Installation/Update Instructions for Integrated Simplex Systems

Attention: If an Applications Installation, Update or Upgrade failure should occur, and there are any questions regarding the Applications server(s) status or recovery, contact your next level of support for assistance.

Attention: For details regarding OpenScape UC Application components please refer to the *"OpenScape UC Application V10, Installation and Upgrade, Installation Guide"* document.

Attention: Refer to the OpenScape Applications release notes for the latest updates to the OpenScape Applications. Carefully review the Installation Prerequisites section of the OpenScape Applications release note for any activities that might be required before creating the response files.

5.2.3.1 Prepare Installation of Integrated Simplex

To prepare the integrated environment for the installation please refer to Section 5.2.10, "Providing a Setup Medium for the Applications", on page 341.

Section 5.2.10 will guide you through the preparation of the media for installation. At the end of Section 5.2.10 a link back to Section 5.2.3.2, "Response File for Integrated Deployments", on page 302 is provided.

5.2.3.2 Response File for Integrated Deployments

Attention: If you arrived here from Section 9.12.2.1, “Log In to Node 2”, Table 27, step 7; It is recommended the /enterprise/servicetools/install/conf/responsefile.txt file (saved in step 3a of Table 27) be used as a template for creating the response file. Please note that no deviations from the values recorded in the saved responsefile.txt file are allowed.

You must know the following passwords to create the new response file (and complete the Task List procedure);

1) The password of the Symphonia administrator.
2) The password of the Solid database administrator.

The Symphonia administrator and Solid database administrator passwords must be entered as 'clear' text (i.e., unencrypted) in the new response file.

Note: Before creating response files, ensure that the customer administrator or representative has provided you with the necessary configuration data.

Execute the following steps on the application computer to create a response file for the application computer.

All commands should be executed as the user *root*.

1. Change directory to the installation repository created in the corresponding step of Section 5.2.10.4, “Finish the Installation Medium Setup” and then copy the appropriate response file to the /root path. In the examples of this guide the path was "/software/tmpREPO"

   ```
   # cd /software/tmpREPO
   ```

   ```
   # cp templates/knut.responsefile.txt.templ_IntegratedSimplex
   /root/knut.responsefile.txt
   ```

   Attention: Copy the file as specified to the directory named `/root` but not to the Root directory `/`.

   ---

2. Open the response file with an editor (for example with vi):

   ```
   vi /root/knut.responsefile.txt
   ```

3. Look for the following line:

   ```
   SI_SYMPHONIA_ADMIN_PASSWORD=<PLACEHOLDER_symphonia_admin_pass
   word>
   ```

Replace `<PLACEHOLDER_symphonia_admin_password>` with the password of the Symphonia administrator.

Note: This password must comply with the security policies, which are defaulted as follows:
- At least 8 characters
- At least one special character
- At least one number
- At least one capital letter
- Not more than 3 identical characters in a row

---

4. Look for the following line:

   `SI_COMMUNITY_NAME=<PLACEHOLDER_community_name>`

   Replace `<PLACEHOLDER_community_name>` with the community name.

Attention: The Community has nothing to do with SNMP.
Capital letters, small letters and underscore are permitted. The latter must not appear at the beginning or end of the name. The corresponding regular expression reads as follows: `[A-Za-Z0-9][A-Za-Z0-9_]*[A-Za-Z0-9]`

Note: The value you assign to `SI_COMMUNITY_NAME` must be the same in all `knut.responsefile.txt` files on all computers (application, front-end and Media Server computers).

---

5. Look for the following line:

   `SI_PRIMARY_NODE_HOST=<PLACEHOLDER_hostname>`

   Replace `<PLACEHOLDER_hostname>` with the fully qualified domain name (FQDN) or the (administration subnet) IP address of the Integrated Simplex server. We recommend using the FQDN.

6. Look for the following line:
   `SI_LOCAL_HOST=<PLACEHOLDER_hostname>`

   Replace `<PLACEHOLDER_hostname>` with the fully qualified domain name (FQDN) or the (administration subnet) IP address of the Integrated Simplex server. We recommend using the FQDN.

7. Look for the following line:
   `SI_DB_HOST=<PLACEHOLDER_hostname>`

   Replace `<PLACEHOLDER_hostname>` with the fully qualified domain name (FQDN) or the (administration subnet) IP address of the Integrated Simplex server. We recommend using the FQDN.

8. Look for the following line:

   `SI_DB_LOGON_PASSWORD=<PLACEHOLDER_dbms_dba_password>`

Replace `<PLACEHOLDER_dbms_dba_password>` with the password of the Solid database administrator. It must not be the default password (`dba`). Employ a secret, complex string of characters for the database password.

9. If the response file is created for an upgrade scenario, in which the applications database has to be migrated from an older release to a new release, proceed as follows:

   a) Look for the following line:

   ```
   SI_FW_DB_MIGRATION=false
   ```

   b) Set the migration flag to “true”:

   ```
   SI_FW_DB_MIGRATION=true
   ```

10. Verify response file on the node. Change directory to the installation repository and run the checkResponsefileOnLocalNode.sh script. For our example case;

    ```
    # cd /software/tmpREPO
    # sh support/checkResponsefileOnLocalNode.sh
    ```

11. Ensure that the response file is saved and kept in a safe location. The response file is not currently contained in the system backup sets, but it is needed to rebuild the system during a crash recovery.

Note: The restore mechanism uses the database administrator password from the original system, where the backup was taken, to access the Solid database. If this password is not known, no recovery is possible. This password is defined in the response file and that is why the created response file must be backed up in a safe location.

If you are performing a new Applications installation (not an upgrade or migration), proceed to Section 5.2.3.3, “Installation of Integrated Applications”, on page 305.

If you are performing an upgrade or migration procedure and arrived here from Section 9.11.2, “Building Simplex Response File from Template”, on page 563, follow this link back to step 1 on page 563, Section 9.11.2, “Building Simplex Response File from Template”.

5.2.3.3 Installation of Integrated Applications

Information regarding Integrated OpenScape Voice system backups can be found in the “OpenScape *Voice V11 Service Manual, Service Documentation.*”

Note: DLS is installed by default on the integrated Simplex.

Note: The Media Server SIP endpoint for Integrated Simplex deployments is associated with the non-standard port numbers 5062 (SIP) and 5063 (SIP-TLS) for the signaling between the OSV and the Media Server. Change the Integrated Media Server SIP listening ports via CMP from 5060/5061 to 5062/5063. If you need to create a SIP endpoint for the MS, use ports 5062/5063 as well. Update the corresponding packet filter rules with the new port numbers.

---

1. From the installation repository, execute the following commands to install UC Applications on the integrated simplex system.

   These commands should be executed as the user *root*.

   Note: The path "/software/tmpREPO" is taken from the command examples provided in Section 5.2.10.4, “Finish the Installation Medium Setup”, step 6 on page 352.

   Command examples;

   ```
   # cd /software/tmpREPO
   # sh support/installIntegratedSimplex.sh importBuildKey
   ```

   Note: (If asked to import data into the rpm db, enter y)

   ```
   # sh support/installIntegratedSimplex.sh install /root/
   knut.responsefile.txt
   ```

   Note: A blank space follows the word “install” in the command above (i.e., `install /root/knut.responsefile.txt`). The typical installation takes approximately one hour.

   ---

2. In case of an error, always select the option “despite the inferior architecture”. Example given:

   Problem: OpenScapeUC_Large_MS-6.0_1.0.0-007.noarch requires OpenScapeUC_Large_MS, but this requirement cannot be provided uninstallable providers: OpenScapeUC_Small-6.0_1.0.0-007.noarch[270fc4d9389754e36bb4dbe2a725408d]
   Solution 1: Following actions will be done:

install symphonia-6.0_1.5.0-058.i586 **despite the inferior architecture**
install symphonia-jre-ibm-6.0.9.2-4.i386 despite the inferior architecture
Solution 2: do not install OpenScapeUC_Large_MS-6.0_1.0.0-007.noarch
Solution 3: break OpenScapeUC_StandardDuplexSmall by ignoring some of its dependencies
Choose from above solutions by number or cancel [1/2/3/c] (c):

3. Type **1** and press **Enter**.
4. When the 'Continue' prompt is presented push the 'y' key and then the return key. Example given;

   72 packages to upgrade.
   Overall download size: 724.7 MiB. After the operation, 17.7 MiB will be freed.
   Continue? [y/n/?] (y): y

5. Check for any newer Applications patch sets or HotFixes and install them according to the corresponding release notes (if applicable).

Attention: If more packages are required for your install (i.e.; languages besides English), do not execute step 7 on page 307 until **Section 5.2.5.4, "Adding Additional Packages/Languages", on page 330** is reviewed.

---

6. Start the OpenScape Applications;

   ```
   # /etc/init.d/symphoniad start
   ```

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

Questions should be addressed to your next level of support.

7. If the installation process is complete the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.2.3.4 Adding Additional Packages/Languages

For media server announcement and treatments, refer to *OpenScape Voice V11 Administration, Administrator Documentation*, the section titled *Media Services*.

This section includes instructions for media server language package adds. Refer to Appendix 28, “Guidelines for Language and Application Package adds to Simplex Systems”, on page 783 for more application and language package add instructions.

For Integrated systems, the default installation applies only the English language for the Media Server telephone prompts. If you wish to install further languages, execute the following steps:

All commands are to be executed as user *root*.

1. Verify that the installation files (ISO files) you require for languages are provided in osc-setup with the 'list repository' (lr) command;

   Command example;

   ```
   # osc-setup lr
   ```

   ```
   Logging to: /var/log/OpenScapeUC/osc-setup-2012-04-12_10-04-42.log
   ```

   ```
   osc-setup version: "1.4.5-17"
   ```

   ```
   SUSE VERSION: 11 SERVICEPACK: 1
   Registered repository (url):
   1   dir:///software/tmpREPO
   Operation took:  0 seconds
   ```

2. If the installation repository does not exist proceed to step 4 on page 308.

   If the installation repository exists, use the osc-setup search (se) option to list the available packages (in this case announcements);

   ```
   osc-setup se --match-any announ
   ```

   Command example:

   ```
   # osc-setup se --match-any announ
   ```

   ```
   Loading repository data...
   ```

   ```
   Reading installed packages...
   ```

```
S | Name | Summary | Type
--+--------------+-------------------------------------------------------------------
| mediaserver_announcements_ar | Mediaserver_announcements_ar | package
| mediaserver_announcements_bg | Mediaserver_announcements_bg | package
...
i | mediaserver_announcements_en_us | Mediaserver_announcements_en_us | package
| mediaserver_announcements_en_za | Mediaserver_announcements_en_za | package
...
```

Note: An 'i' in the column S column indicates that package is already installed.

---

3. If the language is not listed, proceed to step 4 on page 308.

   If the required language is listed then execute the following command for installing another language;

   ```
   sh support/installIntegratedSimplex.sh addLang <component>
   <lang[,lang]>
   ```

   Change directory to the installation repository and run the command. Examples follow;

   a) Adding 1 language;

   ```
   # /etc/init.d/symphoniad stop
   # cd /software/tmpRepo
   # sh support/installIntegratedSimplex.sh addLang
   mediaserver_announcements en_za
   ```

   b) Adding multiple languages;

   ```
   # /etc/init.d/symphoniad stop
   # cd /software/tmpRepo
   # sh support/installIntegratedSimplex.sh addLang
   mediaserver_announcements en_za,de,es
   ```

   Note: This language is used for the media server announcements provided for the PBX.

   If you were able to install all language packages, then proceed with step 5 on page 309, otherwise continue with step 4 on page 308.

4. If the language is not available then the 'Repository' and required language ISO files will have to be staged for installation. See Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341 for details of this procedure.

   Attention: It is recommended the installation repository be created with the 'Base', 'Repository' and the additional language package ISOs that are required. Please include the English language package ISO in the installation repository. These files would be found in the initial build package for the current Applications version. Example given; If the Applications server is at the V10 FR0 H1 (BUILD 12 H1) level, the required ISO files will be in the

repository for V10FR0 (BUILD 12). Following this convention will ensure all packages are available in case dependencies are not met during a language package install.

Note: Providing an ISO file as repository retrospectively deletes the provision of the current repository. Install all required RPMs from the repository to be deleted before removing it.

The language package can be installed (after establishing the repository) with the same syntax demonstrated in step 3 on page 308 of this procedure. Remember to stop the symphoniad before adding a new package.

```
support/installIntegratedSimplex.sh addLang {LANGUAGE_PKG}
```

5. Start the Applications server;

   Command example:

   `# /etc/init.d/symphoniad start`

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

6. Check NSS service status by executing:

   ```
   /etc/init.d/NSSservice status
   ```

   NSSserver is running

   - NSSservice.service - LSB: Speech Server

   Loaded: loaded (/etc/init.d/NSSservice; bad; vendor preset: disabled)

   Active: active (exited) since Thu 2021-12-02 11:41:51 EET; 4 days ago

   Docs: man:systemd-sysv-generator(8)

Process: 15587 ExecStart=/etc/init.d/NSSservice start (code=exited, status=0/SUCCESS)

Main PID: 2585 (code=exited, status=0/SUCCESS)

Tasks: 0

CGroup: /system.slice/NSSservice.service

If the output is similar to the above then there is nothing else to do. In any other case please execute:

```
support/nss_start.sh
```

Note: The script can be found under the support directory of the UC ISO file.

7. If the update process is complete, the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.2.3.5 Update/Upgrade of Integrated Applications

We differentiate between updating and upgrading as follows:

- Update

  An update is performed when a new fix release or hotfix is available for an installed version of the OpenScape Applications (within the same release). This chapter describes the fix release/ build update.

  Example:

  An OpenScape Application V10 R0 was installed in version FR1 (Fix Release 1). A V10 R0 FR2 or FR2 HF1 is released as an update.

  Note: The hotfix update is described in Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”

- Upgrade

  Examples:

a) If an OpenScape Application V10R6 is installed and a V11R1 Applications setup medium is to be used, we refer to this as an “upgrade” to V11.

b) If an OpenScape UC Application V10R6 has been installed and an OpenScape UC Application V11 setup medium is to be used for updating the OpenScape UC Application, we refer to this as an upgrade.

Note: For the integrated Simplex OpenScape Voice deployment, the Applications upgrade is included in the integrated OpenScape Voice server's upgrade or migration process. Refer to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11” for details.

Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

Execute the following steps on the OpenScape Voice server as the root user.

1. Create a backup. The Information regarding Integrated OpenScape Voice system backups can be found in the “OpenScape *Voice 11 Service Manual, Service Documentation”*. Another backup option is to synchronize the OpenScape Voice partitions.
2. If Openfire, external or internal, is installed, stop it by executing the following command:

   ```
   # /etc/init.d/openfire stop
   ```

3. Stop OpenScape UC Applications (stop symphonia).

   ```
   # /etc/init.d/symphoniad stop
   ```

4. Prepare the Update Medium of the Integrated Simplex.

   To prepare the integrated environment for the Update, please execute steps 5-7 from section Section 5.2.10.4, “Finish the Installation Medium Setup”.

5. Start the update of the applications.

   Note: In the commands below, the path "/software/tmpREPO" is taken from the command examples provided in Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349, step 6 on page 352.

   Command examples;

   ```
   # cd /software/tmpREPO
   # osc-setup up osc-setup
   # sh support/installIntegratedSimplex.sh update
   ```

The update process is fully automatic and, since no configuration files will be overwritten, you need not back up the configuration files before the update.

Note: If hotfixes are required, proceed to Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313. If hotfixes are not required, complete steps 7 and 9.

---

6. Reconfigure the web client in an integrated simplex.

   Command example;

   #/enterprise/HiPathCA/bin/reconfiguration.sh

7. After the successful update, start the OpenScape UC Application by executing the following commands:

   # /etc/init.d/symphoniad start

   # /etc/init.d/openfire start

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   # tailf /log/osgi.log

   For External (offboard) applications servers;
   # tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

Warning: Once the update/upgrade completes successfully, it is noted that the active partition contains the latest fixes to a number of issues of the previous state of the system (e.g. bugs, vulnerabilities etc.), but the fallback partition still contains these issues. Therefore, and in order to eliminate any possibility of activating that fallback partition by mistake, it is strongly recommended to synchronize the active partition to the fallback one immediately after the successful update/upgrade or as close to it as possible.

Questions should be addressed to your next level of support.

8. Check NSS service status by executing:

   `/etc/init.d/NSSservice status`

NSSserver is running.

- NSSservice.service - LSB: Speech Server

Loaded: loaded (/etc/init.d/NSSservice; bad; vendor preset: disabled)

Active: active (exited) since Thu 2021-12-02 11:41:51 EET; 4 days ago

Docs: man:systemd-sysv-generator(8)

Process: 15587 ExecStart=/etc/init.d/NSSservice start (code=exited, status=0/SUCCESS)

Main PID: 2585 (code=exited, status=0/SUCCESS)

Tasks: 0

CGroup: /system.slice/NSSservice.service

If the output is similar to the above then there is nothing else to do. In any other case please execute:

```
support/nss_start.sh
```

Note: The script can be found under the support directory of the UC ISO file.

9. If the update process is complete the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.2.3.6 Installing a HotFix - Integrated Apps server

Information regarding Integrated OpenScape Voice system backups can be found in the "OpenScape Voice V11 Service Manual, Service Documentation".

Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

To provide the set-up medium from ISO files downloaded to the Applications server, refer to Section 5.2.10.1, “Create Setup medium from ISO files on the server hard disk”, on page 343, step 1 on page 343. After step 1 is completed a doclink back to this section will be available.

To provide the set-up medium from ISO files on a USB refer to Section 5.2.10.2, “Create Setup medium from ISO files on a USB media”, on page 345 steps 1 on page 345 through 5. After the indicated steps are completed a doclink back to this section will be available.

To provide the set-up medium from ISO files on a USB refer to Section 5.2.10.3, “Create Setup medium from ISO files on a CD/DVD media”, on page 347, steps 1 on page 348 and 2 on page 348. After the indicated steps are completed a doclink back to this section will be available.

Questions should be addressed to your next level of support.

For the purposes of this example, the procedure employs an ISO file downloaded to the server.

1. Transfer the ISO file to the server. In this example the ISO is transferred to `/software`.
2. Stop the Applications Symphonia and Openfire, external or internal, if they are installed.

   Command example;

   ```
   #> /etc/init.d/symphoniad stop
   ```

   ```
   # /etc/init.d/openfire stop
   ```
3. If you have not already done so, mount the ISO file.

   `mount -o loop <ISO file including the path> /<mount_point>`

   Command examples;

   For the ISO medium on the server hard disk case;

   ```
   #> mount -o loop /software/OpenScapeUcSuiteApps_PATCH-
   V10.0.0-100002.iso /mnt
   ```

   For the ISO medium on the USB case;

   ```
   # mount /dev/sdf1 /media
   ```

   For the ISO medium on the CD/DVD media case;

   ```
   # mount /dev/sr0 /media/
   ```
4. Change directory to the mounted ISO.

   Command examples;

   For the ISO medium on the server hard disk case example;

   ```
   #> cd /mnt
   ```

   For the ISO medium on the USB and CD/DVD case examples;

   ```
   # cd /media
   ```
5. Running the update script.

   ```
   # bash support/installIntegratedSimplex.sh update
   ```

Run the update script

Command example;

```
#> bash updateIntegratedSimplex.sh
```

Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

---

6. Reconfigure the web client in an integrated simplex.

   Command example;

   ```
   #/enterprise/HiPathCA/bin/reconfiguration.sh
   ```

7. Start the Applications.

   Command example;

   ```
   #/etc/init.d/openfire start
   ```

   ```
   #/etc/init.d/symphoniad start
   ```

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

8. After a successful HotFix install the system should be cleaned of the installation medium. First exit the setup medium path.

   Command example;

   ```
   #> cd /
   ```

9. Next, unmount the HotFix ISO.

   Command example;

   ```
   #> umount /mnt
   ```

10. Remove the ISO file.

    Command example;

    ```
    # rm /software/OpenScapeUcSuiteApps_PATCH-V10.0.0-100002.iso
    ```

5.2.3.7 Special Instructions: How to upgrade OSV Integrated Simplex to an OSV Image with OpenScape Applications lower than the already installed

On an Integrated Simplex, the Applications are installed as part of the OpenScape Voice Image installation.

The instructions below refer to the case where the OpenScape Applications on the Integrated Simplex are upgraded to a greater version than the one that is part of the installed OpenScape Voice Image, and then the Integrated Simplex is desired to be upgraded to a higher OpenScape Voice Image, containing lower version of the already installed OpenScape Applications.

Example:

1. OpenScape Voice Integrated Simplex is installed with OpenScape Voice Image V11_R0_8.0_UCV10R6_IMG, with integrated OpenScape Applications V10 R6.14.0
2. The OpenScape Applications are upgrated to OpenScape Applications V11 R1.1.0
3. Then, the Intregrated Simplex is desired to be upgraded to OpenScape Voice Image V11_R0_9.0_UCV10R6_IMG, which contains the OpenScape Applications V10 R6.16.0

To maintain the configuration performed at step 2, the following procedure has to be followed:

1. Export system's configuration data. The relevant information can be found in the “OpenScape Voice V11 Service Manual, Service Documentation”, chapter 4 of the current document.
2. Perform the installation of the desired OpenScape Voice Image. The relevant information can be found in chapter 4.
3. Upgrade the OpenScape Applications again to the desired version.
4. Import the system's configuration. The relevant information can be found in the “OpenScape Voice V11 Service Manual, Service Documentation”, chapter 4.

5.2.4 Updating using the CMP (UI Patching) instead of osc-setup

5.2.4.1 General Considerations

Apache Web Server certificates have a period validity of 1001 days.
This can cause an error to the functionality of UI Patching resulting in loss of connectivity between nodes.

The error encountered when executing prepareUpdate.sh is the following:

```
curl: (60) SSL certificate problem, verify that the CA cert
is OK. Details:
error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
failed
More details here: http://curl.haxx.se/docs/sslcerts.html
```

As a solution for this problem and if the certifcates contained under `/etc/apache2/ssl.crt/` are more than 1001 days old the following steps should be followed:

1. Execute `/<SYMPHONIA_HOME>/servicetools/install/bin/reconfigure_apache_certificates.sh firstinstall`
2. Execute `/<SYMPHONIA_HOME>/servicetools/install/bin/prepareUpdate.sh` again

Attention: <SYMPHONIA_HOME> is either /opt/siemens or /enterprise depending on your deployment.

Attention: When you must use UI patching for the first time, then you must run the following script:
`/enterprise/servicetools/install/bin/prepareUpdate.sh`

Attention: Perform the UI Patching process as described below.

Note: <SYMPHONIA_HOME> is either /opt/siemens or /enterprise depending on your deployment.

The deployment scenarios that are covered by this documentation and that are supported by updating via the CMP (UI Patching) are the following:

- Integrated Deployment
- Small Deployment
- Large Deployment
- Very Large Deployment

Attention: Updating using the CMP (UI patching) is only supported for an OpenScape UC Application update but not for an upgrade.

Instead of updating the OpenScape UC Application by using the actual `osc-setup up` command in a command line in *OpenScape UC Application, Installation and Upgrade, Installation Guide, "*Updating to a new Fix Release" or "Installing a Hotfix" you can update it by clicking on buttons in the CMP (UI Patching). This reduces the number of steps to be executed for Large Deployment and Very Large Deployment considerably, because only actions are performed manually on the application computer but not the actual update steps on the frontend computers and media server computers.

The feature “update via CMP (UI Patching)” is always included in the OpenScape Voice setup but disabled by default. It must be activated by executing the `prepareUpdate.sh` script (see below).

Note: You find further details of updating in the CMP in the administrator documentation *OpenScape Common Management Platform, Administration*.

5.2.4.2 Procedure

This section describes the installation of a minor release and a HF.

Note: The following procedure covers updates from a minor release to a newer minor release and hotfix in one step (see example 1) or a hotfix of the same release (see example 2).
Example 1: Update from OpenScape UC Application V9R2 HF0 to V9R3 HF1
Example 2: Update from OpenScape UC Application V9R2 HF9 to V9R2 HF10

In this section, perform all command invocations in command lines on the application computer.

1. Ensure that the instructions given in *OpenScape UC Application V10, Installation and Upgrade*, chapter **Update and Upgrade Preparations** have been carried out.

If an HTTP proxy is configured for the application computer, the frontend computers, the media server computers and for other computers, these settings must be restricted to such an extent that the application computer, the frontend computers and the media server computers do not use an HTTP proxy when communicating with each other. To do this, execute either step 2 on page 319 (use of YaST) or step 3 on page 319 (editing the `/etc/sysconfig/proxy` file).

2. Execute the following sub-steps:

   a) Execute the `yast` command.

   b) Open the **Network Services** > **Proxy**.

   c) Add the fully qualified domain names of the application computer, the frontend computers and the media server computers in the `No Proxy Domains` field.

Note: You receive the FQDN of a computer by executing the `hostname -f` command on this computer.

---

   d) Select **Finish**.

   e) Select **Quit**.

   f) Continue with step 4 on page 319.

3. Execute the following sub-steps:

   a) Open the `/etc/sysconfig/proxy` file in an editor, for example:

   ```
   vi /etc/sysconfig/proxy
   ```

   b) Add the fully qualified domain names (FQDN) of the application computer, the frontend computers and the media server computers to the value of the `NO_PROXY` parameter.

Note: You receive the FQDN of a computer by executing the `hostname -f` command on this computer.

---

   c) Save the `/etc/sysconfig/proxy` file.

   d) Continue with step 4 on page 319.

4. Open **Maintenance** > **Inventory** > **Nodes & Applications** > **Applications** > **OpenScape UC** in the CMP. Click on the small triangle to the right of **OpenScape UC** and select **Software activation...**.

   The feature “update via CMP (UI patching)” is not yet activated.

```
This feature is not yet activated.
```

Note: See the administrator documentation *OpenScape Common Management Platform Administration* for details about the software activation.

5. Log on with user name `root` in a command line on the application computer.
6. Perform the activation:

   ```
   bash /opt/siemens/servicetools/install/bin/prepareUpdate.sh
   ```

   Example output:

```
2012/03/28-19:52:33 # INFO = ##################### EXECUTION OF /opt/siemens/
servicetools/install/bin/prepareUpdate.sh STARTS ####################
2012/03/28-19:52:33 # INFO = Reading deployment from response file
2012/03/28-19:52:33 # INFO = Deployment StandardDuplexSmall is supported, continue...
2012/03/28-19:52:33 # INFO = Local path to installation media is not specified, skip
YUM repository setup
2012/03/28-19:52:33 # INFO = Reading backend node (BE) info: 10.235.200.23
2012/03/28-19:52:33 # INFO = No frontend nodes (FE) found
2012/03/28-19:52:33 # INFO = No media server nodes (MS) found
2012/03/28-19:52:33 # INFO = Checking for YUM repositories...
2012/03/28-19:52:33 # INFO = OSC Update repository does not exist, create directory /
OSCupdate.
2012/03/28-19:52:33 # INFO = OSC Base repository does not exist, create directory /
OSbase.
2012/03/28-19:52:33 # INFO = Feature is not activated (prepare run for first time or
last run was unsuccessful)
2012/03/28-19:52:33 # INFO = Checking if trusted ssl connections already exist...
2012/03/28-19:52:33 # INFO = Only BE node found, no FE/MS to check trusted connections
2012/03/28-19:52:33 # INFO = Allo 'sym' user run updateAllNodes.sh script as 'root'
user
2012/03/28-19:52:33 # INFO = Http configuration file created to setup base/update
repositories
2012/03/28-19:52:33 # INFO = Http configurations applied successfully
2012/03/28-19:52:33 # INFO = HTTP access to /OSCbase repository verified
2012/03/28-19:52:33 # INFO = HTTP access to /OSCupdate repository verified
2012/03/28-19:52:33 # INFO = Feature installed successfully, create lock file to mark
activation
2012/03/28-19:52:33 # INFO = ##################### EXECUTION OF /opt/siemens/
servicetools/install/bin/prepareUpdate.sh ENDED SUCCESSFULLY ####################
```

   You can check the `/var/siemens/common/log/install/uipatching/prepareUpdate.log` file for more details.

7. If you use syncUC as fallback solution (see *OpenScape UC Application V10, Installation and Upgrade*, chapter **Preparing to the syncUC Fallback**), we recommend activating the check box **Synchronize Active to Passive partitions** in the **Synchronize** section of the CMP. When you do this, the active partition is automatically copied to the passive partition before the update to be prepared for a fallback.

8. Both minor releases and hotfixes are provided through ISO files.

   Example:

   HF:

   `OpenScapeUcSuiteApps_PATCH-<version>.iso`

   Minor Release:

   `OpenScapeUcSuiteApps-Repository-<version>.iso`

   Administrators can either update to a minor release or hotfix by providing the absolute path of the ISO file into the field "Path"

   For example

   HF update

   `/mnt/DVD_iso/HP8K_V10_R2/OpenScapeUcSuiteApps_PATCH-V10R2.0.5-030005.iso`

   For example

   Minor release update V9R1->V9R2

   `/mnt/DVD_iso/HP8K_V9_R2/Build_3/OpenScapeUcSuiteApps-Repository-V9R2.0.0-030000.iso`

   Administrators can also perform a direct (one step) update to a hotfix and minor release by providing the repository ISO "of the minor release" in the "Build Path" and the HF ISO in the "Hotfix Path".

   For example

   Build Path:

   `/mnt/DVD_iso/HP8K_V9_R2/Build_3/OpenScapeUcSuiteApps-Repository-V9R2.0.0-030000.iso`

   Hotfix Path:

   `/mnt/DVD_iso/HP8K_V9_R2/OpenScapeUcSuiteApps_PATCH-V9R2.0.5-030005.iso`

   Note: Mount the ISO file according to the following example:

```
mount -o loop <path>/OpenScapeUcSuiteApps-PATCH-<version>.iso /mnt
```

IMPORTANT: Only USB sticks that are formatted with a file system that is natively supported by SLES (ext3, ext2, FAT32, reiserfs etc.) are supported. All ISO installation files are smaller than 4 GB and can thus be processed by FAT32.

a) List all sd devices:

`ls /dev/sd*`

Example output:

`/dev/sda /dev/sda1 /dev/sda2 /dev/sda3`

b) Connect the USB stick to the computer.

c) List all sd devices once again:

`ls /dev/sd*`

Example output:

`/dev/sda /dev/sda1 /dev/sda2 /dev/sda3 /dev/sdf /dev/sdf1`

The connected USB stick makes the difference between the two outputs. In this example it is a USB stick (sdf) with one partition (sdf1). If the USB stick had several partitions, sdf2, sdf3 etc. would also be put out.

You can also use the `fdisk -l` command. If a device is connected to the USB interface, the line `/dev/sdxx` of this command's output shows the connected USB device.

d) If the `/media` directory does not exist yet, create it:

`mkdir /media`

e) Mount the USB stick.

Example:

`mount /dev/sdf1 /media`

f) If the `/mnt` directory does not exist yet, create it:

`mkdir /mnt`

9. Click on **Start** in the CMP.
10. Click on the **OK** button.

    IMPORTANT: Your CMP session is closed. All components of the OpenScape UC Application on the application computer and - if available - on the frontend and media server computers are shut down.

11. Enter the following command in a command line on the application computer:

`tailf /var/siemens/common/log/install/uipatching/updateAllNodes.log`

    The last lines of this log file are always displayed.

12. Wait for the following message that indicates the successful update:

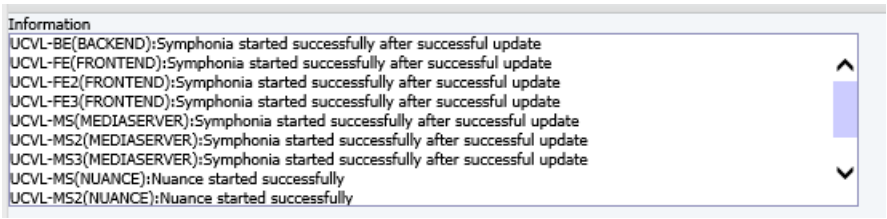
```
...Execution of script /opt/siemens/servicetools/install/bin/updateAllNodes.sh ended
(exit code 0)
```

Warning: Once the update/upgrade completes successfully, it is noted that the active partition contains the latest fixes to a number of issues of the previous state of the system (e.g. bugs, vulnerabilities etc.), but the fallback partition still contains these issues. Therefore, and in order to eliminate any possibility of activating that fallback partition by mistake, it is strongly recommended to synchronize the active partition to the fallback one immediately after the successful update/upgrade or as close to it as possible.

13. Remove the repository in osc-setup by entering the following command in a command line on the application computer:

    ```
    osc-setup cr -clean
    ```

14. After a login, the CMP indicates the successful performance.



5.2.5 Installation/Update Instructions for Media Server Standalone

Attention: If an Applications Installation, Update or Upgrade failure should occur, and there are any questions regarding the Applications server(s) status or recovery, contact your next level of support for assistance.

Attention: An external (offboard) CMP has a Survival Authority component that is included as part of the CMP Applications software installation. The Standalone Survival Authority snmpreceiver rpm **IS NOT** intended for installation on a CMP. Installation of the Standalone Survival Authority rpm on a CMP will negatively impact the CMP snmpreceiver functionality.

The SNMPReciever should only be installed in the case of a Standalone Survival Authority as described in **Section 5.3, “Starting and Stopping the OpenScape Applications”, on page 370**.

Attention: Refer to the OpenScape Applications release notes for the latest updates to the OpenScape Applications. Carefully review the Installation Prerequisites section of the OpenScape Applications release note for any activities that might be required before creating the response files.

Attention: For offboard (external) Applications servers the OpenScape UC Application components are installed by osc-setup (NOT zypper or yast). Only use zypper or yast to install the osc-setup RPM package.

For media server announcement and treatments, refer to *OpenScape Voice V11 Administration, Administrator Documentation*, the section titled *Media Services.*

For media server hardware requirements, refer to *OpenScape Media Server Vx Administrator Documentation* (where *x is the software release version*).

For Prefix Access Code (PAC) information, refer to Section 14.2, “How to Add/Delete Default PACs for Vertical Services”, on page 598.

A Standalone Media Server deployment which can be installed for a Joint Interoperability Test Command (JITC) solution is available. An additional parameter must be added into a knut.responsefile to activate the MediaServerStandalone deployment.

The parameter is: `SI_MEDIASERVER_MODE=mgcponly`

Add the parameter manually at the end of the knut.responsefile file MediaServerStandalone scenario deployment.

This will automatically remove some unnecessary providers, for example SIP, CTI and MS Tomcat from the MediaServerStandalone deployment.

After the MediaServerStandalone installation has ended, run the related hardening scripts manually on the server. Follow the steps below:

1. Go to: cd /opt/siemens/mediaserver/application_host/tools/
2. unzip hardening.zip
3. cd hardening

```
4. chmod -R a+x *
5. sh execute.sh
```

6. reboot the MediaServerStandalone server

Note: After applying manually the hardening scripts, you can login remotely using the putty tool with the credentials:
username = sysad
password = 1clENtk=

If needed later, you can change to 'root' user with the following credentials:
$ sudo su
default password for root user is: T@R63dis

You can also login via the console of the physical/virtual server itself with the credentials:
username = root
password = T@R63dis

5.2.5.1 Prepare the Installation Medium of a Standalone Media Server

To prepare the Standalone Media Server environment for the installation, please refer to Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341.

Section 5.2.10 will guide you through the preparation of the media for installation. At the end of Section 5.2.10 a link back to Section 5.2.5.2, “Response File for Media Server Standalone deployments”, on page 325 is provided.

5.2.5.2 Response File for Media Server Standalone deployments

---

Note: Before creating response files, ensure that the customer administrator or representative has provided you with the necessary configuration data.

Execute the following steps to create a response file for the application computer.

All commands should be executed as the user *root*.

1. Change directory to the installation repository created in step 6 on page 352 of Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349 and then copy the appropriate response file to the /root path. In the examples of this guide the path was "/software/tmpREPO"

   ```
   # cd /software/tmpREPO
   ```

```
# cp templates/
knut.responsefile.txt.templ_MediaServerStandalone /root/
knut.responsefile.txt
```

Attention: Copy the file as specified to the directory named /root but not to the Root directory /.

2. Open the response file with an editor (for example with vi):

   `vi /root/knut.responsefile.txt`

3. Look for the following line:

   `SI_SYMPHONIA_ADMIN_PASSWORD=<PLACEHOLDER_symphonia_admin_password>`

   Replace `<PLACEHOLDER_symphonia_admin_password>` with the password of the Symphonia administrator.

Note: This password must comply with the security policies, which are defaulted as follows:
- At least 8 characters
- At least one special character
- At least one number
- At least one capital letter
- Not more than 3 identical characters in a row

4. Look for the following line:

   `SI_COMMUNITY_NAME=<PLACEHOLDER_community_name>`

   Replace `<PLACEHOLDER_community_name>` with the community name.

Attention: The Community has nothing to do with SNMP.
Capital letters, small letters and underscore are permitted. The latter must not appear at the beginning or end of the name. The corresponding regular expression reads as follows: `[A-Za-Z0-9][A-Za-Z0-9_]*[A-Za-Z0-9]`

Note: To avoid login issues with UC WebClient when OSV and UC systems co-exist in a solution (non integrated simplex), you have to configure a different `SI_COMMUNITY_NAME` for OpenScape Voice Media Server StandAlone and UC Media Server StandAlone.

5. Look for the following line:

   `SI_PRIMARY_NODE_HOST=<PLACEHOLDER_hostname>`

   Replace `<PLACEHOLDER_hostname>` with the fully qualified domain name (FQDN) or the IP address of the Media server Standalone. We recommend using the FQDN.

6. Look for the following line:
   `SI_LOCAL_HOST=<PLACEHOLDER_hostname>`
   Replace `<PLACEHOLDER_hostname>` with the fully qualified domain name (FQDN) or the IP address of the Media server Standalone. We recommend using the FQDN.
7. Look for the following line:
   `SI_DB_HOST=<PLACEHOLDER_hostname>`
   Replace `<PLACEHOLDER_hostname>` with the fully qualified domain name (FQDN) or the IP address of the Media server Standalone. We recommend using the FQDN.
8. Look for the following line:
   `SI_DB_LOGON_PASSWORD=<PLACEHOLDER_dbms_dba_password>`
   Replace `<PLACEHOLDER_dbms_dba_password>` with the password of the Solid database administrator. It must not be the default password (`dba`). Employ a secret, complex string of characters for the database password.
9. If the response file is created for an upgrade scenario, in which the applications database has to be migrated from an older release to a new release, proceed as follows:
   a) Look for the following line:
      `SI_FW_DB_MIGRATION=false`
   b) Set the migration flag to "true":
      `SI_FW_DB_MIGRATION=true`
10. Verify response file on the node. Change directory to the installation repository and run the checkResponsefileOnLocalNode.sh script. For our example case;
    ```
    # cd /software/tmpREPO
    # sh support/checkResponsefileOnLocalNode.sh
    ```
11. Ensure that the response file is saved and kept in a safe location. The response file is not currently contained in the system backup sets, but it is needed to rebuild the system during a crash recovery.

Note: The restore mechanism uses the database administrator password from the original system, where the backup was taken, to access the Solid database. If this password is not known, no recovery is possible. This password is defined in the response file and that is why the created response file must be backed up in a safe location.

5.2.5.3 Installing Media Server Standalone

Information regarding Offboard (external) Apps servers backups can be found in;

- *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section "Installing and Configuring the Computer and Operating System"*.
- *OpenScape UC Application V10 Configuration and Administration.*

The syncUC script can be used for backing up the current version of Applications to a 'passive' or Fallback partition of your server hard drive. For more information regarding syncUC, refer to Section 5.2.16, "syncUC", on page 365.

Attention: When using syncUC with the "Multiple Communication Admin Server" or "Media Server Standalone" Applications deployments; the recommended disk sizing is 2 x 300GB in RAID-1 configuration.

By default, the installation only includes the English language. **It is necessary to install any other language packages after the installation.** If your installation requires additional languages please refer to **Section 5.2.5.4, "Adding Additional Packages/Languages", on page 330.**

1. From the installation repository, execute the following commands to install the Applications on the server.

   These commands should be executed as the user *root*.

   Note: The path "/software/tmpREPO" is taken from the command examples provided in **Section 5.2.10.4, "Finish the Installation Medium Setup", on page 349, step 6 on page 352.**

   Command examples;

   ```
   # cd /software/tmpREPO
   # osc-setup in OpenScapeUC_MediaServerStandalone
   ```

2. In case of an error, always select the option "**despite the inferior architecture**". Example given:

   ```
   Problem: OpenScapeUC_Large_MS-6.0_1.0.0-007.noarch requires
   OpenScapeUC_Large_MS, but this requirement cannot be provided

   uninstallable providers: OpenScapeUC_Small-6.0_1.0.0-
   007.noarch[270fc4d9389754e36bb4dbe2a725408d]

   Solution 1: Following actions will be done:

      install symphonia-6.0_1.5.0-058.i586 despite the inferior
      architecture
      install symphonia-jre-ibm-6.0.9.2-4.i386 despite the
      inferior architecture
   ```

```
Solution 2: do not install OpenScapeUC_Large_MS-6.0_1.0.0-
007.noarch

Solution 3: break OpenScapeUC_StandardDuplexSmall by ignoring
some of its dependencies

Choose from above solutions by number or cancel [1/2/3/c]
(c):
```

3. Type **1** and press **Enter**.
4. When the '**Continue**' prompt is presented push the '**y**' key and then the return key. Example given;

```
72 packages to upgrade.

Overall download size: 724.7 MiB. After the operation, 17.7
MiB will be freed.

Continue? [y/n/?] (y): y
```

Note: The typical installation takes approximately one hour.

5. Check for any newer Applications patch sets or HotFixes and install them according to the corresponding release notes (if applicable).

Attention: If more packages are required for your install (i.e.; languages besides English), do not execute step 7 until **Section 5.2.5.4, "Adding Additional Packages/Languages", on page 330** is reviewed.

6. Start the OpenScape Applications;

```
# /etc/init.d/symphoniad start
```

The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

For integrated applications servers;
tailf /log/osgi.log

For External (offboard) applications servers;
tailf /var/siemens/common/log/osgi.log

Monitor the file osgi.log for the services startup sequence. When the osgi.log

file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

Press **'ctrl+c'** to exit the tail function.

Questions should be addressed to your next level of support.

7. If the installation process is complete the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.2.5.4 Adding Additional Packages/Languages

Please refer to Section 5.2.15, “Adding Additional Packages/Languages - Offboard (External) Apps Server”, on page 362.

5.2.5.5 Update Media Server StandAlone

Please refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356.

5.2.5.6 Installing a HotFix - Media Server StandAlone

Please refer to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359.

5.2.5.7 Uninstall the Media Server Applications

Currently there is no generally available method to remove the External Applications Server (OffBoard) Applications.

If the removal of the Applications is necessary please contact your next level of support.

5.2.6 Installation/Update Instructions for Multiple Communications Server Admin deployment

---

Attention: If an Applications Installation, Update or Upgrade failure should occur, and there are any questions regarding the Applications server(s) status or recovery, contact your next level of support for assistance.

The Multiple Communications Server Admin Applications deployment can administer 10 OpenScape Voice systems. **An snmpreceiver installed with the applications server software allows this deployment to act as a Survival Authority for the monitored OSV systems.** For more Survival Authority details, refer to Section 6.4, “Survival Authority on the CMP”, on page 392.

The Multiple Communications Server Admin deployment does not support UC services/features. Standard Duplex Large or Small Applications server deployments do support UC services/features.

Attention: An external (offboard) CMP has a Survival Authority component that is included as part of the CMP Applications software installation. The Standalone Survival Authority snmpreceiver rpm **IS NOT** intended for installation on a CMP. Installation of the Standalone Survival Authority rpm on a CMP will negatively impact the CMP snmpreceiver functionality.

The SNMPReciever should only be installed in the case of a Standalone Survival Authority as described in Section 6.5, “Installing a Standalone Survival Authority”, on page 395.

Attention: Refer to the OpenScape Applications release notes for the latest updates to the OpenScape Applications. Carefully review the Installation Prerequisites section of the OpenScape Applications release note for any activities that might be required before creating the response files.

Attention: For offboard (external) Applications servers the OpenScape UC Application components are installed by osc-setup (NOT zypper or yast). Only use zypper or yast to install the osc-setup RPM package.

A new MCSA Secure deployment is available which can be installed for Joint Interoperability Test Command (JITC) solution. The Multiple Communications Server Admin Secure deployment delivers the OSV Assistant tool. Related MediaServer / UC functionality is not supported/delivered with this deployment.

Note: During Multiple Communications Server Admin Secure deployment installation, the related hardening scripts run automatically on the server during the installation job (at the end).

You can remotely login using the putty tool with the credentials;
username = sysad
password = 1clENtk=

If needed later, you can change to 'root' user with
$ sudo su
default password for root user is: T@R63dis

One can login also via the physical/virtual server itself console with the credentials:
username = root
password = T@R63dis

5.2.6.1 Providing a Server Standalone Setup Medium

To prepare the Multiple Communications Server environment for the installation please refer to Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341.

Section 5.2.10 will guide you through the preparation of the media for installation. At the end of Section 5.2.10 a link back to Section 5.2.6.2, “Response File for Multiple Communication Server Administration deployments” is provided.

5.2.6.2 Response File for Multiple Communication Server Administration deployments

---

Note: Before creating response files, ensure that the customer administrator or representative has provided you with the necessary configuration data.

Execute the following steps to create a response file.

All commands should be executed as the user *root*.

1. Change directory to the installation repository created in step 6 on page 352 of Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349 and then copy the appropriate response file to the /root path. In the examples of this guide the path was "/software/tmpREPO"

   # cd /software/tmpREPO

   # cp templates/knut.responsefile.txt.templ_Multiple CommunicationServerAdmin /root/knut.responsefile.txt

   Attention: Copy the file as specified to the directory named /root but not to the Root directory /.

2. Open the response file with an editor (for example with vi):

   `vi /root/knut.responsefile.txt`

3. Look for the following line:

   `SI_SYMPHONIA_ADMIN_PASSWORD=<PLACEHOLDER_symphonia_admin_password>`

   Replace `<PLACEHOLDER_symphonia_admin_password>` with the password of the Symphonia administrator.

   Note: This password must comply with the security policies, which are defaulted as follows:
   - At least 8 characters
   - At least one special character
   - At least one number
   - At least one capital letter
   - Not more than 3 identical characters in a row

4. Look for the following line:

   `SI_COMMUNITY_NAME=<PLACEHOLDER_community_name>`

   Replace `<PLACEHOLDER_community_name>` with the community name.

   Attention: The Community has nothing to do with SNMP.
   Capital letters, small letters and underscore are permitted. The latter must not appear at the beginning or end of the name. The corresponding regular expression reads as follows: `[A-Za-Z0-9][A-Za-Z0-9_]*[A-Za-Z0-9]`

   Note: The value you assign to `SI_COMMUNITY_NAME` must be the same in all `knut.responsefile.txt` files on all computers (application, front-end and Media Server computers).

5. Look for the following line:

   `SI_PRIMARY_NODE_HOST=<PLACEHOLDER_hostname>`

Replace <PLACEHOLDER_hostname> with the fully qualified domain name (FQDN) or the IP address of the Multiple Communications Server. We recommend using the FQDN.

6. Look for the following line:
   `SI_LOCAL_HOST=<PLACEHOLDER_hostname>`
   Replace <PLACEHOLDER_hostname> with the fully qualified domain name (FQDN) or the IP address of the Multiple Communications Server. We recommend using the FQDN.
7. Look for the following line:
   `SI_DB_HOST=<PLACEHOLDER_hostname>`
   Replace <PLACEHOLDER_hostname> with the fully qualified domain name (FQDN) or the IP address of the Multiple Communications Server. We recommend using the FQDN.
8. Look for the following line:
   `SI_DB_LOGON_PASSWORD=<PLACEHOLDER_dbms_dba_password>`
   Replace `<PLACEHOLDER_dbms_dba_password>` with the password for the admin user "`dba`". It must not be the default password (dba). Employ a secret, complex string of characters for the database password.
9. If the response file is created for an upgrade scenario, in which the applications database has to be migrated from an older release to a new release, proceed as follows:
   a) Look for the following line:
      `SI_FW_DB_MIGRATION=false`
   b) Set the migration flag to "true":
      `SI_FW_DB_MIGRATION=true`
10. Verify response file on the node. Change directory to the installation repository and run the checkResponsefileOnLocalNode.sh script. For our example case;

    ```
    # cd /software/tmpREPO
    # sh support/checkResponsefileOnLocalNode.sh
    ```

11. Ensure that the response file is saved and kept in a safe location. The response file is not currently contained in the system backup sets, but it is needed to rebuild the system during a crash recovery.

Note: The restore mechanism uses the database administrator password from the original system, where the backup was taken, to access the Solid database. If this password is not known, no recovery is possible. This password is defined in the response file and that is why the created response file must be backed up in a safe location.

5.2.6.3 Installing Multiple Communications Server

Information regarding Offboard (external) Apps servers backups can be found in;

- *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide.*
- *OpenScape UC Application V10 Configuration and Administration.*

The syncUC script can be used for backing up the current version of Applications to a 'passive' or Fallback partition of your server hard drive. For more information regarding syncUC, refer to Section 5.2.16, “syncUC”, on page 365.

Attention: When using syncUC with the "Multiple Communication Admin Server" or "Media Server Standalone" Applications deployments; the recommended disk sizing is 2 x 300GB in RAID-1 configuration.

By default the installation only includes the English language. It is necessary to install any other language packages **after** the installation. If your installation requires additional languages please refer to Section 5.2.5.4, “Adding Additional Packages/Languages”, on page 330.

1. From the installation repository, execute the following commands to install the Applications on the server.

   These commands should be executed as the user *root*.

   Note: The path "/software/tmpREPO" is taken from the command examples provided in Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349, step 6 on page 352.

   Command examples;

   # cd /software/tmpREPO

   # osc-setup in OpenScapeUC_MultipleCommunicationServerAdmin

2. In case of an error, always select the option "**despite the inferior architecture**". Example given:

```
Problem: OpenScapeUC_Large_MS-6.0_1.0.0-007.noarch requires
OpenScapeUC_Large_MS, but this requirement cannot be provided
uninstallable providers: OpenScapeUC_Small-6.0_1.0.0-
007.noarch[270fc4d9389754e36bb4dbe2a725408d]

Solution 1: Following actions will be done:

      install symphonia-6.0_1.5.0-058.i586 despite the inferior
      architecture

      install symphonia-jre-ibm-6.0.9.2-4.i386 despite the
      inferior architecture

Solution 2: do not install OpenScapeUC_Large_MS-6.0_1.0.0-
007.noarch
```

```
Solution 3: break OpenScapeUC_StandardDuplexSmall by ignoring
some of its dependencies

Choose from above solutions by number or cancel [1/2/3/c] (c):
```

3. Type **1** and press **Enter**.
4. When the '**Continue**' prompt is presented select '**y**' and then the Enter/return key. Example given;

   ```
   72 packages to upgrade.

   Overall download size: 724.7 MiB. After the operation, 17.7
   MiB will be freed.

   Continue? [y/n/?] (y): y
   ```

   Note: The typical installation takes approximately one hour.

5. Check for any newer Applications patch sets or HotFixes and install them according to the corresponding release notes (if applicable).

Attention: If more packages are required for your install (i.e.; languages besides English) do not execute step 7 on page 337 until **Section 5.2.5.4, "Adding Additional Packages/Languages", on page 330** is reviewed.

6. Start the OpenScape Applications;

   ```
   # /etc/init.d/symphoniad start
   ```

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* **Start processing all bundles done.*** " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press '**ctrl+c**' to exit the tail function.

   Questions should be addressed to your next level of support.

7. If the installation process is complete the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.2.6.4 Adding Additional Packages/Languages

Please refer to Section 5.2.15, “Adding Additional Packages/Languages - Offboard (External) Apps Server”, on page 362.

5.2.6.5 Update Multiple Communications Server

Please refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356.

5.2.6.6 Installing a HotFix - Multiple Communications Server

Please refer to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359.

5.2.6.7 Remote Access for srx Account

Verify the OpenScape Voice servers' */etc/security/access.conf* file is configured to allow remote access for user *srx* from the External Applications server. Refer to Section 4.5.2, “Verify Remote Access for srx Account in a Standard Duplex”, on page 339" (a link back to this section is provided).

5.2.6.8 Survival Authority on the Multiple Communications Server Admin deployment

The snmpreceiver is installed with the applications server software in this deployment. This applications deployment **can also act as a Survival Authority for the monitored OSV systems.** For more details regarding the Survival Authority on a CMP, refer to Section 6.4, “Survival Authority on the CMP”, on page 392.

5.2.6.9 Uninstall the Multiple Communications Server Admin Applications

Currently there is no generally available method to remove the External Applications Server (OffBoard) Applications.

If the removal of the Applications is necessary please contact your next level of support.

5.2.7 Configuring the OSV Connectivity in CMP

Configure the CMP as follows:

1. Log in as administrator (provide the ADMIN_PASSWORD specified in the response file) to the CMP with the link:

   `https://<applications server IP address>/management`

2. On the CMP home page, select the **Configuration** tab, click **OpenScape Voice**, click the **General** icon, click **Switches**, and click **Add**. The Add Switch screen is displayed.

   Note: OpenScape Voice was formerly known as OpenScape Voice. References to HiPath 8000 in the following example are equivalent to OpenScape Voice.

   ---

3. On the Add Switch screen, place a check in the Use cluster name box, type the node1 IP address, type the *srx* password, and click **SAVE**.

   Note: If configuring UC applications proceed with step 4 other wise move onto Section 5.2.8, “Activating IPSec Between OpenScape Voice and the External Applications Server”, on page 339.

   ---

4. To configure bcom (CSTA) access to OpenScape Voice: Select the **Configuration** tab, click **Unified Communications,** click **Connections**, click **OS Voice**.

   The OpenScape Voice Switch Connections window is presented. Select the **Add** button.

   The Add OpenScape Voice Connection window is presented.

   a) Update/verify the OpenScape Voice parameters **Switch** and Version parameters (required).

   b) Update/Verify the CSTA access configuration IP Address and Port parameters (required).

   c) Update/Verify the BCOM configuration Node parameter (required).

   d) Update/Verify the SOAP access config configuration **IP Address** and **Port** parameters (required).

   e) Click the **SAVE** button.

f) If more CSTA server connections are required repeat 4a) through 4e), otherwise click **Close**.

5. Complete the office codes: Select the **Configuration** tab, click **Unified Communications**, click **Devices**, then **Office Codes**. The Office Codes window is presented. Under the "List of all Office Codes", select your Comm. System (OSV system) from the drop down list.

   A list of the imported office codes is displayed. Click an Office Code to edit it. An Edit Office Code dialog box is opened.

Note: OpenScape Voice was formerly known as HiPath 8000. References to HiPath 8000 in the following example are equivalent to OpenScape Voice.

---

6. This completes the OSV to CMP connectivity process. For more information on the OpenScape UC configuration refer to the “OpenScape *UC Application V10 Configuration and Administration, Administrator Documentation”*, section titled “*System Configuration”*. Review these three sections and then begin the UC configuration:

   - Configuration requirements - Not all requirements may be applicable to your system.
   - Overview of the Configuration process.
   - Configuration Checklist - Configuration of individual UC features are detailed. In this way the OpenScape UC environment can be customized to your needs.

5.2.8 Activating IPSec Between OpenScape Voice and the External Applications Server

Refer to Appendix 19, “IPSec Configuration” for the procedure to activate IPSec between OpenScape Voice and external Applications Server. The Appendix contains a link back to this page.

5.2.9 Configuring Billing Servers and Billing Clients

The billing records are stored on the OSV servers but they have to be deleted after a period of time due to limited disk space on the OSV servers. In general, customers prefer using external billing servers for storing the billing records rather than having them stored on the OSV servers. The OSV servers use "push" operation to transfer the billing records to the external billing servers. Alternatively, an external billing client uses a "pull" operation to transfer the billing records from the OSV servers to a billing server.

SFTP protocol (Secure FTP) is used for transferring billing records.

5.2.9.1 Configure Billing Servers

1. Login to CMP web page.
2. Navigate to **Configuration > OpenScape**
3. From the dropdown menu, select your OSV switch.
4. Click on **Administration** icon **> General Settings > CDR**
5. CDR Delivery Method: Push
6. FTP Control Port: 21
7. IP Address: Specify the IP Address of billing server.
8. Username: Specify SFTP user name of billing server.
9. Password: Specify SFTP password of billing server.
10. Confirm Password: Retype the same password of previous field.

If a backup billing server is used, specify the required information for the required fields similar to the above.

If there is only one billing server (no physical backup server), configure the backup server using the same values defined for the primary billing server.

Never leave the backup server undefined as this prevents the OSV server from being persistent in pushing billing records after a single transfer error.

Additionally, the external billing server has to be configured to allow the OSV servers to login using SFTP protocol to push the billing records onto the billing server. Refer to the external billing server's documentation for more information.

Note: Static routes for the billing server and the backup billing server are needed to transfer data over the billing subnet. The IFgui in Update mode can be used to add static routes without causing an OpenScape Voice server outage. For details refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. Alternatively, the ManageRoutes.pl (/etc/hiq8000/ManageRoutes.pl) script can be employed to Update (Add or Delete) static routes in the OpenScape Voice systems while the system is in state 2, 3 or 4. The script is node specific, meaning only updates to the OpenScape Voice configuration data and O/S route data on the current node will take place. On a cluster system the command should be repeated on the other node. As user *root*, enter this command from the OpenScape Voice server command line (the resulting output is quite extensive

and can be copied for future reference);

 # /etc/hiq8000/ManageRoutes.pl -info

5.2.9.2 Configure Billing Clients

1. Login to CMP web page.
2. Navigate to **Configuration > OpenScape**
3. From the dropdown menu, select your OSV switch.
4. Click on **Administration** icon **> General Settings > CDR**
5. CDR Delivery Method: Pull
6. PISN ID: Click on the **Generate PISN ID** button to generate a PISN ID.
7. IP Address: Specify the IP Address of billing client.

If a backup billing client is used, specify the required information for the required fields similar to the above.

Additionally, external billing clients such as OpenScape Accounting or OpenScape AM must be configured to use SFTP protocol to pull the billing records from the OSV servers using the "cdr" account's credentials as defined on the OSV system. Refer to the external billing client's documentation for more information.

Note: When the billing client sets up SFTP to pull billing records from the OSV server, it should specify the billing subnet IP address of the OSV node.

5.2.10 Providing a Setup Medium for the Applications

Attention: For offboard (external) Applications servers the OpenScape UC Application components are installed by osc-setup (**NOT zypper or yast**). Only use **zypper** or **yast** to install the **osc-setup** RPM package.

Attention: This text applies to **Applications installations only (new/fresh installation).**

Only the English language is installed by default for Standalone Media Server, Multiple Communication Server Administration and Integrated Simplex

deployments.

It is necessary to install any other language packages after the installation. If your installation requires additional languages, please refer to Section 5.2.5.4, “Adding Additional Packages/Languages”, on page 330.

It is recommended to download the additional languages that meet your site installation requirements when downloading the Applications ISOs (in step 1 of this procedure). This way the languages will already be available for update to the server after the Applications installation is complete.

Attention: This text applies to **Applications Updates and Upgrades only (updating a DVD/Build level within the same release (e.g., from Build 8 to Build 9)).**

It is a good practice to download any additional languages that meet your site installation requirements when downloading the Applications ISOs (in step 1 of this procedure).

These languages are **automatically** included as part of the Update (or Upgrade) process.

Prerequisite Software Packages for Standalone Media Server Installation

To ensure a successful installation of the Standalone Media Server on SLES 15, the following software packages must be installed prior to starting the application installation:

- `procmail`
- `libatomic1`
- `insserv-compat`
- `zip`
- `apache2`
- `glibc-32bit`
- `zlib-32bit`
- `iio-sensor-proxy`
- `gstreamer-plugins-base`
- `gstreamer-plugins-good`
- `libhyphen0`

- `libwebp7`
- `libQt5Core5`
- `libQt5Network5`
- `libQtQuick5`
- `libQt5Svg5`
- `libncurses5`
- `pciutils`

These packages must be installed using **zypper** or **yast** before executing the **osc-setup** installer.

Example:

```
zypper install procmail libatomic1 insserv-compat zip apache2
glibc-32bit \

zlib-32bit iio-sensor-proxy gstreamer-plugins-base gstreamer-
plugins-good \

libhyphen0 libwebp7 libQt5Core5 libQt5Network5 libQtQuick5
libQt5Svg5 \

libncurses5 pciutils
```

Providing a Setup Medium for the Applications: Chapter references

To provide the set-up medium from ISO files downloaded to the Applications server, refer to Section 5.2.10.1, “Create Setup medium from ISO files on the server hard disk”, on page 343.

To provide the set-up medium from ISO files on a USB refer to Section 5.2.10.2, “Create Setup medium from ISO files on a USB media”, on page 345.

To provide the set-up medium from ISO files on a CD/DVD media, refer to Section 5.2.10.3, “Create Setup medium from ISO files on a CD/DVD media”, on page 347.

5.2.10.1 Create Setup medium from ISO files on the server hard disk

1. As the root user, create a directory to store the ISOs needed for your installation. Typically this would be the BasePackage and Repository ISOs plus the language ISOs that meet your site installation requirements. The

path /software is used in the following examples because it has more than enough free space to handle the disk space requirements for the ISOs and installation repository.

Command example;

```
# mkdir /software/oscISOs
# cd /software/oscISOs
```

Note: If you are Installing a HotFix on an Integrated Apps server, follow this link back to Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313.

Note: If you are Installing a HotFix on an Offboard (External) Apps server, follow this link back to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359.

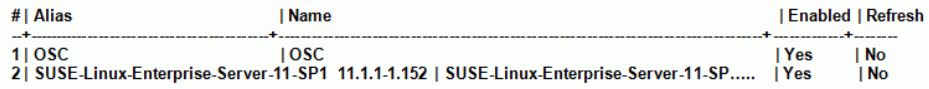
If neither of the preceding Notes apply then proceed to the next step.

2. Execute the zypper lr (list repository) command to check which sources have been provided in zypper:

   `zypper lr`

   Command example:

   # zypper lr



#	Alias	Name	Enabled	Refresh
1	OSC	OSC	Yes	No
2	SUSE-Linux-Enterprise-Server-11-SP1 11.1.1-1.152	SUSE-Linux-Enterprise-Server-11-SP.....	Yes	No

3. Verify that only the SLES setup medium is registered.
4. If further setup media are registered, remove them with the following command:

   `zypper rr <number>`

   <number> is the number you find in the first column of the zypper lr output.

   Command Example:

   # zypper rr 2

5. Execute the zypper lr (list repository) command to verify your changes are in effect;

   # zypper lr

6. After transferring the required ISOs to the directory (/software/oscISOs), use zypper 'add repository' (ar) to register the Repository ISO in the zypper Service list.

Command syntax;

zypper ar <URI> <Alias>

<URI>

Example of <URI> when using a local repository:

iso:/?iso=/<ISO file including path>

<Alias>

Attention: Replace <Alias> with a character string that does **not** end in DVD<number> (for example DVD1). If this string contains at least one blank, it must be enclosed by quotation marks.

Example of <Alias> : OSC

Command example;

 # zypper ar iso:/?iso=/software/oscISOs/OpenScapeUcSuiteApps-Repository-V10.0.0-060000.iso OSC

```
Adding repository 'OSC' [done]
Repository 'OSC' successfully added
Enabled: Yes
Autorefresh: No
URI: iso:///?iso=/software/oscISOs/OpenScapeUcSuiteApps-
Repository-V10.0.0-060000.iso
```

7. Go to Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349 to complete the installation medium setup.

5.2.10.2 Create Setup medium from ISO files on a USB media

Attention: Only FAT32-formatted USB sticks are natively supported by SLES 15. All ISO setup files are smaller than 4 GB and can thus be processed by FAT32.

If you wish to mount the Repository ISO file from a USB stick proceed as follows:

1. List all sd-devices:

   ls /dev/sd*

   Example output:

   /dev/sda /dev/sda1 /dev/sda2 /dev/sda3

2. Connect the USB stick to the computer.

3. List all sd-devices once again:

   ls /dev/sd*

Example output:

/dev/sda /dev/sda1 /dev/sda2 /dev/sda3 /dev/sdf /dev/sdf1

The connected USB stick makes the difference between the two outputs. In this example it is a USB stick (sdf) with one partition (sdf1). If the USB stick had several partitions, sdf2, sdf3 etc. would also be put out.

You can also use the **fdisk -l** command. If a device is connected to the USB interface, the line /dev/sdxx of this command's output shows the connected USB device.

4. If the /media directory does not exist yet, create it:

   Command example;

   # mkdir /media/

5. Mount the USB stick:

   Command example:

   # mount /dev/sdf1 /media

Note: If you are Installing a HotFix on an Integrated Apps server, follow this link back to Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313.

Note: If you are Installing a HotFix on an Offboard (External) Apps server follow, this link back to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359.

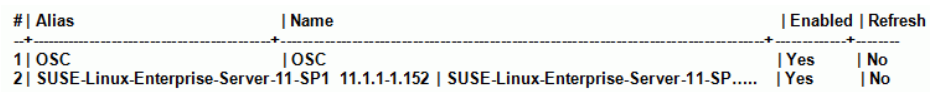
If neither of the preceding Notes apply then proceed to the next step.

6. Execute the zypper lr (list repository) command to check which sources have been provided in zypper:

   `zypper lr`

   Command example:

   # zypper lr



#	Alias	Name	Enabled	Refresh
1	OSC	OSC	Yes	No
2	SUSE-Linux-Enterprise-Server-11-SP1	11.1.1-1.152 | SUSE-Linux-Enterprise-Server-11-SP.....	Yes	No

7. Verify that only the SLES setup medium is registered.

8. If further setup media are registered, remove them with the following command:

   `zypper rr <number>`

<number> is the number you find in the first column of the zypper lr output.

Command Example:

```
# zypper rr 2
```

9. Execute the zypper lr (list repository) command to verify your changes are in effect;

   Command Example:

   ```
   # zypper lr
   ```

10. Now we are ready to use the zypper 'add repository' (ar) command to register the Repository ISO in the zypper Service list.

    Command syntax;

    ```
    zypper ar <URI> <Alias>
    ```

    <URI>

    Example of <URI> when using a local repository:

    iso:/?iso=/<ISO file including the path>

    <Alias>

    Attention: Replace <Alias> with a character string that does **not** end in DVD<number> (for example DVD1). If this string contains at least one blank, it must be enclosed by quotation marks.

    Example of <Alias>: OSC

    Command example;

    ```
    # zypper ar iso:/?iso=/media/OpenScapeUcSuiteApps-Repository-V10.0.0-060000.iso OSC
    Adding repository 'OSC' [done]
    Repository 'OSC' successfully added
    Enabled: Yes
    Autorefresh: No
    URI: iso:///?iso=/media/OpenScapeUcSuiteApps-Repository-V10.0.0-060000.iso
    ```

11. Go to Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349 to complete the installation medium setup.

5.2.10.3 Create Setup medium from ISO files on a CD/DVD media

After creating a CD/DVD drive with the ISO files required for you installation scenario proceed as follows:

1. If the /media directory does not exist yet, create it:

   Command example;

   # mkdir /media/

2. Mount the CD/DVD media

   Command example;

   root@bocast4a:[/dev] #
   # mount /dev/sr0 /media/
   mount: block device /dev/sr0 is write-protected, mounting read-only

   ---

   Note: If you are Installing a HotFix on an Integrated Apps server, follow this link back to Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313.

   Note: If you are Installing a HotFix on an Offboard (External) Apps server, follow this link back to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359.

   If neither of the preceding Notes apply then proceed to the next step.

3. Execute the zypper lr (list repository) command to check which sources have been provided in zypper:

   `zypper lr`

   Command example:

   # zypper lr

   ```
   # | Alias | Name | Enabled | Refresh
   --+-----------------------------------------------+---------
   1 | SUSE-Linux-Enterprise-Server-11-SP1 11.1.1-1.152 | SUSE-
   Linux-Enterprise-Server-11-SP111.1.1-1.152 | Yes | No
   ```

4. Verify that only the SLES setup medium is registered.

5. If further setup media are registered, remove them with the following command:

   `zypper rr <number>`

   <number> is the number you find in the first column of the zypper lr output.

   Command Example:

   # zypper rr 2

6. Execute the zypper lr (list repository) command to verify your changes are in effect;

   Command Example:

   # zypper lr

7. After transferring the required ISOs to the directory (/software/oscISOs), use zypper 'add repository' (ar) to register the Repository ISO in the zypper Service list.

   Command syntax;

   zypper ar <URI> <Alias>

   <URI>

   Example of <URI> when using a local repository:

   iso:/?iso=/<ISO file including path>

   <Alias>

   Attention: Replace <Alias> with a character string that does **not** end in DVD<number> (for example DVD1). If this string contains at least one blank, it must be enclosed by quotation marks.

   Example of <Alias>: OSC

   Command example;

   ```
   # zypper ar iso:/?iso=/media/OpenScapeUcSuiteApps-Repository-V10.0.0-060000.iso OSC
   Adding repository 'OSC' [done]
   Repository 'OSC' successfully added
   Enabled: Yes
   Autorefresh: No
   URI: iso:///?iso=/media/OpenScapeUcSuiteApps-Repository-V10.0.0-060000.iso
   ```

8. Go to Section 5.2.10.4, “Finish the Installation Medium Setup”, on page 349 to complete the installation medium setup.

5.2.10.4 Finish the Installation Medium Setup

1. The result of the add repository action can be verified the 'list repository' (lr) option;

   Command example;

   ```
   # zypper lr
   # | Alias                          | Name | Enabled | Refresh
   --+--------------------------------+------+---------+--------
   1 | OSC                            | OSC  | Yes     | No
   ```

2. Use the zypper refresh (ref) command to determine if the repository was defined correctly.

Note: In the case the command result asks;

"Do you want to reject the key, trust temporarily, or trust always? [r/t/a/?]"

A positive response would be 't' (temporarily) or 'a' (always). Reference the example provided. **In this case the 'a' response is chosen.**

Command example;

```
# zypper ref
Retrieving repository 'OSC' metadata [\]

New repository or package signing key received:
Key ID: 9351C8D3C9172AE7
Key Name: SEN-HiPathApplication (Signing of RPMs) <e-sw-
production-team.com@siemens.com>
Key Fingerprint: 03DF2920E8C51F91E2B6B4EB9351C8D3C9172AE7
Repository: OSC


Do you want to reject the key, trust temporarily, or trust
always? [r/t/a/?] (r): a
Retrieving repository 'OSC' metadata [done]
Building repository 'OSC' cache [done]
All repositories have been refreshed.
```

3. After the repository is correctly defined, the osc-setup package can be installed or updated.

   To determine whether the osc-setup is already installed the following command can be run;

   rpm -qa | grep -i osc-setup

   Output if osc-setup **IS** installed (in this example 'osc-setup-1.4.6-7');

   ```
   root@lc061:[/software/oscISOs] #330
   # rpm -qa | grep -i osc-setup
   osc-setup-1.4.6-7
   root@lc061:[/software/oscISOs] #331
   #
   ```

   Output if osc-setup **IS NOT** installed;

   ```
   root@lc061:[/software/oscISOs] #331
   # rpm -qa | grep -i osc-setup
   root@lc061:[/software/oscISOs] #332
   #
   ```

   If osc-setup IS installed proceed to step 3a), then step 4.

   If osc-setup IS NOT installed proceed to step 3b), then step 4.

a) Use the following command to verify the current osc-setup of the OpenScape UC Application is used. If required, osc-setup is updated automatically.

Command example;

 # osc-setup up osc-setup
Building repository '36775188f3b177bb47bb16464f14b1ee' cache [....done]
Loading repository data...
Reading installed packages...
No update candidate for 'osc-setup'.
Resolving package dependencies...
Nothing to do.

b) For a new installation of the osc-setup;

Note: At the "**Continue? [y/n/?] (y):**" prompt type '**y**' and then press the '**enter**' key. Reference the example provided.

Command example;

```
# zypper in osc-setup
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following NEW packages are going to be installed:
    augeas-osc libzypp-osc osc-setup satsolver-osc zypper-osc

The following packages need additional customer contract to
get support:
    augeas-osc libzypp-osc osc-setup satsolver-osc zypper-osc

5 new packages to install.
Overall download size: 5.0 MiB. After the operation,
additional 16.8 MiB will be used.
Continue? [y/n/?] (y): y

Retrieving package augeas-osc-0.9.0-3.x86_64 (1/5), 555.0 KiB
(1.6 MiB unpacked)
Installing: augeas-osc-0.9.0-3 [done]
Retrieving package satsolver-osc-0.16.1-3.x86_64 (2/5), 1.3
MiB (3.7 MiB unpacked)
Installing: satsolver-osc-0.16.1-3 [done]
Retrieving package libzypp-osc-9.4.0-4.x86_64 (3/5), 2.6 MiB
(9.9 MiB unpacked)
Installing: libzypp-osc-9.4.0-4 [done]
Retrieving package zypper-osc-1.5.3-14.x86_64 (4/5), 570.0
KiB (1.4 MiB unpacked)
Installing: zypper-osc-1.5.3-14 [done]
Retrieving package osc-setup-1.4.1-4.x86_64 (5/5), 27.0 KiB
(112.0 KiB unpacked)
Installing: osc-setup-1.4.1-4 [done]
```

4. At this point, the repository created in step 2 on page 350 is no longer required. Use the zypper clean command to clear the local cache.

```
# zypper clean
All repositories have been cleaned up.
```

5. A directory path must be created in order to build an installation repository from the ISO files;

   Command example;

   # mkdir /software/tmpREPO

6. Use the osc-setup command 'create repository' (cr) option to build the installation repository. The recommended method to create this repository is with the '--base-directory' (b) option. This option will include all ISO files from the directory created in Section 5.2.10.1, Section 5.2.10.2, and Section 5.2.10.3.

   The syntax of the osc-setup create repository command;

   osc-setup cr -b <path_to_ISO_files> -l <path_of_the_installation_repository>

   -b (BaseDir) Include all ISOs files based in Folder of given ISO-Files. The **'Repository'** ISO should be specified with the 'b' option.

   -l (lower case l) export linked repository into the specified DIR (this directory has to be empty!). This creates a temporary, local linked repository. This repository can only be used as long as the ISO files used are not deleted or moved and the computer is not rebooted.

   Command example (and log result) for the Section 5.2.10.1, “Create Setup medium from ISO files on the server hard disk”, on page 343" installation case;

   # osc-setup cr -b /software/oscISOs/OpenScapeUcSuiteApps-Repository-V10.0.0-060000.iso -l /software/tmpREPO

```
Logging to: /var/log/OpenScapeUC/osc-setup-2012-02-
24_10:51:11.log
osc-setup version: "1.4.1-4"
SUSE VERSION: 11 SERVICEPACK: 1
checking Arguments
Option Base-directory: yes
Option Export-linked-dir:/software/tmpREPO
/software/oscISOs/OpenScapeUcSuiteApps-BasePackage-V10.0.0-
060000.iso
performing cleanup....
cleanup sucessfully done
using Loop device /dev/loop8
using Loop device /dev/loop9
using Loop device /dev/loop10
using Loop device /dev/loop11
Splitrepository "base" integrated
Splitrepository "en" integrated
Splitrepository "de" integrated
Splitrepository "meta" integrated
Repository created sucessfully
removing all registered repositories
register new repository
```

```
Logging to: /var/log/OpenScapeUC/osc-setup-2012-02-
24_10:51:47.log
osc-setup version: "1.4.1-4"
SUSE VERSION: 11 SERVICEPACK: 1
Adding repository 'ce832b1ba0006f08893bb85d18632b8b'
[......done]
Repository 'ce832b1ba0006f08893bb85d18632b8b' successfully
added
Enabled: Yes
Autorefresh: No
URI: dir:///software/tmpREPO


Operation took:  2 seconds
Logfile: /var/log/OpenScapeUC/osc-setup-2012-02-
24_10:51:47.log
CreateRepository end
Operation took:  39 seconds
Logfile: /var/log/OpenScapeUC/osc-setup-2012-02-
24_10:51:11.log
```

Command example for the Section 5.2.10.2, “Create Setup medium from ISO files on a USB media”, on page 345 installation case;

```
# osc-setup cr -b /media/OpenScapeUcSuiteApps-Repository-
V10.0.0-060000.iso -l /software/tmpREPO
```

Command example for the Section 5.2.10.3, “Create Setup medium from ISO files on a CD/DVD media”, on page 347 installation case;

```
# osc-setup cr -b /media/OpenScapeUcSuiteApps-Repository-
V10.0.0-060000.iso -l /software/tmpREPO
```

7. Links back to other sections;

   If you are performing Applications Installations (new/fresh installation), please refer to the following links:

   For integrated simplex refer to Section 5.2.3.2, “Response File for Integrated Deployments”, on page 302.

   For a Stand Alone Media Server refer to Section 5.2.5.2, “Response File for Media Server Standalone deployments”, on page 325.

   For Multiple Communications Server Administration deployment refer to Section 5.2.6.2, “Response File for Multiple Communication Server Administration deployments”, on page 332.

   If you are performing Applications Updates (updating a DVD/Build level within the same release (e.g., from Build 8 to Build 9)), please refer to the following links:

   For Integrated systems refer to Section 5.2.3.5, “Update/Upgrade of Integrated Applications”, on page 310, step 3 on page 311.

   For Offboard Apps Server refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356, step 2 on page 357.

If you are Adding Additional Packages/Languages:

And you arrived here from Appendix 28.9.1, “Adding Additional Packages/Languages”, step 4 then return to 4 on page 791 of Appendix 28.9.1, “Adding Additional Packages/Languages”.

For Offboard Apps Server refer to Section 5.2.15, “Adding Additional Packages/Languages - Offboard (External) Apps Server”, on page 362 step 4 on page 364.

If you are Upgrading V8R1 Offboard Applications to V10:

Follow this link back to Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377 step 5 on page 379.

5.2.11 Cleaning up the Repositories

Attention: If more packages are required for your site (i.e.; languages besides English) do not perform these steps until **Section 5.2.5.4, “Adding Additional Packages/Languages”, on page 330** is reviewed.

Note: For Media Server StandAlone or Multiple Communication Server Admin deployments only;

The 'syncUC sync' command synchronizes the currently active partition towards the passive partition (fallback partition). The following paths are not synchronized by the syncUC action;

- /tmp
- /proc
- /sys
- /mnt

If the clean up task is not performed and a 'syncUC sync' action is executed; Installation, Upgrade, Update or Hotfix repositories mounted to other paths will be copied to the fallback partition. For more information regarding syncUC, refer to Section 5.2.16, “syncUC”, on page 365.

Note: For Simplex OSV deployments only;

Simplex OSV partitions can be synchronized from the CMP Dashboard. If the

clean up task is not performed and a synchronization action is executed, the Installation, Upgrade, Update or Hotfix repositories would be copied to the fallback partition.

If the installation/update/upgrade process is complete, the system should be cleaned of ISOs and repositories.

1. Unmount all isos and clean internal linked repo (**This does not remove repositories from repolist!**). This command cannot be used with other commands.

   # osc-setup cr --clean

2. De-register the temporary repository from the list of registered repositories. The osc-setup lr (list repository) command will present a list of repositories.

   Note: The repository can be either the repository URI or its index (starting from 1) as reported by the list repositories command (**osc-setup lr**). If the repository is not defined the first repository from list will be removed.

   # osc-setup rr dir:///software/tmpREPO

3. De-register any ISO repository from the list of registered repositories.

   Note: A repository can be removed with the URI or Alias. All of the examples used the Alias OSC.

   Command example(s) with Alias;

   # zypper rr OSC

   Command example(s) with URI (for the Section 5.2.10.1, “Create Setup medium from ISO files on the server hard disk”;

```
# zypper rr iso:///?iso=/software/oscISOs/OpenScapeUcSuiteApps-
Repository-V10.0.0-060000.iso
```

4. Clean all local caches created with zypper.

   Command example;

   # zypper clean

5. List the zypper repositories to ensure the 'OSC' repository does not exist.

   # zypper lr

6. Remove data from the /software/tmpREPO path;

   Command example;

   # cd /
   # rm -rf /software/tmpREPO

7. Remove data from the /software/oscISOs/ path;

   Command example;

   # rm -rf /software/oscISOs/

Note: This note only applies to Upgrade and Migration procedures. If you arrived here from the Upgrade and Migration procedure of Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377.

If there are no HotFixes required for the External (offboard) Applications target release return to the appropriate Upgrade and Migration procedure as follows:

Section 8.6.2, “Upgrade Steps for a Duplex System”, step 6 on page 488

Section 8.7.2, “Upgrade Steps for Remote SW Upgrade”, on page 493, step 4 on page 494

In case of applications upgrade failure during Upgrades or Migration procedures, refer to Section 5.7.2, “Fallback During Upgrade Procedure”, on page 382 of this document.

5.2.12 Uninstall External (OffBoard) Applications Server Applications

This section addresses the removal of the Applications from a Multiple Communications Server Admin or Media Server Standalone deployment.

There is no generally available method to remove the External Applications Server (OffBoard) Applications. When you must remove the Applications, please contact your next level of support.

5.2.13 Apply an Update - Offboard (External) Apps Server

This section applies to the Media Server Standalone and Multiple Communication Server Admin. Deployments.

We differentiate between updating and upgrading as follows:

- Update

  An update is performed when a new fix release or hotfix is available for an installed version of the OpenScape Applications (within the same release).

Example:

An OpenScape Application V10 R1 was installed in version FR1 (Fix Release 1). A V10 R1 FR2 or FR2 F1 is released as an update.

- Upgrade

  For example, if in contrast, an OpenScape Application V9 R1 is installed and a V10 R0 Applications setup medium is to be used, we refer to this as an “upgrade” to V10. For Offboard Applications Upgrade, refer to Section 5.7, “Upgrade of Offboard (External) Apps Server”, on page 376.

Information regarding Offboard (external) Apps servers backups can be found in;

- *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section “Installing and Configuring the Computer and Operating System”*.
- *OpenScape UC Application V10 Configuration and Administration.*

The syncUC script can be used for backing up the current version of Applications to a 'passive' or Fallback partition of your server hard drive. For more information regarding syncUC, refer to Section 5.2.16, “syncUC”, on page 365.

Attention: This section describes how to manually install an update from the command line. To install an update from the CMP (which significantly reduces the manual steps required) see the subsection titled *“Software Activation (User Interface Patching)” in the “OpenScape Common Management Platform Vx, Administration, Administrator Documentation” (*where *x* is the software release version*).*

It would be a good practice to review the “Software *Activation (User Interface Patching)*" section in its entirety before proceeding with the User Interface Patching procedure.

Execute the following update steps:

1. Prepare the Update Medium for the Offboard Apps server.

   To prepare the environment for the update, please refer to Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341. At the end of Section 5.2.10 a link back to this section is provided.

2. Stop the OpenScape UC Application by executing the following command:

   Command example;

   ```
   # /etc/init.d/symphoniad stop
   ```

3. Update the Applications using the following syntax;

   Command example:

   ```
   # osc-setup up
   ```

The upgrade process is fully automatic and since no configuration files are overridden, you need not back up these files before the upgrade.

Note: IF HotFixes are required for the External (offboard) Applications server target release, then proceed to Section 5.6, “Installing a HotFix”, on page 376. It is a good practice to review the HotFix Release Notes in case that procedure differs from the "Installing a HotFix" section of this document. The actual HotFix release note should include detailed instructions.

---

4. Start the OpenScape UC Application when the upgrade process is finished by executing the following command:

   Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

   ```
   #/etc/init.d/symphoniad start
   ```

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

   Questions should be addressed to your next level of support.

5. If the update process is complete the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.2.14 Installing a HotFix - Offboard (External) Apps Server

This section applies to the Media Server Standalone and Multiple Communication Server Admin. Deployments.

Information regarding Offboard (external) Apps servers backups can be found in;

- *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section "Installing and Configuring the Computer and Operating System"*.
- *OpenScape UC Application V10 Configuration and Administration.*

The syncUC script can be used for backing up the current version of Applications to a 'passive' or Fallback partition of your server hard drive. For more information regarding syncUC, refer to Section 5.2.16, "syncUC", on page 365.

To provide the set-up medium from ISO files downloaded to the Applications server, refer to Section 5.2.10.1, "Create Setup medium from ISO files on the server hard disk", on page 343, step 1 on page 343. After step 1 is completed a doclink back to this section will be available.

To provide the set-up medium from ISO files on a USB refer to Section 5.2.10.2, "Create Setup medium from ISO files on a USB media", on page 345, steps 1 on page 345 through 5. After the indicated steps are completed a doclink back to this section will be available.

To provide the set-up medium from ISO files on a USB refer to Section 5.2.10.3, "Create Setup medium from ISO files on a CD/DVD media", on page 347, steps 1 on page 348 and 2. After the indicated steps are completed a doclink back to this section will be available.

Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

Note: This procedure has the user remove all repository entries (except the '**SUSE Linux**' entry - if it exists). Install all required RPMs from the repository to be deleted before removing it.

Attention: This section describes how to manually install a HotFix from the command line. To install a HotFix from the CMP (which significantly reduces the manual steps required) see the subsection titled "*Software Activation (User Interface Patching)"* in the "OpenScape *Common Management Platform Vx, Administration, Administrator Documentation" (*where *x* is the software release

version*)*.

It would be a good practice to review the "*Software Activation (User Interface Patching)"* section in its entirety before proceeding with the User Interface Patching procedure.

---

1. Transfer the ISO file to the server. In this example the ISO is transferred to /software.
2. Stop the Applications.

   Command example;

   #> /etc/init.d/symphoniad stop
3. Execute the zypper lr (list repository) command to check which sources have been provided in zypper:

   `osc-setup lr`

   Command example:

   # osc-setup lr

```
# | Alias | Name | Enabled | Refresh
--+-------------------------------------------+------+---------+--------
1 | SUSE-Linux-Enterprise-Server-11-SP1 11.1.1-1.152 | SUSE-Linux-Enterprise-
Server-11-SP111.1.1-1.152 | Yes | No
```

4. Verify that only the SLES setup medium is registered.
5. If further setup media are registered, remove them with the following command:

   `osc-setup rr <number>`

   <number> is the number you find in the first column of the zypper lr output

   Command Example:

   # osc-setup rr 2
6. Execute the zypper lr (list repository) command to verify your changes;

   # osc-setup lr
7. Now the ISO can be added as a repository.

   Command example;

   #> osc-setup ar iso:/?iso=/software/ OpenScapeUcSuiteApps_PATCH-V10.0.0-100002.iso
8. Verify you have the latest version of the osc-setup too.

   Command example;

   #> osc-setup up osc-setup
9. Update the Applications.

Command example;

```
#> osc-setup up
```

Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

---

10. After the successful update start the Applications.

    Command example;

    ```
    #> /etc/init.d/symphoniad start
    ```

    The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

    For integrated applications servers;
    tailf /log/osgi.log

    For External (offboard) applications servers;
    tailf /var/siemens/common/log/osgi.log

    Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

    Press **'ctrl+c'** to exit the tail function.

11. If the HotFix install is complete the system should be cleaned of ISOs. Start by listing the current repositories;

    ```
    osc-setup lr
    ```

12. Remove unnecessary setup media. '**SUSE-Linux**' media entry should not be deleted.

13. If further setup media are registered, remove them with the following command:

    ```
    osc-setup rr <number>
    ```

    <number> is the number you find in the first column of the zypper lr output.

    Command Example:

    ```
    # osc-setup rr 2
    ```

14. Execute the zypper lr (list repository) command to verify your changes;

    ```
    # osc-setup lr
    ```

15. Remove the ISO file that was transferred to the server in step 1 of this procedure.
16. The HotFix install is complete.

Note: This note only applies to Upgrade and Migration procedures. If you arrived here from the Upgrade and Migration procedure of Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377.

If there are no HotFixes required for the External (offboard) Applications target release return to the appropriate Upgrade and Migration procedure as follows:

Section 8.6.2, “Upgrade Steps for a Duplex System”, step 6 on page 488

Section 8.7.2, “Upgrade Steps for Remote SW Upgrade”, step 4 on page 494

In case of applications upgrade failure during Upgrades or Migration procedures, refer to Section 5.7.2, “Fallback During Upgrade Procedure”, on page 382 of this document.

5.2.15 Adding Additional Packages/Languages - Offboard (External) Apps Server

This section applies to the Media Server Standalone and Multiple Communication Server Admin. Deployments.

Information regarding Offboard (external) Apps servers backups can be found in;

- *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section “Installing and Configuring the Computer and Operating System”.*
- *OpenScape UC Application V10 Configuration and Administration*.

The syncUC script can be used for backing up the current version of Applications to a 'passive' or Fallback partition of your server hard drive. For more information regarding syncUC, refer to Section 5.2.16, “syncUC”, on page 365.

The default installation sets up only the basic language English for the Offboard Apps Server telephone prompts. If you wish to install further languages, execute the following steps:

All commands are to be executed as user *root*.

1. Verify that the installation files (ISO files) you require for languages are provided in osc-setup with the 'list repository' (lr) command;

   Command example;

   ```
   # osc-setup lr
   Logging to: /var/log/OpenScapeUC/osc-setup-2012-04-12_10-04-42.log
   osc-setup version: "1.4.5-17"
   SUSE VERSION: 11 SERVICEPACK: 1
   Registered repository (url):
       1   dir:///software/tmpREPO
   Operation took:  0 seconds
   ```

2. If the installation repository does not exist proceed to step 4 on page 364.

   If the installation repository exists use the osc-setup search (se) option to list the available packages (in this case announcements);

   ```
   osc-setup se --match-any announ
   ```

   Command example:

   ```
   # osc-setup se --match-any announ
   Loading repository data...
   Reading installed packages...
   ```

   ```
   S | Name | Summary | Type
   --+--------------+-------------------------------------------------------------------
   | mediaserver_announcements_ar | Mediaserver_announcements_ar | package
   | mediaserver_announcements_bg | Mediaserver_announcements_bg | package
   ...
   i | mediaserver_announcements_en_us | Mediaserver_announcements_en_us | package
   | mediaserver_announcements_en_za | Mediaserver_announcements_en_za | package
   ...
   ```

Note: An 'i' in the column S column indicates that package is already installed.

3. If the language is not listed proceed to step 4 on page 364.

   If the required language is listed then execute the following command for installing another language;

   ```
   osc-setup in mediaserver_announcements_<language code>
   ```

   Comand examples;

   ```
   # /etc/init.d/symphoniad stop
   # osc-setup in mediaserver_announcements_en_za
   ```

   Note: This language is used for the media server announcements provided for the PBX.

You can install several languages with one command.

Command example:

```
# osc-setup in mediaserver_announcements_en_za
mediaserver_announcements_es_es
```

If you were able to install all languages then proceed to step 5 on page 364, otherwise continue with step 4 on page 364.

4. If the language is not available then the 'Repository' and required language ISO files will have to be staged for installation. See Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341 for details of this procedure.

Note: Providing an ISO file as repository retrospectively deletes the provision of the current repository. Install all required RPMs from the repository to be deleted before removing it.

Now the language package can be installed with the same syntax demonstrated in step 3 on page 363 of this procedure. **Remember to stop the symphoniad before adding a new package.**

```
osc-setup in mediaserver_announcements_<language code>
```

5. Start the Applications server;

   Command example:

   ```
   # /etc/init.d/symphoniad start
   ```

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* **Start processing all bundles done.*** " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

5.2.16 syncUC

Attention: syncUC command can be used on an Offboard (external) Apps server if the Apps server was installed in V7 or higher or upgraded to V7 or higher.

Attention: When using syncUC with the "Multiple Communication Admin Server" or "Media Server Standalone" Applications deployments; the recommended disk sizing is 2 x 300GB in RAID-1 configuration.

This section applies to the Media Server Standalone and Multiple Communication Server Admin. Deployments.

All commands should be executed as the root user.

It is a good practice to review this section in its entirety and address any questions to your next level of support before proceeding with any command executions.

5.2.16.1 Introducing syncUC

Note: The syncUC feature is intended for offboard (external) Applications servers.

An Integrated Simplex OSV deployment has the OpenScape Applications installed on the same server that hosts OpenScape Voice. This deployment employs the 'sync8k' command to backup the Active partition to the Fallback partition; therefore syncUC is not required in an Integrated Simplex OSV deployment.

There are the following fallback options:

- syncUC

  syncUC uses a partition of the local hard disk. The OpenScape UC Application is installed in this Root partition of the LVM2 memory. The syncUC script enables synchronizing this installation on the free memory in the LVM2 (command syncUC sync). Both OpenScape UC Application installations are fully equivalent. After a computer reboot you can start the OpenScape UC Application on the Root partition or the synchronized version of the OpenScape UC Application. You can start the synchronized version if the installation on the Root partition was performed on the grounds of one of the following situations:

  – Faulty upgrade

  - Faulty installation of a fix release or hotfix
  - Configuration error, for example deletion of large numbers of users
  - Software problems, for example Solid database crash

  You will find details about using syncUC in Section 5.2.16.2, “syncUC Commands”, on page 366.

- File system backup

  The file system backup serves to restore files after a catastrophic failure. It is executed by the lvBackupManagementUtility.sh script (see *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section “Installing and Configuring the Computer and Operating System”, Section 4.5, “Configuring the File System Backup”*).

5.2.16.2 syncUC Commands

You can use syncUC as follows:

- syncUC sync

  The syncUC sync command synchronizes the currently active partition towards the passive partition (fallback partition).

  The following paths are not synchronized by the syncUC action;

  - /tmp
  - /proc
  - /sys
  - /mnt

  Installation, Upgrade, Update or Hotfix repositories mounted to other paths will be copied to the fallback partition. If you wish to 'clean up' the repositories prior to the syncUC action, refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

  1. When executing syncUC initially it realizes that no configuration is available yet. The following is put out:

     ```
     Do you want to configure and enable partitioning now?
     Please enter yes or no (default = no):
     ```

  2. Enter **yes** and push the return key.
  3. The following is displayed for example:

     ```
     Found logical volumes:
     1 ) /dev/OpenScapeUC/UC1 [actually mounted to /]
     2 ) /dev/OpenScapeUC/UC2 [actually not mounted]
     ```

```
Please enter the first partition (Number or devicefile ,
default: 1):
```

syncUC has detected the two displayed partitions and asks for the partition on which the OpenScape UC Application is installed. OpenScape UC Application should have been installed on the partition you have set up. Reference *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section "Installing and Configuring the Computer and Operating System", Section 4.2.2.5, "Creating the Logical Volume UC1"*.

Note: You will find the names of the Logical Volume Group (example: OpenScape UC) and of the logical partitions (logical volumes) (examples: UC1 and UC2) again in *Table 4 "Partition Sizes when using a USB Hard Disk for File System Backup"* of the *OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section "Installing and Configuring the Computer and Operating System"*.

Perform one of the following actions:

a) You need not do anything if the partition suggested as default solution is the correct one.

b) If a solution different from the default is correct, enter the corresponding digit.

c) Enter the complete path of the correct partition. This path can be displayed by the lvdisplay command.

   Example result:

```
- Logical volume -
LV Name /dev/OpenScapeUC/UC1
VG Name UCVolumeGroup
LV UUID E1zTel-MtSn-Okmt-J1ud-Fhpk-o4G=-EUNryH
...
```

4. Push the return key.

   The following is output:

```
Please enter the second partition (Number or devicefile ,
default: 2):
```

5. Based on the step 3 on page 366 results, specify the partition created as the fallback partition for the OpenScape UC Application.

6. Push the return key.

   Eventually the following is output:

```
The configuration has been saved.
```

Note: You will find an overview of the partitions on the computer in *Table 3* and *Table 4* of the *"OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section "Installing and Configuring the Computer and Operating System"*.

- syncUC query

  The syncUC query command delivers the current status of the active and passive partition. In this way you can see which of the partitions is active and which is passive. Example given:

  ```
  Active version is 6_1.0.0-000000 (SOL6.1 OSC6.1 DVD0)
  installed on Mon Oct 24 21:06:02 2011 located on /dev/
  OpenScapeUC/UC2

  Passive version is 6_1.0.0-000000 (SOL6.1 OSC6.1 DVD0)
  installed on Mon Oct 24 21:06:02 2011 located on /dev/
  OpenScapeUC/UC1 which was synchronized on Mon Oct 24 22:00:00
  2011
  ```

  If no system has been configured, an output similar to the following is displayed.

  ```
  Active version is package OpenScapeUC_ProductVersion is not
  installed (package OpenScapeUC_ProductVersion is not
  installed) installed on package
  OpenScapeUC_ProductVersion is not installed located on /dev/
  OpenScapeUC/UC1.

  Passive version is package OpenScapeUC_ProductVersion is not
  installed (package OpenScapeUC_ProductVersion is not
  installed) installed on package
  OpenScapeUC_ProductVersion is not installed located on /dev/
  OpenScapeUC/UC2 which was synchronized on unknown date.
  ```

- syncUC fallback

  Executing the syncUC fallback command marks the active partition as passive and the passive partition as active. When you reboot the computer, it boots from the partition marked as active, i. e. this partition becomes active and the partition marked as passive becomes passive.

5.2.16.3 Switching from File System Backup to syncUC

If you use syncUC on this computer already, continue with Section 5.2.16.4, "Fallback Preparation", on page 370.

Follow the instructions in this section if you have used the file system backup on this computer so far and wish to deploy syncUC from now on.

1. Unmount the partition of the file system backup.

   Example:

```
# umount /backups
```

2. Execute the command:

   ```
   lvdisplay
   ```

   In the following example the output for the partition of the Volume Group (example: OpenScapeUC) file system backup of the OpenScape UC Application:

   ```
   ...
   --- Logical volume ---
   LV Name /dev/OpenScapeUC/backups
   VG Name OpenScapeUC
   LV UUID Upi8lc-IyML-O5Qj-X3EE-OdJz-NQsT-g9OWhc
   LV Write Access read/write
   LV Status available
   # open 1
   LV Size 50.00 GB
   Current LE 12800
   Segments 1
   Allocation inherit
   Read ahead sectors auto
   - currently set to 1024
   Block device 253:2
   ```

3. Remove the partition of the file system backup.

   Example:

   ```
   # lvremove /dev/OpenScapeUC/backups
   ```

   The following is output:

   ```
   Do you really want to remove active logical volume "backups"?
   [y/n]:
   ```

4. Push the **y** key.

   ```
   Logical volume "backups" successfully removed
   ```

5. Remove from the /etc/fstab file the line in which this file system has been configured for permanent mounting. In the following example this is the last line.

   ```
   /dev/sda1 swap swap defaults 0 0
   /dev/OpenScapeUC/UC / ext3 acl,user_xattr 1 1
   /dev/sda2 /boot ext3 acl,user_xattr 1 2
   proc /proc proc defaults 0 0
   sysfs /sys sysfs noauto 0 0
   debugfs /sys/kernel/debug debugfs noauto 0 0
   usbfs /proc/bus/usb usbfs noauto 0 0
   devpts /dev/pts devpts mode=0620,gid=5 0 0
   /dev/OpenScapeUC/backups /backups ext3 acl,user_xattr 1 2
   ```

   The partition of the file system backup and the entry in the /etc/fstab file will be automatically created again when you back up the file system the next time.

6. Continue with Section 5.2.16.4, “Fallback Preparation”, on page 370.

5.2.16.4 Fallback Preparation

1. Check whether the active partition has already been synchronized to the passive partition with syncUC.

   # syncUC query

   Example output:

   ```
   Active version is 6_1.0.0-000000 (SOL6.1 OSC6.1 DVD0)
   installed on Mon Oct 24 21:06:02 2011 located on /dev/
   OpenScapeUC/UC2

   Passive version is 6_1.0.0-000000 (SOL6.1 OSC6.1 DVD0)
   installed on Mon Oct 24 21:06:02 2011 located on /dev/
   OpenScapeUC/UC1 which was synchronized on Mon Oct 24 22:00:00
   2011
   ```

2. If this level of the passive partition is the level the OpenScape UC Application is to fall back on after a possibly failed update, upgrade, migration or installation of a hotfix, you need not become active here.

   If, in contrast, the OpenScape UC Application is to fall back on the current level of the OpenScape UC Application, execute the following command:

   # syncUC sync

5.2.16.5 Links back

If you are performing Applications Installations please refer to the following links;

For a Stand Alone Media Server refer to Section 5.2.5.3, “Installing Media Server Standalone”, on page 328.

For Multiple Communications Server Administration deployment refer to Section 5.2.6.3, “Installing Multiple Communications Server”, on page 335.

If you are performing Applications Updates please refer to the following links;

For Offboard Apps Server refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356.

If you are Adding Additional Packages/Languages;

For Offboard Apps Server refer to Section 5.2.15, “Adding Additional Packages/Languages - Offboard (External) Apps Server”, on page 362.

5.3 Starting and Stopping the OpenScape Applications

To start the OpenScape Applications, as user *root*, enter the command:

```
/etc/init.d/symphoniad start
```

The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

For integrated applications servers;
tailf /log/osgi.log

For External (offboard) applications servers;
tailf /var/siemens/common/log/osgi.log

Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

Press **'ctrl+c'** to exit the tail function.

Questions should be addressed to your next level of support.

To stop, enter the command:

```
/etc/init.d/symphoniad stop
```

5.4 Accessing the OpenScape Applications

5.4.1 Accessing the CMP/OpenScape Voice Assistant

From a web browser, access the CMP/OpenScape Voice Assistant with the URL https://<IP address>/management and enter the password:

User: **administrator@system**
password: Provide the ADMIN_PASSWORD specified in the response file.

The IP address you use in the URL to access the CMP/OpenScape Voice Assistant is dependant on the type of OpenScape Voice system:

- Integrated simplex systems

  Use the IP address specified by the **'node_1_ip'** parameter of the node.cfg file. From node 1's SSH prompt, run the following command to identify the **'node_1_ip'** IP address:

  # grep 'node_1_ip' /etc/hiq8000/node.cfg

  Example given;

  ```
  sysad@x3550st1n1:[/home/sysad] #5
  ```

  $ grep -i 'node_1_ip' /etc/hiq8000/node.cfg

```
node_1_ip: 10.235.85.6
lsm_node_1_ip: 10.235.85.8
```

In this example 10.235.85.6 (the **'node_1_ip'** result) would be employed to access the CMP/OpenScape Voice Assistant.

- External OpenScape Applications server

  Use the IP address of *eth0* of the external applications server. From the external applications server SSH prompt, run the following command to identify the *eth0* IP address:

  # ifconfig eth0

5.4.2 Accessing DLS

From a web browser, access the DLS with the URL `https://<IP address where DLS is installed>/DeploymentService`, enter the following user name and password pair:

```
User: admin
Password: Asd123!.
```

Note: This default password is for Linux DLS and is not applicable for the Windows version of DLS

Access to the DLS interface is established via the *bond_node_alias* address.

5.4.3 Accessing CLM

In order to log onto the CLM, modifications have to be made to the ClmSettings.xml file.

On the integrated system, execute the following commands:

 # cd /enterprise/clm/

 # sh remoteAccess.sh <IP address 1>,<IP address 2>,<IP address n>

<IP address 1>,<IP address 2>,<IP address n> are the remote IP addresses to be allowed access to the CLM.

For example,

```
# sh remoteAccess.sh 10.5.12.40,10.0.251.42,10.235.65.221
```

Attention: Verify that no blanks are entered between the IP addresses.

On an external applications server, execute the following commands:

 # cd /opt/licenses/clm

 # sh remoteAccess.sh <IP address 1>,<IP address 2>,<IP address n>

<IP address 1>,<IP address 2>,<IP address n> are the remote IP addresses to be allowed access to the CLM.

Example:

 # sh remoteAccess.sh 10.235.200.113,10.235.200.28,10.235.65.221

Attention: Verify that no blanks are entered between the IP addresses.

5.5 Retrieving Trace File Information

Note: For information relating to the OpenScape Voice 'SESAP' or 'Trace Manager';
- For SESAP, refer to Section “Continuous *Trace*” in the *OpenScape Voice V11, Service Manual, Service Documentation, Serviceability Features*

- For the OpenScape Voice Trace Manager (OSVTM), refer to the “OpenScape *Voice Vx, Trace Manager, Service* D*ocumentation”* (where *x is the software release version*).

The OpenScape Applications include a small tool for easy gathering of diagnostic information.

Generate and retrieve the trace file as follows:

1. Log in as *root* on the machine where the Common Management Platform (CMP) is installed (external server where the OpenScape Applications are installed for a non-integrated system or OpenScape Voice for an integrated system) and issue the appropriate command for the type of system:

   Standard duplex (external applications server):

   ```
   # sh /opt/siemens/assistant/scripts/traces.sh
   ```

   Integrated systems (integrated applications):

   ```
   # sh /enterprise/assistant/scripts/traces.sh
   ```

   The system displays information similar to the following example:

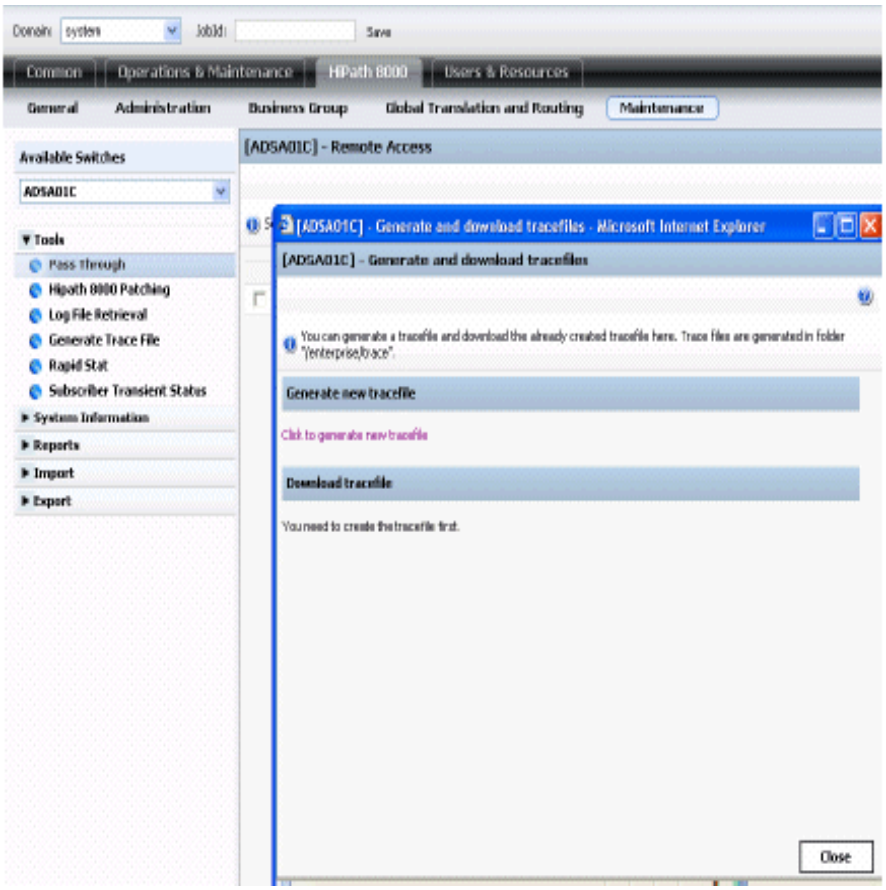
   Note: OpenScape Voice was formerly known as HiPath 8000. References to HiPath 8000 in the following example are equivalent to OpenScape Voice.

```
adsa11n1:~ # sh /opt/siemens/assistant/scripts/traces.sh
Old trace files deleted.
Storing HiPath 8000 Assistant Traces at adsa11n1-2007-03-06-
15-30-55
Old trace files deleted.
Storing HiPath 8000 Assistant Traces at adsa11n2-2007-03-06-
15-30-55
Trace files stored, getting system information...
Trace files stored, getting system information...
Tar and compressing information
Trace Archive created in /opt/siemens/trace
total 1884
-rw-r--r-- 1 root root 1921742 Mar 6 15:31 trace-adsa11n2-
2007-03-06-15-30-55.tar.gz
Tar and compressing information
Trace Archive created in /opt/siemens/trace
trace-adsa11n2-2007-03-06-15-30-55.tar.gz
100% 1877KB 1.8MB/s 00:00
trace-adsa11n1-2007-03-06-15-30-55.tar.gz
trace-adsa11n2-2007-03-06-15-30-55.tar.gz
/opt/siemens/trace/trace-adsa11n2-adsa11n1-2007-03-06-15-30-
55.tar.gz: No such file or directory
tar: /opt/siemens/trace/trace-adsa11n2-adsa11n1-2007-03-06-
15-30-55.tar: file is the archive; not dumped
total 4488
-rw-r--r-- 1 root root 4579331 Mar 6 15:32 trace-adsa11n2-
adsa11n1-2007-03-06-15-30-55.tar.gz
```

The script gathers required information in a compressed tar file archived for further analysis.

2. To retrieve the trace file from the CMP, click **Operation & Maintenance**, **Diagnostics, Diagnostics Data, Trace File**, and then **Download Trace File**.

Note: OpenScape Voice was formerly known as HiPath 8000. References to HiPath 8000 in the following example are equivalent to OpenScape Voice.


Domain: system
JobId:
Save
Common
Operations & Maintenance
HiPath 8000
Users & Resources
General
Administration
Business Group
Global Translation and Routing
Maintenance
Available Switches
ADSA01C
Tools
Pass Through
Hipath 8000 Patching
Log File Retrieval
Generate Trace File
Rapid Stat
Subscriber Transient Status
System Information
Reports
Import
Export
[ADSA01C] - Remote Access
[ADSA01C] - Generate and download tracefiles - Microsoft Internet Explorer
[ADSA01C] - Generate and download tracefiles
You can generate a tracefile and download the already created tracefile here. Trace files are generated in folder "/enterprise/trace".
Generate new tracefile
Click to generate new tracefile
Download tracefile
You need to create the tracefile first.
Close

5.6 Installing a HotFix

For Integrated systems please refer to Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313.

For Media Server Standalone and Multiple Communication Admin Server deployments please refer to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359.

5.7 Upgrade of Offboard (External) Apps Server

This section applies to the Multiple Communication Server Admin and Media Server Standalone deployments.

The following documents should be available because they will be referenced in this section;

- *Documentation OpenScape UC Application V10, Installation and Upgrade, Installation Guide.*
- *OpenScape Common Management Platform Vx Administration, Administrator Documentation (*where *x* is the software release version*)*

For the integrated Simplex OpenScape Voice deployments, the Applications upgrade is included in the integrated OpenScape Voice server's upgrade or migration process. Refer to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11” for details.

We differentiate between updating and upgrading as follows:

- Update

  An update is performed when a new fix release or hotfix is available for an installed version of the OpenScape Applications (within the same release).

  For example:

  A V10 OpenScape Application was installed in version FR1 (Fix Release 1). A V10 FR2 or FR2 HF1 is released as an update.

- Upgrade

  If in contrast, a V9 OpenScape Application is installed and a V10 Applications setup medium is to be used, we refer to this as an “upgrade” to V10.

Note: The “Upgrade of Offboard (External) Apps Server” sections are related to the Upgrade of Applications servers to new releases. To update an Applications server to the latest DVD Build/PatchSet/HotFix level, refer to one of the following sections as appropriate for your deployment scenario:

For DVD Build/PatchSet Updates
- Integrated system deployments, refer to Section 5.2.3.5, “Update/Upgrade of Integrated Applications”, on page 310

- Offboard (External) Apps Server, refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356

For HotFix Updates
- Integrated system deployments, refer to Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313

- Offboard (External) Apps Server, refer to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359

Overview

Multiple Communication Server Admin and Media Server Standalone Deployments are installed on a single node. It is recommended to use an one step upgrade with mixed repositories. Follow the steps below to perform the procedure:

- Create a complete backup of the system (disk + database) for fallback
- Stop UC Applications manually
- Upgrade V8R1 OpenScape UC applications to V10
- Upgrade the Operating System to SLES 15 by rebooting with SLES 15 DVD and following the Update steps of SLES 15
- Repartition the system, if required
- Start the applications manually after completing the upgrade

5.7.1 Upgrade of V8R1 Offboard Applications to V10

1. Update the source release Applications server to the latest released V10 DVD Build/PatchSet/HotFix level. These levels of the source release (as well as the target release) are specified in the V10 Release Notes.

   Note: The Applications installation includes the English language by default.

   If your upgrade includes a Media Server, take note of the languages that are already installed. Any additional languages would need to be downloaded and included in the installation repository.

Any customized announcement files should be saved to an offboard server (for restoral after the Applications install).

2. Create a complete backup of the offboard Applications server (database + system) by using the CMP (Common Management Platform). These backups will be needed in case of fallback. Any questions should be referred to your next level of support before proceeding.

   More details regarding backing up the Applications configuration data can be found in “OpenScape *Common Management Platform Vx Administration, Administrator Documentation”* (where *x* is the software release version).

   Attention: Backup archives created from the OpenScape Applications server can only be restored to the Applications server at that same software level (DVD Build / PatchSet / HotFix). Restoring Applications backup archives created at a different software level is not supported.

3. Store these backups as necessary to a local PC:

   a) Copy the previously created backup set to an external location. If the default archive has been used, the backup set folder can be found under "/var/siemens/backup".

   b) The response file used for the initial installation must also be saved externally, as it will be used for the reinstallation of the applications in case of fallback.

   c) In case CLM (Customer License Manager) is installed, save to an external location file ClmSettings.xml, which can be found under '/opt/licenses/clm/ApacheTomcat/'.

      This file contains the access configuration for the CLM.

   d) If your Applications employ the Executive - Assistant with Cockpit feature, the source release '.eag' files must be backed up to an external server for restoral after the upgrade. The files are found on the External Applications Server(OFFBoard) server at:

      "/opt/siemens/HiPathCA/WebSpace/Portal/webapps/eacockpit-osc/WEB-INF/groups"

      In the target release, these '.eag' files will be copied to the upgraded Applications server.

4. Stop the applications Symphonia and Openfire, external or internal, if installed, by executing the following commands:

   ```
   # /etc/init.d/symphoniad stop
   # /etc/init.d/openfire stop
   ```

5. Perform the OpenScape Applications upgrade. Start by preparing the setup medium for the offboard Apps server. To prepare the environment for the upgrade, refer to Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341. At the end of Section 5.2.10 a link back to this section is provided.

6. Upgrade the Applications using the following syntax:

   `# osc-setup dup`

   The upgrade process is fully automatic and since no configuration files are overridden, you need not back up these files before the upgrade.

Note: This note applies when the upgrade of the applications to V10 fails. These steps are outside the scope of an Upgrade or Migration procedure. In general, the following needs to be performed:

- Perform the steps of Section 5.7.2.2, “Fallback of External Applications Server using syncUC”, on page 382.

- Re-install the Applications server software to the same level as was backed up in Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377 step 2 on page 378 of this procedure.

- Restore the Applications with the backup set taken in Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377 step 2 on page 378 of this procedure.

Attention: Ensure that all workarounds described in the Release Notes were executed before you start the OpenScape UC Application for the first time. If you do not perform these workarounds the system may adopt a defective state.

---

7. The partitioning of the OpenScape Applications server should be verified.

   If the OpenScape Application server is installed with LVM partitions, refer to the section titled “Checking *the Partitioning*” in the document *OpenScape UC Application V10, Installation and Upgrade, Installation Guide*.

   If the LVM was installed with only a single partition, it must be updated. **Starting at step 3, execute all steps to the end.**

   When the OpenScape Application server is NOT installed with LVM Partitions, you need to follow these general steps:

   - Make a complete data backup using the CMP. Refer to steps 2 and 3 of this procedure.

- New Install UC V8R1 Applications to the same software level that was used in the first bullet item of this step.

  For Installation instructions refer to:

  - Section 5.2.4, “Updating using the CMP (UI Patching) instead of osc-setup”, on page 317

  - Section 5.2.6, “Installation/Update Instructions for Multiple Communications Server Admin deployment”, on page 331

  For DVD Build/PatchSet Updates:

  - Offboard (External) Apps Server, refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356

  For HotFix Updates:

  - Offboard (External) Apps Server, refer to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359

- New Install SLES 15 including LVM Partition layout.

  This is described in document *OpenScape UC Application V10, Installation and Upgrade, Installation Guide, Section “Installing and Configuring the Computer and Operating System”*. It is recommended that this section be reviewed in its entirety before partitioning the server and installing the appropriate SLES OS and service pack level.

- Restore data backup from the first bullet item of this step using the CMP.

Note: This note only applies to Upgrade and Migration procedures. If you arrived here from the Upgrade and Migration procedure of Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377 and DVD Build/PatchSet/HotFixes are required for the External (offboard) Applications server target release, then proceed as indicated:

For DVD Build/PatchSet Updates:

- Offboard (External) Apps Server, refer to Section 5.2.13, “Apply an Update - Offboard (External) Apps Server”, on page 356

For HotFix Updates:

- "Offboard (External) Apps Server, refer to Section 5.2.14, “Installing a HotFix - Offboard (External) Apps Server”, on page 359

It is a good practice to review the Release Notes in case that procedure differs from the section of this document. A HotFix release note should include detailed instructions.

If there are no DVD Build/PatchSet/HotFixes required for the External (offboard) Applications target release, complete steps 7 through 10of this procedure. Links to the upgrade procedures will be provided at the end of Section 5.2.11, “Cleaning up the Repositories”, on page 354.

Any questions should be referred to your next level of support before proceeding.

---

8. Upgrade the Operating System to SLES 15. Follow the instructions given in *OpenScape UC Application V10, Installation and Upgrade, Installation Guide.*
9. Start the OpenScape UC Application when the upgrade process is finished by executing the following commands:

   ```
   # /etc/init.d/symphoniad start
   # /etc/init.d/openfire start
   ```

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command, there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For External (offboard) applications servers:
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* ", the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'Ctrl+C'** to exit the tail function.
10. If the upgrade process is complete, the system should be cleaned of ISOs and repositories. Please refer to Section 5.2.11, “Cleaning up the Repositories”, on page 354.

5.7.2 Fallback During Upgrade Procedure

5.7.2.1 Fallback of Integrated System

Fallback of an integrated installation is tied to the OpenScape Voice system fallback. See the descriptions for fallback in Section 8.9.3, “Login to the console (native OSV/VM) or the RSA interface.”, on page 509.

Attention: In some failure scenarios a Fallback to the source release partition may not be necessary.
Contact your next level of support before proceeding.

5.7.2.2 Fallback of External Applications Server using syncUC

If fallback solution by means of syncUC is used, execute the following command:

```
syncUC fallback
```

See Section 5.2.16.2, “syncUC Commands”, on page 366 for details.

5.7.2.3 Fallback of External Applications Server through Restoration in the CMP

You wish to upgrade a Media Server Standalone or the Multiple Communication Server Admin to V11 and keep the deployment scenario. If this upgrade is abandoned, you need to execute the following steps to return to the previously installed version.

We assume that a backup by means of the CMP, a backup of the access configuration to the CLM (Customer License Manager) and, if required, a backup of the E/A Cockpit configuration files are available (see step 3 of Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377.)

Installing the operating system

1. Check the version of the installed operating system:

   ```
   cat /etc/SuSE-release
   ```

   Example output:

   ```
   SUSE Linux Enterprise Server 15 (x86_64)
   VERSION = 15
   PATCHLEVEL = 1
   ```

   Using the following command you can check whether the SLES setup medium is available:

   ```
   zypper lr
   ```

   Example output:

   ```
   # | Alias                                          | Name          | Enabled | Refresh
   --+------------------------------------------------+---------------+---------+--------
   1 | SUSE-Linux-Enterprise-Server-11-SP2 11.2.2-1.234| SUSE-Linux-…. | Yes     | No
   ```

2. Consult the documentation of the previously installed version of the OpenScape Applications server to find out which operating system is required.

   a) Install the required operating system if it has not been set up yet.

   b) If the required operating system has already been installed, uninstall the OpenScape Applications and all associated applications.

Installing the OpenScape UC Application

3. Execute the instructions given in the documentation of the corresponding OpenScape Applications server version to set up the previously installed version again.

Restoring using the CMP

4. Using the CMP, restore the data according to the administrator documentation *OpenScape UC Application Configuration and Administration,* section “Backing up and restoring OpenScape System Components”.

Attention: The software version (fix release, patchset and hotfix) of OpenScape Applications server must be the same when backing up and restoring data. Restoring data on a software version different from the one used for backing up data is not supported.

Note: A **Container Configuration files** warning during the restore process does not pose any problem. The demanded actions **WARN Pre/Post Action** and **Please restart the container** are performed after the data restore. **Restoring the CLM access configuration**.

---

5. Open the backed up file `ClmSettings.xml` with the CLM access configuration.
6. Execute the following commands to create a new file `/opt/licenses/clm/ApacheTomcat/ClmSettings.xml` and to update the database:

```
# cd /opt/licenses/clm
# cd /opt/licenses/clm
# bash remoteAccess.sh <IP addr 1>,<IP addr 2>,<IP addr…>,<IP addr n>
```

Attention: All IP addresses listed in the `AllowedClients` field must be restored.

Example:

```
bash remoteAccess.sh 10.235.200.113,10.235.200.28,10.235.65.221
```

Attention: Make sure no blanks are entered between the IP addresses.

The backed up file `ClmSettings.xml` was in a directory “`/opt/siemens/clm/ApacheTomcat`”. It is different from the one that includes the file `ClmSettings.xml` created here.

Restoring the E/A Cockpit configuration files

7. Restore the E/A Cockpit configuration files that may have been backed up.

- SFTP the '.eag' files that were saved to an external location prior to the upgrade to:
  `/opt/siemens/HiPathCA/WebSpace/Portal/webapps/eacockpit-osc/WEB-INF/groups`

  These file contains the Executive Assistant configuration data.

- Restore file ownership and access rights as follows:

```
# cd /opt/siemens/HiPathCA/WebSpace/Portal/webapps/
eacockpit-osc/WEB-INF/groups
# chown sym:sym eagroup*
# chmod 664 eagroup*
```

Start the Applications

8. For the Multiple Communication Server Admin, execute the following command on the application computer to start the MRCP service, the Nuance TTS and the Nuance ASR, if available:

   `/etc/init.d/NSSservice start`

9. Start OpenScape Applications:

   `/etc/init.d/symphoniad start`

10. Wait several minutes before logging on to the CMP.

    If you cannot log on, terminate the OpenScape Applications, restart it, wait several minutes and log on to the CMP.

6 Survival Authority and IPMI Shutdown Agents

There are two parameters that can impact the shutdown agent behavior. Shutdown agent behavior is described in Section 6.1, “Shutdown Agent Overview (Non-Virtual environment)” and Section 6.2, “Shutdown Agent Overview (Virtual environment)”. A brief description of the two parameters follows;

1. **Preferred Node to Takeover** - This parameter indicates which node reacts first to an x-channel failure. The value defaults to node 2. If the x-channel fails, node 2 will be the first to call the shutdown agents in order to "kill" node 1.
2. **Cluster Timeout** - This parameter indicates how long the cluster cross channel (AKA x-channel and cluster interconnect) can be down before the Cluster Manager declares "Changed cross channel state to DOWN" and initiates shutdown agent activity to prevent a split brain condition. If a node to node connection failure is less likely than a server failure (e.g.; in a co-located configuration) the timeout should be set to 10 seconds. If the likelihood of short term connection failures is higher, values of up to 15 seconds are recommended.

These parameters are available as NCPE Installation and Update options. NCPE Installation (Expert and Wizard modes) instructions can be found in Section 2.6, “Creating a Node.cfg File”, on page 50. Refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)” for EZIP information.

OpenScape Voice cluster communication failures are handled by the OSV shutdown agents sa_ipmi and sa_down. The sa_ipmi shutdown agent tries to verify a partner node failure by sending ipmi commands to the mtc controller of the partner node (e.g., IMM, iRMC) while the sa_down shutdown agent communicates with the Survival Authority to decide whether to switchover, shut down or enter StandAlone operation.

Attention: An external (offboard) CMP has a Survival Authority component that is included as part of the CMP Applications software installation. The Standalone Survival Authority snmpreceiver rpm IS NOT intended for installation on a CMP. Installation of the Standalone Survival Authority rpm on a CMP will negatively impact the CMP snmpreceiver functionality.

A snmpreceiver should only be installed in the case of a Standalone Survival Authority as described in Section 6.5, “Installing a Standalone Survival Authority”, on page 395.

The Standalone Service option is available for duplex configurations. If it is enabled, a node that does not receive permission to take over from the Survival Authority stays active (in Standalone Secondary mode). For more information regarding the Standalone Service feature, refer to Section 2.6.2.9, “Stand Alone Service Enabled”, on page 57, of this document or to the OpenScape Voice Vx,

Feature Description documentation, section "Survival Authority" (where *x is the software release version*).

The Survival Authority and IPMI Shutdown Agents (`sa_down` and `sa_ipmi` respectively) are integral parts of OSV and, hence, are installed during the OpenScape Voice image installation.

The Survival Authority shutdown agent (sa_down) employs the node.cfg Survival Authority IP address as the Survival Authority. **The external (offboard) CMP has a Survival Authority component that is included as part of the CMP Applications software installation.**

The IPMI shutdown agent (sa_ipmi) employs the node.cfg RSA IP addresses as the IPMI remote administrative IP addresses.

The sa_ipmi shutdown agent is NOT applicable to a Virtual OSV environment.

The sa_down and sa_ipmi shutdown agents are applicable to non-Virtual OSV environments.

Changes to the shutdown agent configuration files are not recommended. It is a good practice to always consult the next level of support before changing any shutdown agent file configuration. If a customer alters the shutdown agent file configuration, the updated files must be verified after every patch set and MOP installation because the default (expected) settings may be restored.

The USERID:PASSWORD credentials of the sa_ipmi shutdown agent can be changed. Refer to Section 4.4.3, "Changing the User ID and Password for the IMM/iRMC/BMC Account" of this document. This activity should have been addressed during installation of the OSV image Section 2.2.4, "OpenScape Voice Installation Checklist", on page 30 task 11.

To change the sa_ipmi shutdown agent RSA IP addresses employ the IFgui tool in Update mode. Refer to Appendix 13, "Updating the Node.cfg File (Also Known as EZIP)".

If the CMP is not used as a Survival Authority (e.g., because it is co-located with one of the OSV nodes and not the other), a Standalone Survival Authority can be created. Refer to Section 6.3, "Hints on Survival Authority placement", on page 391 and Section 6.8, "Verifying the Shutdown Agents Configuration", on page 409.

6.1 Shutdown Agent Overview (Non-Virtual environment)

Attention: The sa_ipmi and sa_down shutdown agents are applicable to Non-Virtual OSV environments.

Attention: After an x-channel failure, node 1 (default) would wait 38 seconds to be 'killed' by node 2 (the sum of the shutdown agent timeouts). If node 1 was not reset when the 38 second timer expired, node 1 would invoke its shutdown agents in an attempt to 'kill' node 2.

The failover timing is improved. After an x-channel failure, node 1 will only wait 20 seconds to be shutdown (20 seconds is the timeout of the sa_ipmi shutdown agent). If node 1 is not reset after the 20 second timer expires, node 1 invokes its shutdown agents in an attempt to 'kill' node 2.

When the x-channel between the two OSV nodes fails, each OSV node tries to avoid a 'split-brain' situation by power cycling the partner node via the Maintenance Controller interface **(whether Stand Alone Service is enabled or not)**. The sa_ipmi shutdown agent is employed for this purpose.

If this power cycle does not work the nodes block the x-channel and contact the Survival Authority (via the sa_down shutdown agent), which responds to one node with 'takeover' and to the other with 'shutdown'. It is possible that the Survival Authority does not respond at all (example given; due to network issues). The OSV node treats a missing response from the Survival Authority as having received 'shutdown'.

If the StandAlone feature is disabled;

- The node that received 'takeover' switches over as in a partner node failure
- The node that received 'shutdown' (or no response at all) shuts down.

If the StandAlone feature is enabled;

- The node that received 'takeover' becomes 'stand-alone-primary'
- The node that received 'shutdown' (or no response at all) becomes 'stand-alone-secondary'. It is possible that both nodes enter the standalone-secondary state.
- Nodes in standalone do not takeover the virtual IP addresses, especially all signaling IPs of the partner node, which is a functional restriction for L2-geo-separation. The reason is that a node in a StandAlone mode has to assume that the partner node is active. In standalone, both nodes support all subscribers. It does not matter where the registration took place, since

registrations are replicated between the nodes. Of course, new registrations in standalone cannot be replicated. This is done as soon as the x-channel is restored.

StandAlone Service is the default when node.cfg parameter **Node Separation = separate** is selected.

If Node Separation = none is selected in the node.cfg **then Stand Alone service must be enabled manually.**

The Stand Alone feature can be configured while creating the node.cfg file when preparing to install an OSV cluster (refer to Section 2.6.2.9, “Stand Alone Service Enabled”, on page 57.)

For clusters already in-service, if it is necessary to change the Stand Alone Service feature refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”

6.2 Shutdown Agent Overview (Virtual environment)

Attention: Only the sa_down shutdown agent is applicable to a Virtual OSV environment.

Attention: After an x-channel failure, node 1 (default) would wait 16 seconds to be 'killed' by node 2 (the sum of the shutdown agent timeouts). If node 1 was not reset when the 16 second timer expired, node 1 would invoke its shutdown agents in an attempt to 'kill' node 2.

The failover timing is improved. After an x-channel failure, node 1 will only wait 5 seconds to be shutdown. If node 1 is not reset after 5 seconds, node 1 invokes its shutdown agents in an attempt to 'kill' node 2.

When the x-channel between the two OSV nodes fails, each OSV node tries to avoid a 'split-brain' situation by contacting the Survival Authority (via the sa_down shutdown agent). Survival Authority responds to one node with 'takeover' and to the other with 'shutdown'. By default, node 2 contacts Survival Authority first and most likely node 2 gets back the response from Survival Authority first and becomes the standalone-primary node. It is possible that the Survival Authority does not respond at all (example given; due to network issues). The OSV node treats a missing response from Survival Authority as having received 'shutdown'.

If the StandAlone feature is disabled:

- The node that received 'takeover' switches over as in a partner node failure

- The node that received 'shutdown' (or no response at all) shuts down.

If the StandAlone feature is enabled:

- The node that received 'takeover' becomes 'stand-alone-primary'
- The node that received 'shutdown' (or no response at all) becomes 'stand-alone-secondary'. It is possible that both nodes enter the standalone-secondary state.
- Nodes in standalone do not takeover the virtual IP addresses, especially all signaling IPs of the partner node, which is a functional restriction for L2-geo-separation. The reason is that a node in a StandAlone mode has to assume that the partner node is active. In standalone, both nodes support all subscribers. It does not matter where the registration took place, since registrations are replicated between the nodes. Of course, new registrations in standalone cannot be replicated. This is done as soon as the x-channel is restored.

For the StandAlone Service feature to be available in a virtual environment the node.cfg parameter **Node Separation = separate** must be selected. **The Stand Alone Service is enabled by default in this configuration.**

The Stand Alone feature can be configured while creating the node.cfg file when preparing to install an OSC Voice cluster (refer to Section 2.6.2.9, “Stand Alone Service Enabled”, on page 57.

For clusters already in-service, if it is necessary to change the Stand Alone Service feature refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”.

6.3 Hints on Survival Authority placement

For the Survival Authority to be useful, it cannot be placed within a failure unit that is common to either node of the cluster. A simple example of a common failure unit would be a node and the Survival Authority sharing a common power source.

Another example for this rule; if the two nodes are in different locations (the meaning of geo redundancy), the Survival Authority should be in a third location. The Survival Authority has to survive a disaster that disables one location in order to support the failover of the surviving node in the other location.

If both nodes are in the same data center, the Survival Authority can be in that data center, but not on a server hosting one of the nodes. There is still a potential for a common failure unit in this configuration.

The OSV cluster with the Stand Alone Service enabled may be considered an exception to this rule. With Stand Alone service enabled it may be ok to co-locate the Survival Authority with one OSV node, if the OSV node is in the same failure unit as the CMP or the provisioning systems. If the provisioning system fails

together with the OSV node and the Survival Authority, the surviving node transitions to the standalone-secondary operation mode. This mode means call processing, but blocking of all provisioning. This could be acceptable, because the provisioning system is not functioning either.

6.4 Survival Authority on the CMP

The Survival Authority function can be provided by the CMP or by a Standalone Survival Authority.

If the CMP cannot be used as Survival Authority, because it may fail together with one of the OSV nodes, the Standalone Survival Authority can be installed. Refer to Section 6.3, “Hints on Survival Authority placement”, on page 391 and Section 6.5, “Installing a Standalone Survival Authority”, on page 395.

The Standard Duplex Large, Standard Duplex Small and Multiple Communications Server Admin applications deployments include a snmpreceiver as part of the Applications software installation. **The snmpreceiver allows these CMP deployments to act as a Survival Authority for their monitored OSV systems.**

Attention: Installation of the Standalone Survival Authority rpm on a CMP will negatively impact the CMP snmpreceiver functionality.

A snmpreceiver should only be installed in the case of a Standalone Survival Authority as described in Section 6.5, “Installing a Standalone Survival Authority”, on page 395.

For the CMP to function as the Survival Authority of an OpenScape Voice cluster, the CMP needs to manage this cluster and the cluster needs to be configured with the CMP IP address as the Survival Authority.

The Survival Authority can be configured while creating the node.cfg file when preparing to install an OSC Voice cluster (refer to Section 2.6.2.9, “Stand Alone Service Enabled”, on page 57).

For clusters already in-service, if it is necessary to change the Survival Authority IP address in the OpenScape Voice nodes, refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. If the customer cannot accept system downtime, the voice server Survival Authority can also be configured via the Cli. The result of a successful Cli execution is the Survival Authority configuration files and the firewall (packet filtering rules) of the OpenScape Voice server are updated. **The node.cfg file on the OSV server will not be updated with the 'new' Survival Authority IP address.**

a) To execute the Survival Authority update with Cli, as user *root* on the voice server primary node, issue the following:

```
# su - srx -c "startCli -x"
```

b) Log in as user **sysad**.

c) At the CLI> prompt, run the following commands. These two commands remove packet filter rules that are not needed. Responses indicating the packet filter rules do not exist are acceptable.

```
pktFltrRulesRemove "SnmpStandaloneSurvAth1"
pktFltrRulesRemove "SnmpStandaloneSurvAth2"
```

These names are examples. The packet filtering rule may exist with a different name(s). A review of the OSCV packet filtering rules is required if you would like to ensure the proper rule is removed. The packet filtering rule of interest would have a 'Description' field similar to this; "SNMP from Survival Authority to admin IP of each node".

Any questions should be addressed to your next level of support before proceeding.

The packet filtering rules can be displayed with Cli, the log collected and reviewed.

From 'expert' Cli;

CLI>**pktfltrrulesquery ""**

From Cli Menu mode, select these options from the main menu;

- 6 Application-level Management
- 8 Network Element Security Management
- 4 Packet Filter Rules Security Management
- 4 Display

Note: Hint for Cli Menu mode: Use the default name (blank-no entry) and 10 rules at a time will be displayed. Answer yes to the prompt asking if the display should Continue. When the Packet Filter Rules Security Management (methods) menu is presented the packet filtering rule display is complete.

---

d) The Survival Authority configuration is updated and the voice server firewall is opened for the Standalone Survival Authority with the '**mainsetsurvivalauthority**' command (these commands **are NOT** case sensitive). At the CLI> prompt, run the following command (replace <HOST IP> with the IP address of the Survival Authority:

Attention: Execution of the mainsetsurvivalauthority command does not update the "Survival Authority" IP in the node.cfg file (of either node). To update the node.cfg file "Survival Authority" IP an IFgui Update (EZIP) must be performed. More information on the EZIP can be found in Appendix 13, “Updating the

Node.cfg File (Also Known as EZIP)". After reviewing Appendix 13 any questions should be addressed to your next level of support.

```
mainSetSurvivalAuthority "<HOST IP>"
```

Note: If a rule with the same properties as that of the packet filtering rule being created already exists the packet filtering rule will not be created. The command response will indicate as much and identify the already existing packet filtering rule.

---

e) To display the 'new' Survival Authority IP execute the following command;

```
mainGetSurvivalAuthority
```

f) To verify the 'new' Survival Authority configuration refer to Section 6.8, "Verifying the Shutdown Agents Configuration", on page 409.

Note: Execution of the **mainsetsurvivalauthority** command **does not update the "Survival Authority" IP in the node.cfg file** (of either node). After verifying the shutdown agents, update the node.cfg file "Survival Authority" IP with an IFgui Update (EZIP) action. More information on the EZIP can be found in Appendix 13, "Updating the Node.cfg File (Also Known as EZIP)" After reviewing Appendix 13 any questions should be addressed to your next level of support.

6.5 Installing a Standalone Survival Authority

Attention: An external (offboard) CMP has a Survival Authority component that is included as part of the CMP Applications software installation. The Standalone Survival Authority snmpreceiver rpm **IS NOT** intended for installation on a CMP. Installation of the Standalone Survival Authority rpm on a CMP will negatively impact the CMP snmpreceiver functionality.

If you prefer to use a third machine as the Survival Authority (Standalone Survival Authority), instead of your External Applications Server, these requirements must be met:

- Install the Standalone Survival Authority on a third SLES 15 machine. It is recommended the Standalone Survival Authority be installed in advance of the OpenScape Voice installation so the verification of the OpenScape Voice shutdown agents can take place as soon as time permits.
- The firewall on the third machine must either be disabled or packet filter rules need to be created on the third machine in order to allow the required SNMP messages to be exchanged between the Standalone Survival Authority and the standard duplex nodes (co-located or geographically separated).
- Configure the needed packet filter rules on your duplex voice server for the Standalone Survival Authority application.
- **Remember**, the Standalone Survival Authority listens on the standard SNMP trap port (162) and should not be installed on any server with an already existing SNMP trap process because the existing SNMP function or the Standalone Survival Authority receiver may fail (e.g.; the Survival Authority may not respond to takeover requests).

The minimum hardware, software, and performance requirements for the Standalone Survival Authority are as follows:

- Intel or AMD processor
- SLES 15
- Minimum of 500 MB RAM
- Non-volatile storage (for example: disk or compact flash)
- One or more Ethernet ports

- Enough performance that the time between SNMP trap and corresponding SET is below two seconds under maximum PC load.

Note: Maximum load is defined by the customer based on the customer-provided applications that might be installed on the PC in addition to the Survival Authority (the stand-alone CLM may also be installed on this PC).

6.5.1 Installing the Java Runtime Environment

The *snmpreceiver* needs Java runtime environment (JRE) version equal to or greater than V1.7. Install it using the yaST2 tool by following the steps below.

Note: The use / installation of any other java application in parallel with the Survival Authority (snmpreceiver) is not supported and as a result the snmpreceiver will not start.

Note: It is recommended to install the highest available JRE. If both the V1.7 and V1.8 JRE are available, then install the V1.8 JRE version.

Note: The java packages provided by SLES 15 and generally the openjdk headless java packages can be used to run java applications that do not require a GUI, and therefore are suitable for running the survival authority.

These instructions were written based on user actions executed with a server running SLES 15 SP6.

1. Run yast2 with the command:

   ```
   # yast2
   ```

2. Select **Software** and then **Software Management**. The **Search** tab is displayed.
3. Under **Search In**, select the **Name**, **Summary**, **Keywords** and **Provides** check boxes.
4. Ensure **Search Mode = Contains** and the **Case Sensitive** checkbox is NOT selected.
5. Type **jre** in the box located to the left of the **Search** button. Press the Enter key to trigger the search.
6. Select the latest available JRE from the search results. Select the **Accept** button.

7. If prompted, select **Continue** to install any Automatic Changes (dependent packages).
8. After the successful JRE install, exit the YaST Control Center.

   The JRE package should resolve any dependencies - any JRE greater than or equal to 1_7 is acceptable.

6.5.2 Minimal Firewall Recommendations for the Standalone Survival Authority

---

Note: In order to provide for the Standalone Survival Authority machine functionality it is recommended that its firewall is enabled and its firewall rules are configured. **A minimal configuration to allow the Standalone Survival Authority functionality follows.** The actual firewall configuration is dictated by local policy and the server's purpose in the network. Applicable documentation should be referenced to ensure the server is hardened as recommended (e.g.; *OSV Security Checklist Planning Guide*). Experience with 'yast' operations/ actions is a prerequisite for this procedure.

---

a) On the Standalone Survival Authority machine, run yast2 with the command:

   # **yast2**

   Note: For assistance with navigating the YaST Control Center, refer to the Help dialog listed on each page.

   ---

b) From the **YaST Control Center** window, select the **Security and Users** dialog, and then **Firewall**.

c) From the **Firewall Configuration** dialog, select **Allowed Services**.

d) On the **Firewall Configuration: Allowed Services** page, select **External Zone** for **Allowed Services for Selected Zone**. For the **External Zone,** allow **Secure Shell Server** and the specified snmp ports as follows;

   - For **Service to Allow** select **Secure Shell Server**.
   - Tab through to the **Add** action to add **Secure Shell Server**.
   - In the **Allowed Service** table **Secure Shell Server** should be present.
   - Select the **Advanced** dialog; in the **Additional Allowed Ports** table make the following selections:

TCP Ports: **161 162**
UDP Ports: **161 162 8163**
RPC Ports: <Leave blank>
IP Protocols: <Leave blank>

- Select the **OK** button and you are returned to the **Firewall Configuration: Allowed Services window**.
- On the **Firewall Configuration: Allowed Services** window, select **Protected Firewall from Internal Zone**.

This completes the selections for the External Zone.

e) On the **Firewall Configuration: Allowed Services** page**,** select **Internal Zone** for **Allowed Services for Selected Zone**. For the **Internal Zone** make these selections;

- For **Service to Allow** select **Secure Shell Server.**
- Tab through to the **Add** action to add **Secure Shell Server**.
- In the **Allowed Service** table **Secure Shell Server** should be present.
- Select the **Advanced** dialog; in the **Additional Allowed Ports** table make the following selections:

TCP Ports: **161 162**
UDP Ports: **161 162 8163**
RPC Ports: <Leave blank>
IP Protocols: <Leave blank>

- Select the **OK** button and you are returned to the **Firewall Configuration: Allowed Services window**.

This completes the selections for the Internal Zone.

f) After the **Internal Zone** selections are complete, select **Next** from the **Firewall Configuration: Allowed Services** window.

g) From the **Firewall Configuration: Summary** window, select **Finish**

h) From the **YaST Control Center** window, select the **Security and Users** dialog, and then **Firewall**

i) From the **Firewall Configuration: Allowed Services** window, navigate back to the firewall **Start-Up** dialog.

j) In the **Firewall Configuration: Start-Up** window;

- Select **Enable Firewall Automatic Starting**
- Select **Start Firewall Now**

- Select **Next**
- Select **Finish**

k) Exit the YaST Control Center.

6.5.3 Installing the Standalone Survival Authority

Install the Standalone Survival Authority onto a third SLES 15 SP6 machine by following the steps below:

1. The 'BasePackage' ISO of the latest released OpenScape Applications version must be downloaded. Mount the file (or installation media), change directory to the mount point, resolve the snmpreceiver rpm name/version, and install the snmpreceiver;

   ```
   # mount -o loop
   <filename_of_BasePackage_iso_distribution>.iso /mnt
   # cd /mnt/x86_64/
   # ll snmp*
   # rpm -i snmpreceiver-<version>.rpm
   ```

   Where <version> = the snmpreceiver version.

   Examples given;

   ```
   # mount -o loop OpenScapeUcSuiteApps-BasePackage-V10R6.0.0-
   030000.iso /mnt
   # cd /mnt/x86_64/
   # cd /mnt/x86_64/
   # ll snmp*
   -r--r--r-- 1 root root 909340 Jun 1 12:13 snmpreceiver-9-
   0.06.x86_64.rpm
   # rpm -ivh --replacefiles --replacepkgs snmpreceiver-9-
   0.06.x86_64.rpm
   ```

   The Standalone Survival Authority daemon will start automatically.

   Note: It would be a good practice to unmount the "BasePackage" ISO at this time;

   ```
   # cd /
   # umount /mnt
   ```

   ---

2. The Standalone Survival Authority can be configured to specific IP, read/write communities and versions of multiple OSV nodes.

   a) There is a configuration file in the Survival Authority dir (*/opt/siemens/survival_authority*) named assistant. The default file configuration is as follows:

   ```
   export HIPATH8000NODE1=10.1.122.10
   export SNMPREAD1=public
   export SNMPWRITE1=public
   export VERSION1=V5.00.02.ALL.11
   export NAT1=true


   export HIPATH8000NODE2=10.1.122.20
   export SNMPREAD2=public
   export SNMPWRITE2=public
   export VERSION2=V5.00.01.ALL.11
   ```

```
export HIPATH8000NODE3=10.11.32.10
export SNMPREAD3=public
export SNMPWRITE3=public
export VERSION3=V4.00.02.ALL.11
export NAT3 = true


export HIPATH8000NODE4=10.11.38.10
export SNMPREAD4=public
export SNMPWRITE4=public
export VERSION4=V4.00.01.ALL.11
export NAT4 = true
```

Attention: For an explanation of the NAT parameter, refer to Section 6.6, “Configuring the Standalone Survival Authority for a Network Address Translation (NAT) case”, on page 405.

b) The Survival Authority can be configured by editing the entries in this file.

Change the HIPATH8000NODE1 parameter value to the IP address of Node1 (<node_1_ip> in node.cfg) and the HIPATH8000NODE2 parameter value to the IP address of Node2 (<node_2_ip> in node.cfg). Enter the appropriate software version for the nodes being added.

There is no need to add the two lines referring to the community strings for Survival Authority (SNMPREAD, SNMPWRITE). Below is an example from OSV V7 showing that 'Network Address Translation' is not required in this example);

```
export HIPATH8000NODE1=10.235.60.6
export VERSION1=V7.00.01.ALL.07


export HIPATH8000NODE2=10.235.60.7
export VERSION2=V7.00.01.ALL.07
```

Attention: If no other entries are required it is a good practice to remove unnecessary export parameter entries. For the step 2b case, if only the V7 entries were required then the entries associated with export entry '3' (HIPATH8000NODE3, SNMPREAD3, SNMPWRITE3, VERSION3 and NAT3) and export entry '4' (HIPATH8000NODE4, SNMPREAD4, SNMPWRITE4, VERSION4 and NAT4) should be removed before saving the assistant file.

For example, the final content of the assistant file with only a V7 Survival Authority configuration would be;

export HIPATH8000NODE1=10.235.60.6
export VERSION1=V7.00.01.ALL.07

```
export HIPATH8000NODE2=10.235.60.7
export VERSION2=V7.00.01.ALL.07
```

---

step c) of this section describes configuring additional nodes in the assistant file.

c) Additional nodes can be configured by entering additional sets of entries to the file. Be careful to;

- Maintain the numbering convention as indicated for the export parameter entries. E.g.; for the case of the assistant file from step 2b) the next set of nodes entered would employ '3' and '4' for the export parameter references.
- Enter the appropriate software version of the nodes being added. In this example a voice server cluster has been added to the *assistant* file Survival Authority configuration. This example configuration includes a Network Address Translation. The default for the NAT parameter is false. If the NAT parameter is not present it is considered false. More details on the NAT configuration is found in Section 6.6, “Configuring the Standalone Survival Authority for a Network Address Translation (NAT) case”, on page 405

```
export HIPATH8000NODE1=10.235.60.6
export VERSION1=V7.00.01.ALL.07


export HIPATH8000NODE2=10.235.60.7
export VERSION2=V7.00.01.ALL.07

export HIPATH8000NODE1=10.239.108.21
export SNMPREAD3=public
export SNMPWRITE3=public
export VERSION3= V4.00.01.ALL.40
export NAT3 = true

export HIPATH8000NODE4=10.11.208.22
export SNMPREAD4=public
export SNMPWRITE4=public
export VERSION4= V4.00.01.ALL.40
export NAT4 = true
```

3. After the Survival Authority configuration, restart the daemon by running the following command:

   `#systemctl start snmpreceiver`

   The daemon status can be verified with the following command - the expected status is "**running**":

   `#systemctl status snmpreceiver`

4. After successful installation of the Standalone Survival Authority, configure the OpenScape Voice packet filtering rules as follows:

Attention: IF the OpenScape Voice system was installed with the node.cfg "survival authority" parameter IP equal to that of the Standalone Survival Authority IP THEN step 4 may be used as a guide to review the Survival Authority configuration. Please remember to verify the Survival Authority configuration (refer to Section 6.8, “Verifying the Shutdown Agents Configuration”, on page 409).

If the OpenScape Voice is in need of an update to match a new Standalone Survival Authority IP proceed as follows;

---

a) Obtain the IP address of the Standalone Survival Authority system. From a command line on the Standalone Survival Authority run:

`# ifconfig`

In the command output result, the “eth0” interface IP address is the IP address of the Standalone Survival Authority system. Use this IP address in place of <HOST IP> for the command listed in step 4e).

b) To complete the configuration, as user *root* on the voice server primary node, issue the following:

`# su - srx -c “startCli -x”`

c) Log in as user *sysad*.

d) At the CLI> prompt, run the following commands. These two commands remove packet filter rules that are not needed. Responses indicating the packet filter rules do not exist are acceptable.

`pktFltrRulesRemove "SnmpStandaloneSurvAth1"`

`pktFltrRulesRemove "SnmpStandaloneSurvAth2"`

These names are examples. The packet filtering rule may exist with a different name(s). A review of the OSCV packet filtering rules is required if you would like to ensure the proper rule is removed. The packet filtering rule of interest would have a 'Description' field similar to this; "SNMP from Survival Authority to admin IP of each node".

Any questions should be addressed to your next level of support before proceeding.

The packet filtering rules can be displayed with Cli, the log collected and then reviewed.

1. From 'expert' Cli;

`CLI>pktfltrrulesquery ""`

2. From Cli Menu mode select these options from the main menu;
   - 6 Application-level Management
   - 8 Network Element Security Management
   - 3 Packet Filter Rules Security Management
   - 4 Display

Note: Hint for Cli Menu mode: Use the default name (blank-no entry) and 10 rules at a time will be displayed. Answer yes to the prompt asking if the display should Continue. When the Packet Filter Rules Security Management (methods) menu is presented the packet filtering rule display is complete.

---

e) It is recommended the **IFgui Update (EZIP)** tool is used to update the **"Survival Authority" IP in the node.cfg file** (of both nodes) and make any other administrative and operating system updates that are required. More information on the EZIP can be found in Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”.

IF the situation does not permit an **IFgui Update (EZIP)** action at this time THEN execution of the **mainsetsurvivalauthority** command is an option. The command is not case sensitive. The Survival Authority configuration is updated and the voice server firewall is opened for the Standalone Survival Authority with the '**mainsetsurvivalauthority**' command (using the syntax indicated). The <HOST IP> should be replaced with the IP address of the Standalone Survival Authority identified in step 4a) on page 403. The expected result is "**Operation successful**":

Attention: Execution of the **mainsetsurvivalauthority** command does not update the **"Survival Authority"** IP in the node.cfg file (of either node). **T**o update the node.cfg file **"Survival Authority"** IP an IFgui Update (EZIP) must be performed. This update will not cause an outage. More information on the EZIP can be found in Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. After reviewing Appendix 13 any questions should be addressed to your next level of support.

```
# mainSetSurvivalAuthority "<HOST IP>"
```

Note: Hint for the mainsetsurvivalauthority command: If a rule with the same properties as that of the packet filtering rule being created already exists the packet filtering rule will not be created. The command response will indicate as much and identify the already existing packet filtering rule.

Note: The **maingetsurvivalauthority** command will list the current Survival Authority IP. An example follows;

```
# mainGetSurvivalAuthority ""
```

Note: After installation of the Standalone Survival Authority, verify the Survival Authority configuration (refer to Section 6.8, “Verifying the Shutdown Agents Configuration”, on page 409).

Note: Execution of the **mainsetsurvivalauthority** command **does not update the "Survival Authority" IP in the node.cfg file** (of either node). After verifying the shutdown agents, update the node.cfg file "Survival Authority" IP with an IFgui Update (EZIP) action. This update will not cause an outage. More information on the EZIP can be found in Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. After reviewing Appendix 13 any questions should be addressed to your next level of support.

6.6 Configuring the Standalone Survival Authority for a Network Address Translation (NAT) case

Attention: This section addresses the **Standalone Survival Authority** Network Address Translation (NAT) case only. **This procedure can not be applied on an external (offboard) applications server.**

Some customers have their **Standalone Survival Authority** placed in the network behind a device that performs Network Address Translation (NAT). This translation will alter the IP address of the OSC Voice server node delivering a takeover request to the **Standalone Survival Authority**. This IP change will cause the Survival Authority dialog with the **Standalone Survival Authority** to fail.

To provide for this scenario the file /opt/siemens/survival_authority/assistant can be updated to include the ‘NAT’ parameter. The line ‘export NAT=true' will signify that the node IP address is transformed by a NAT-service. This feature only applies to a static NAT, a NAT that replaces the OSV node IP address with an 'external' IP address.

The default for the NAT parameter is false. If the NAT parameter is not present it is considered false.

The 'HIPATH8000NODE' IP address must be the real/actual node admin IP of the OSV node(s), not the NAT’d IP.

Remember to maintain the numbering convention for the export parameter entries.

Example assistant file with the NAT = true:

```
export HIPATH8000NODE1=10.49.109.17
export NAT1=true
export VERSION1=V5.00.01.ALL.11
export HIPATH8000NODE2=10.49.109.18
export NAT2=true
export VERSION2=V5.00.01.ALL.11
```

Note: There is no need to add the two lines referring to the community strings for Survival Authority (SNMPREAD, SNMPWRITE).

6.7 Updating the Standalone Survival Authority

Note: It is expected that the Standalone Survival Authority is already running SLES 12 SP5 or SLES 15 SP6 before the rpm is updated.

This section is intended to provide instructions for updating the Standalone Survival Authority rpm.

It is a good practice to verify the Survival Authority configuration before proceeding. Refer to Section 6.8, “Verifying the Shutdown Agents Configuration”, on page 409. For this case we are particularly concerned with the Survival Authority shutdown agent (sa_down) test result.

This procedure should be continued only if the 'sa_down' test result returns success.

A list of the OpenScape Voice systems this StandAlone Survival Authority supports can be found in the file named 'assistant' (located on the StandAlone Survival Authority in /opt/siemens/survival_authority).

It is expected for the following commands to be executed as the *root* user.

1. In the OpenScape Applications Release Note for the latest Generally Available Applications software, a section titled "Software releases" indicates the latest approved snmpreceiver version.

   Alternatively, the 'BasePackage' ISO of the latest released OpenScape Applications version can be downloaded. Mount the file (or installation media), change directory to the mount point, and resolve the snmpreceiver rpm name/version.

   ```
   # mount -o loop <filename_of_BasePackage_iso_distribution>
   .iso /mnt
   # cd /mnt/x86_64/
   # ll snmp*
   ```

   Example given;

   ```
   # mount -o loop OpenScapeUcSuiteApps-BasePackage-V10R6.0.0-
   030000.iso /mnt
   # cd /mnt/x86_64/
   # ll snmp*
   -r--r--r-- 1 root root 909340 Jun 1 12:13 snmpreceiver-9-
   0.06.x86_64.rpm
   ```

2. Verify the version of the snmpreceiver package already installed;

   ```
   # rpm -qa | grep -i snmpreceiver
   ```

The version of the installed snmpreceiver package is presented. Example: snmpreceiver-1-5.04

Note: If the installed snmpreceiver is already at the appropriate version level (or higher), do not proceed; otherwise, continue with the update procedure. Continue with steps 3 through 12 below.

---

3. IF the snmpreceiver requires update THEN copy the snmpreceiver package to the Standalone Survival Authority. The snmpreceiver is included in the 'BasePackage' ISO of the Applications distribution. Use the example given in step 1 as a guide for retrieving the snmpreceiver package.
4. Backup the 'Applications' configuration file by copying the *assistant* file to a temporary storage location on the server. This example uses the /tmp directory;

   # cd /opt/siemens/survival_authority

   # cp -p assistant /tmp/assistant.bak
5. Stop the SNMP receiver daemon.

   # /etc/init.d/snmpreceiverd stop

   The expected response is '**stopping survival authority done'**
6. Verify the daemon is stopped.

   #systemctl start snmpreceiver

   The expected response is '**dead'**
7. Uninstall the snmpreceiver package.

   # rpm -e --allmatches snmpreceiver

   The expected response is '**stopping survival authority done'**
8. From the path where the snmpreceiver package was copied, install the new snmpreceiver package.

   # rpm -ivh --replacefiles --replacepkgs snmpreceiver-<version_number>.rpm

   It is expected the rpm is successfully installed.
9. Restore the backed up 'Applications' configuration file.

   # cd /opt/siemens/survival_authority

   # cp -p /tmp/assistant.bak .

   # cp assistant.bak assistant

   Remember to maintain the numbering convention for the export parameter entries.

   The OSV version value from parameter "**export VersionX**" in the assistant file has to match the version of parameter "**srx_build_id**" from the corresponding OSV's node.cfg.

10. Start the SNMP receiver daemon.

    `# /etc/init.d/snmpreceiverd start`

    The expected response is '**starting survival authority running'**

11. Verify the daemon status.

    `# /etc/init.d/snmpreceiverd status`

    The expected response is '**`running`**'

12. After installation of the Standalone Survival Authority, verify the Survival Authority configuration (refer to Section 6.8, "Verifying the Shutdown Agents Configuration", on page 409).

6.8 Verifying the Shutdown Agents Configuration

Attention: This text applies if you reached this section after employing the **mainsetsurvivalauthority** to change your Survival Authority IP. **The mainsetsurvivalauthority command does not update the "Survival Authority" IP in the node.cfg file** (of either node). After verifying the shutdown agents, update **the node.cfg file(s) "Survival Authority" IP with an IFgui Update (EZIP) action**. This update will not cause an outage. More information on the EZIP can be found in Appendix 13, "Updating the Node.cfg File (Also Known as EZIP)". After reviewing Appendix 13, any questions should be addressed to your next level of support.

Attention: An external (offboard) CMP has a Survival Authority component that is included as part of the CMP Applications software installation. The Standalone Survival Authority snmpreceiver rpm **IS NOT** intended for installation on a CMP. Installation of the Standalone Survival Authority rpm on a CMP will negatively impact the CMP snmpreceiver functionality.

The SNMPReciever should only be installed in the case of a Standalone Survival Authority as described in Section 6.5.3, "Installing the Standalone Survival Authority", on page 400.

Each node tests the Survival Authority function every 10 minutes and will report a Survival Authority test failure with a major communication alarm. RapidStat also performs sa_ipmi and sa_down shutdown agent tests in addition to shutdown agent configuration checks. It is recommended that RapidStat be configured as a cronjob to schedule daily RapidStat health checks. Refer to the *OpenScape Voice Vx Service Documentation, section "How to Configure RapidStat as a Cronjob" for details* (where *x is the software release version*).

Use the following sections to verify the shutdown agent configuration and to monitor Survival Authority activity:

- Section 6.8.2, “Monitoring the Shutdown Agents From the Nodes”, on page 412
- Section 6.8.3, “Examples of sa_down.log and sa_ipmi.log Output”, on page 413
- Section 6.8.4, “Activity Log for Survival Authority Action”, on page 414

6.8.1 Shutdown Agent Verification, Debugging and Data Collection from the OpenScape Voice 'tools' Menu

Overview:

The section describes an OpenScape Voice command line interface that can verify the shutdown agents have been configured correctly or gather logs relating to the shutdown agents. These logs would be collected to aid in debugging shutdown agent problems.

Example displays results of option 53 and 84 are presented in Appendix 23, “Shutdown Agent Failover Model and Data Collection displays”. Links back to this section will be provided at the end of the appendix.

6.8.1.1 Accessing the 'tools' menu

1. Logon to the OpenScape voice node as user srx (or su - srx).
2. Type "tools" and a display similar to the following is presented;

```
srx@srxl41a:[/unisphere/srx3000/srx] #358
$ tools

################################################################################
                    Welcome to the Hipath 8K Tools
          These tools are dangerous! They can affect call processing
           Do not run if you are not familiar with the side effects

################################################################################
Main Menu :
   1. UCE context util - displays UCE contexts (ctxutil)
   2. RDAL shared memory - displays and changes CAC bandwidth and call counts (rdalTool)
   3. SIP-SM dump - displays and accesses SIP SM shared memory (sipsmdump)
   4. FQDN resolver - displays and manages the FQDN black list (fqdnresTool)
   5. CSTA SM dump non-interactive - displays CSTA SM shared memory (cstasmdump)
   6. CSTA SM dump interactive - displays CSTA SM shared memory (cstasmdump)
   7. MLHG print - displays MLHG shared memory (mlhgprint)
   8. NDAL memory display - numbering modification and CAC policies shared memory
(ndalMemDisplay)
   9. OMM print - displays OMM shared memory (ommprint)
  30. CDR decode - decodes CDR into readable text format (cdrdecode)
  31. XLA verify - displays translation information for calling/called numbers (xlaverify)
```

32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)
33. XDM SM Display - displays the content of the XDM Shared Memory (XdmShmDisplay.exe)
50. RTP parameter delta - compares default vs. current RTP parameters
51. Security Model - displays the network packets rules
52. Network model - displays all network connections
53. Failover model - displays the network configuration for survivability
80. System information - collects low-level system information to diagnose platform issues
81. System information - collects SPT and RU log files, traces and data
82. System information - collects SMU and EZIP log files and data
83. System information - collects DB log files and data
84. System information - collects Survival Authority log files and data
99. Exit

Note: The user will be prompted for the root user password after selecting either of the following options.

6.8.1.2 Option 53. Failover Model - Displays the Network Configuration for Survivability

It is only necessary to run the Failover model verification/check from one node because this option will verify/check both nodes of an OpenScape Voice cluster.

Choose option 53 to verify the shutdown agents have been configured and are functioning correctly. The following checks are performed;

- rsa/imm configuration - Tests the configuration for failover
- rsa/imm Reachability test.[icmp] - Tests the ping for each of the interfaces.
- security rules [iptables] - Check if the security rules to Survival Authority are present.
- Contact BMC test [ipmi] - Tests the ipmi protocol from both nodes.
- Contact Survival Authority test[snmp] - Check Survival Authority communication.

6.8.1.3 Option 84. System Information - Collects Survival Authority Log Files and Data

Choose option 84 to collect info related to debugging. This option will collect data from both nodes and place the collected data of both nodes in a tar ball (on the node from which the data collection was initiated).

If the tool can not contact the other node a message advising as much will be presented on the terminal. In that case the tool should be invoked on the partner node also. The data will have to be collected from each node in this case.

Example displays results of option 53 and 84 are presented in Appendix 23, “Shutdown Agent Failover Model and Data Collection displays”. Links back to this section will be provided at the end of the appendix.

6.8.2 Monitoring the Shutdown Agents From the Nodes

Attention: The sa_ipmi test is NOT applicable to a Virtual OpenScape Voice environment. The sa_down test is applicable to Virtual and non-Virtual OpenScape Voice environments.

As *root* user, perform a manual Survival Authority test with the following command(s):

The binaries to test the sa_ipmi and sa_down are located in path /opt/SMAW/SMAWhaext/bin.

For a sa_ipmi test:

```
sa_ipmi -d -s <the partner node hostname>
```

For a sa_down test:

```
sa_down -d -s <the partner node hostname>
```

The ‘`-s`’ option invokes a test of the Survival Authority function.

The ‘`-d`’ option switches logging to the debug mode (which writes test results to the *sa_ipmi.log or sa_down.log* files). The *sa_ipmi.log and sa_down.log* files are located at */var/opt/SMAWhaext/log*. The log files should be reviewed for information regarding the cause of a Survival Authority test failure.

The `<the partner node hostname>` is the hostname of the cluster partner node.

Examples of the commands are as follows:

Attention: The sa_ipmi test is NOT applicable to a Virtual OpenScape Voice environment. The sa_down test is applicable to Virtual and non-Virtual OpenScape Voice environments.

```
root@bocast4a:[/opt/SMAW/SMAWhaext/bin] #424
# ./sa_ipmi -s -d bocast4b

root@bocast4a:[/opt/SMAW/SMAWhaext/bin] #426
# ./sa_down -s -d bocast4b
```

6.8.3 Examples of sa_down.log and sa_ipmi.log Output

An example of the *sa_down.log* output for a successful sa_down shutdown agent test follows. The actual sa_down test command was executed in a different session window (reference command example listed in Section 6.8.2, “Monitoring the Shutdown Agents From the Nodes”, on page 412). Direct questions regarding the content of a *sa_down.log* file to your next level of support. The “NOTICE sa_down: do_test: SaQuery returned success.“ is the expected result of a successful sa_down test.

Note: The ‘tail’ job indicated will initially print the last ten lines in the *sa_down.log* file. To gain separation from these ten lines and your test output, press the Enter key 4 or 5 times.

Note: The sa_down test is applicable to Virtual and non-Virtual OpenScape Voice environments. The sa_ipmi test is NOT applicable to a Virtual OpenScape Voice environment.

This log was collected from the node of an OpenScape Voice cluster at software level V7.00.01.ALL.11_PS0004.

.

```
sysad@fsc201:[/home/sysad] #58
$ tailf /var/opt/SMAWhaext/log/sa_ipmi.log

2012-03-24 16:15:30.560  29470 $Header: SA_ipmi.c /main/17 2012/01/30 13:25:59 try $
2012-03-24 16:15:30.560  29470 global test-Parameter setting: TestLocalStatus
2012-03-24 16:15:30.560  29470 global Parameter setting for testLocal: 1
2012-03-24 16:15:30.560  29470 global Parameter setting for testLocal: 1
2012-03-24 16:15:30.560  29470 global Parameter setting: 'encryptedPassword' 'true'
2012-03-24 16:15:30.560  29470 global test-Parameter setting: useCycle
2012-03-24 16:15:30.560  29470 global Parameter setting for testLocal: 1
2012-03-24 16:15:30.560  29470 global Parameter setting: 'retryPonCnt' '2'
2012-03-24 16:15:30.560  29470 Line: fsc201 cycle
2012-03-24 16:15:30.560  29470 found entry for host >fsc202< cycle >1<
2012-03-24 16:15:30.560  29470 found entry for host >fsc202< cycle >1<
2012-03-24 16:15:30.560  29470 Read from Config File, user: USERID
2012-03-24 16:15:30.560  29470 decryptPassword OK 36 -> 8
2012-03-24 16:15:30.560  29470 Read from Config File, printDevIp: 10.235.16.21:USERID:*****
2012-03-24 16:15:30.560  29470 Read from Config File, printDevIp: 10.235.16.21:USERID:*****
2012-03-24 16:15:30.560  29470 Read from Config File, DevIp: 10.235.16.21
2012-03-24 16:15:30.560  29470 type ipmitool > /dev/null 2>&1
2012-03-24 16:15:30.563  29470 has_ipmitool is: 1
2012-03-24 16:15:30.563  29470 ipmitool -P xyz -V 2>&1
2012-03-24 16:15:30.567  29470 > [ipmitool version 1.8.11]
2012-03-24 16:15:30.568  29470 has_paramP is: 1
2012-03-24 16:15:30.568  29470 status query (has_ipmitool 1) ...
2012-03-24 16:15:30.568  29470 status query (has_ipmitool 1) ...
2012-03-24 16:15:30.568  29470 ipmitool -v -I lan -H 10.235.16.21 -U USERID -P ##### chassis
power status 2>&1
2012-03-24 16:15:30.590  29470 > [Chassis Power is on]
2012-03-24 16:15:30.590  29470 query result is 0
```

An example of the *sa_ipmi.log* output for a successful sa_ipmi shutdown agent test follows. The actual sa_ipmi test command was executed in a different session window (reference command example listed in Section 6.8.2, “Monitoring

the Shutdown Agents From the Nodes", on page 412). Direct questions regarding the content of a *sa_ipmi.log* file to your next level of support.

An 'empty' output is expected as a result for all of the queries and/or tests of a successful sa_ipmi test run from the command line.

Note: The 'tail' job indicated will initially print the last ten lines in the *sa_down.log* file. To gain separation from these ten lines and your test output, press the Enter key 4 or 5 times.

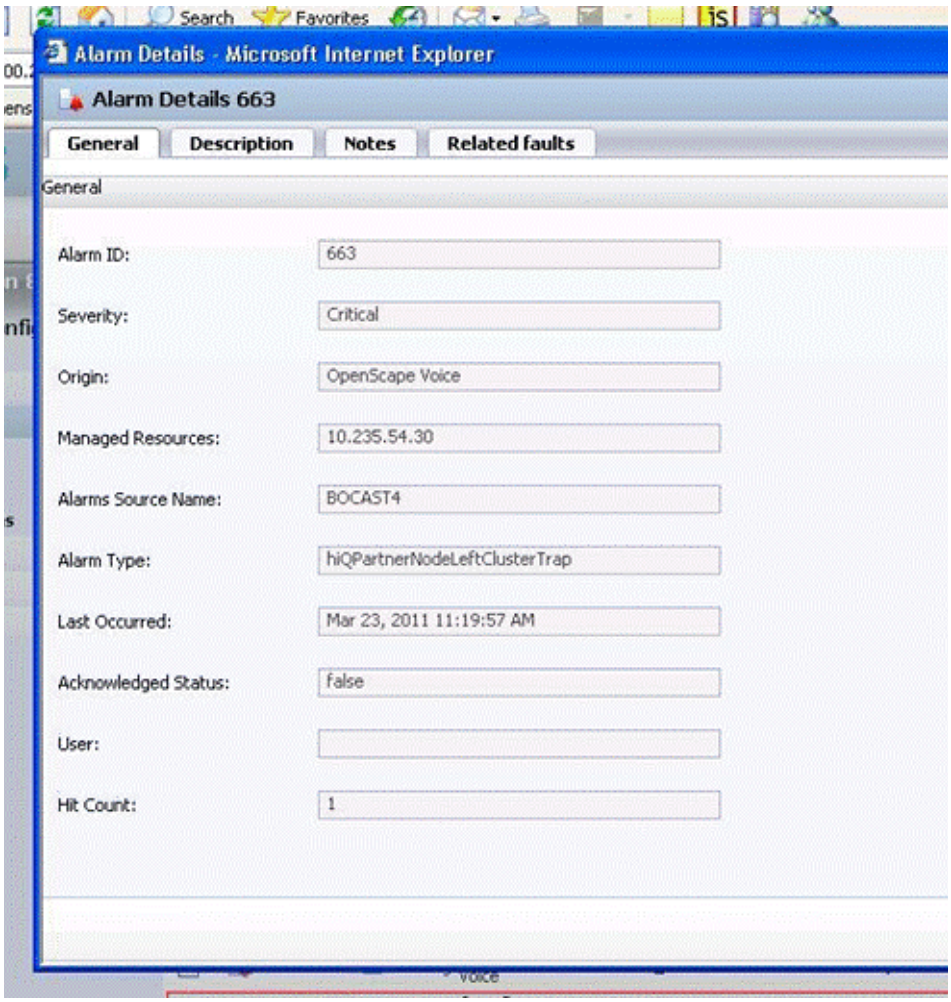
Note: The sa_down test is applicable to Virtual and non-Virtual OpenScape Voice environments. The sa_ipmi test is NOT applicable to a Virtual OpenScape Voice environment.

This log was collected from the node of an OpenScape Voice cluster at software level V7.00.01.ALL.11_PS0004.

```
sysad@fsc201:[/home/sysad] #60
$ tailf /var/opt/SMAWhaext/log/sa_down.log

2012-03-24 16:22:09.292   7819 @(#)$Header: SA_down.c /main/6 2010/08/10 12:49:17 try $ SNI
2012-03-24 16:22:09.292   7819 ReadConfigFile called for host fsc202
2012-03-24 16:22:09.292   7819 Line: fsc201
2012-03-24 16:22:09.292   7819 Configuration entry found for host: >fsc202<
2012-03-24 16:22:09.292   7819 SaQuery -s fsc202
2012-03-24 16:22:09.388   7819
2012-03-24 16:22:09.388   7819 User srx, had no failed login attempts since last successful login.
2012-03-24 16:22:09.446   7819 srx on fsc201 using /dev/pts/1 ...
2012-03-24 16:22:10.762   7819 NOTICE SA_down: do_test: SaQuery returned success
2012-03-24 16:22:10.762   7819 result of status test is: 0
```

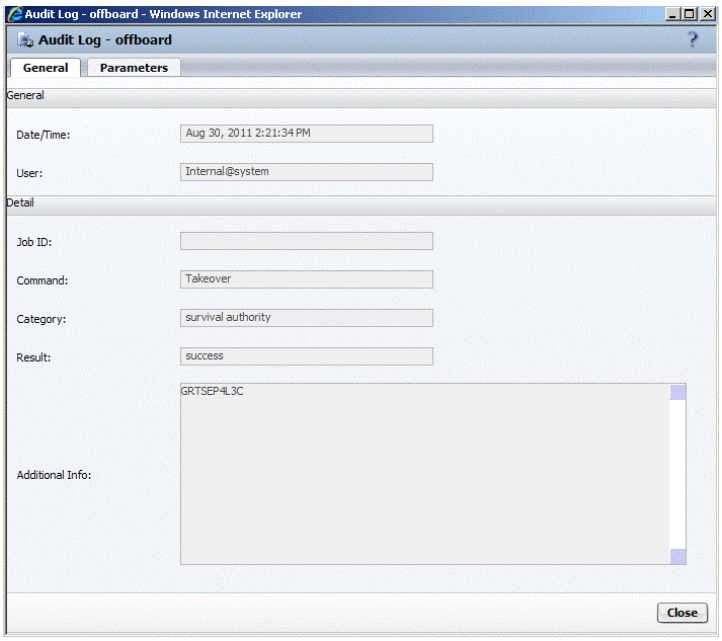
6.8.4 Activity Log for Survival Authority Action

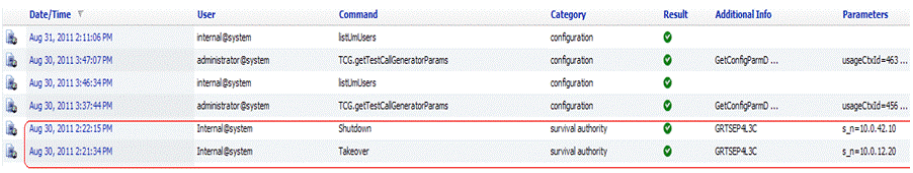
In the case of a complete interconnection failure between OpenScape Voice nodes, and OSV nodes and the partner maintenance controller (IMM, iRMC), each node will send a trap "hiQPartnerNodeLeftClusterTrap" to the Survival Authority. The Survival Authority responds with an SNMP SET command to "takeover" or to "shutdown". The Survival Authority returns "takeover" to the first node to deliver the trap and the "shutdown" to the second node to deliver the trap. An example follows:



Attention: The Standalone Service option is available for duplex configurations. If it is enabled, the node that does not get the permission to take over from the Survival Authority stays active (in Standalone Secondary mode). For more information regarding the Standalone Service feature, refer to Section 2.6.2.9, “Stand Alone Service Enabled”, on page 57 of this document or to the *OpenScape Voice Vx, Feature Description documentation*, section “Survival Authority” (where *x is the software release version*). **Any questions regarding the Standalone Service should be addressed to your next level of support.**

You can monitor the Survival Authority activities via the CMP. Login to the CMP, then select the Maintenance tab and navigate Monitoring --> Logs --> System. Filter for Survival Authority in the 'Advanced' options. You should see two entries similar to the following:





Date/Time	User	Command	Category	Result	Additional Info	Parameters
Aug 31, 2011 2:11:06 PM	internal@system	listUmUsers	configuration			
Aug 30, 2011 3:47:07 PM	administrator@system	TCG.getTestCallGeneratorParams	configuration		GetConfigParmD ...	usageCtxId=463 ...
Aug 30, 2011 3:46:34 PM	internal@system	listUmUsers	configuration			
Aug 30, 2011 3:37:44 PM	administrator@system	TCG.getTestCallGeneratorParams	configuration		GetConfigParmD ...	usageCtxId=456 ...
Aug 30, 2011 2:22:15 PM	Internal@system	Shutdown	survival authority		GRTSEP4L3C	s_n=10.0.42.10
Aug 30, 2011 2:21:34 PM	Internal@system	Takeover	survival authority		GRTSEP4L3C	s_n=10.0.12.20

- **TakeOver** + IP address of the surviving node under ‘Parameters’ for the node which survives the failure (or becomes ‘Standalone Primary’ if StandAloneService is enabled)
- **Shutdown** + IP address of the killed node under ‘Parameters’ for the node which gets shutdown (or becomes ‘Standalone Secondary’ if StandAloneService is enabled)

Note:
Click this link to return to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11”.

---

7 Overview of Upgrades and Migrations to OpenScape Voice V11

The following table shows the hardware platforms that support new installations, Upgrades and Migrations:

Server Model	Comment
Lenovo SR630 V3	• Supported for new installations. • Supported for Upgrade from existing installations. • Supported for Migration from any hardware platform.
Lenovo SR630 V2	• Supported for new installations. • Supported for Upgrade from existing installations. • Supported for Migration from any hardware platform.
Lenovo SR530	• Supported for Upgrade from existing installations. • Supported for Migration.

Supported Hardware Servers for New Installations, Upgrades & Migrations

Attention: Before beginning an upgrade on a redundant system, ensure that the Survival Authority and IPMI shutdown agents are functioning correctly on the source release.

For more information refer to Section 6.8, “Verifying the Shutdown Agents Configuration”, on page 409.

Note: The Upgrade or Migration from a source system to a target system with both having the same release version (e.g., from V10 to V10) is usually performed when the installed image is to be replaced with a newer image of the same release.

Attention: There is no need to re-provision/re-assign the MediaServer announcement/treatments or Prefix Access Code (PAC) data after completing the Upgrade/Migration. The upgrade process manages the required database and configuration changes.

Attention: For Simplex systems, after the successful Upgrade or Migration, the English language will be installed by default. Any other languages will have to be installed. Reference Appendix 28, “Guidelines for Language and Application Package adds to Simplex Systems” page 783 for more details.

To expedite the installation of the additional language packages, it is recommended you know which language packages are necessary for installation after the successful Upgrade or Migration procedure is executed.

If it is decided to install the additional packages at a later date, it is recommended this activity take place in a maintenance window because the affected Applications server will be out-of-service for the duration of the package add(s). Any features provided by the Applications server will be unavailable for the duration of the package addition(s).

When performing an upgrade, the source system must have a smaller or equal version compared to the target system. For example, from UC V9R3 HF3 to UC V9R3 HF5. In case you want to upgrade to a higher version of OSV and the UC version is lower than the one you have, perform the following steps:

1. Starting from source OSV Integrated Simplex, on node1 enter the command as user root:
   ```
   # cd /root; upgrade8k -quiet -noimport
   ```
   This will install the higher edition of the OSV IMG on the fallback side and it will not import the data automatically after the update.
2. Once the update has finished, the UC application must be updated to, in our example, V9 R3 HF5 again (as the image installed only UC HF3)

3. Install the toolkit
4. Execute command `import8k -local` on OSV node 1. This will retrieve the data from the source version and will finish successfully as now the UC will be on the same level, in our example V9R3 HF5.

OpenScape Voice Server system migrations with a network schema change are supported (refer to Chapter 9, “Migrations to OpenScape Voice V11”). Another strategy to implement a network change migration scenario is to upgrade (or migrate) the OpenScape Voice server to the target release first and then update to the new network schema with the Installation Framework Update (EZIP). Refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”. Questions should be addressed to your next level of support.

During an installation or an upgrade process, the hard disk drives for each node are divided into two partitions of equal size. These HDD partitions are referred to as the “Primary” partition and the “Secondary” partition.

The partition on which the running software resides is called the "Active" partition (this could be either the "Primary" or "Secondary") and the other partition is called the "Fallback" partition (also referred to as the "standby" partition).

Note: To determine the contents of the OSV system active and passive partitions, execute as user *root*:

 # /unisphere/srx3000/srx/bin/sync8k -v

Should the Active partition become unstable during the upgrade, one option is to recover by booting off of the Fallback partition. Fallback procedures are described in Section 8.9, “Fallback Procedures”, on page 507.
When a decision to Fallback is made the associated Fallback Procedure is determined based on how far the upgrade procedure has progressed. Different Fallback procedures are called for based on the upgrade progress.

Read the following sections carefully before beginning any upgrade or migration:

- Section 7.2, “Solution Upgrade Considerations”, on page 422.
- Section 7.2.2, “Hardware Platform Migrations”, on page 422.
- Section 7.3, “Upgrade and Migration Scenarios”, on page 424.
- Section 7.4, “Completing the Upgrade/Migration to V11”, on page 428.

7.1 Feature Support Notes

7.1.1 Source Based Routing

Source based routing is supported. Employing source based routing, the OSV sends IP packets to an IP gateway/router based on which subnet the source IP of the packet belongs to. For this default, gateways should be specified for the OSV IP subnets admin, signaling and billing. If, for example, a billing gateway is specified, the OSV sends billing files via this gateway and there is no need for the creation of static routes to each billing server.

Another advantage of source base routing is that responses to admin requests from a remote IP network to the OSV admin IP address are sent back via the default admin gateway. Without this admin gateway, the response would be sent via the default router, which is usually on the signaling network. It is therefore highly recommended to specify default gateways via NCPE when preparing the node.cfg for the new release. Additional notes regarding source based routing follow;

a) There is no source based routing for the OSV x-channel subnet. But, an xchannel default gateway is still required if the x-channel subnets of the two nodes are different. It is used by the OSV to automatically create a static route to the partner node x-channel IP address.

b) Even with source based routing, static routes are still required for OSV trap destinations, NTP and DNS (this is because the OSV software does not control the source IP of packets sent to these devices).

c) OSV automatically replicates each static route to the source based routing table of the subnet that the router belongs to. For example, if the admin network is 1.2.3.0 to 1.2.3.255 and if a static route to IP 4.4.4.4 is specified via router 1.2.3.1, there will be two static routes, one in the admin source based routing table and one in the global routing table. So even if the OSV sends out a packet to 4.4.4.4 with source IP 2.2.2.2, it will still go via 1.2.3.1.

d) If source based routes are already established on the source release, these default gateways will be reflected in the node.cfg built from the system data collection step. The system data collection step is included in each upgrade procedure (refer to Section 8.3.1, “Create the Node.cfg for the Target System”, on page 456, for details on this procedure). This data collection node.cfg will be the basis for the target release installation node.cfg. The source based routes will be included in the target release node.cfg. It is a good practice to review the target release node.cfg before installation of the target release.

e) There are two options to implement source based routes during an upgrade:

- Implementing or updating of source based routes during an upgrade will require the use of a Migration strategy (and therefore a system outage). These Migration strategies are detailed in Chapter 9, “Migrations to OpenScape Voice V11”.
- For duplex systems, if an OpenScape Voice system outage cannot be tolerated during an upgrade, the implementation of source based routes is a two step process:

– First, the Outage Free toolkit upgrade will need to be performed. The procedure is detailed in Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”, on page 483. As a general rule, no changes to the OSV target release node.cfg are allowed during the three upgrade procedures detailed in Chapter 8, “Upgrades to OpenScape Voice V11”

– After a Chapter 8 upgrade procedure is completed, the EZIP feature can be employed to establish source based routing (by specifying default gateway addresses). For more information regarding EZIP, Chapter 13, “Updating the Node.cfg File (Also Known as EZIP)”.

7.1.2 Flexible Ethernet circuit and IP Address Configuration

Before starting the Upgrade or the Migration, ensure that the servers to be used for the target release are supported for the activity. For details, refer to Table on page 417.

7.1.3 Cluster Timeout

In older OSV versions the node.cfg parameter was introduced; **Cluster Timeout**. The **Cluster Timeout** parameter indicates how long the cluster cross channel (AKA x-channel and cluster interconnect) can be down before the Cluster Manager declares "Changed cross channel state to DOWN" and initiates shutdown agent activity to prevent a split brain condition.

If a node to node connection failure is less likely than a server failure (e.g.; in a co-located configuration), a **Cluster Timeout** of 10 seconds is recommended. If the likelihood of short term node to node connection failures is higher, values of up to 15 seconds are recommended. After a successful upgrade, the **Cluster Timeout** can be changed with the IFgui Update tool (EZIP). Refer to Appendix 13, "Updating the Node.cfg File (Also Known as EZIP)"

In case of a version upgrade, the **Cluster Timeout** value of the source will be maintained in the target.

7.1.4 Broadcast Routes

Broadcast route '239.255.255.253 255.255.255.255 0.0.0.0 nafo0' is no longer necessary for the OpenScape Voice (OSV) server. The route will not be carried forward from the source release to the target release system.

Source release Broadcast routes configured on the OSV can be found in the node.cfg file "Section 3: IP configuration". Source release Broadcast routes can also be listed by opening the source release node.cfg file with the "Generally Available" source release NCPE (in expert mode). The broadcast routes are found in IP Configuration (5/6).

7.2 Solution Upgrade Considerations

Refer to Appendix 30, “Solution Upgrades” for an overview of solution upgrades and the recommended V11 solution upgrade sequence.

7.2.1 Servers No Longer Supported

Before starting the Upgrade or the Migration, ensure that the servers to be used for the target release are supported for the activity. For details, refer to Table on page 417.

7.2.2 Hardware Platform Migrations

Attention: An upgrade that includes a migration to a different hardware platform, for whatever reason, is performed using the migration toolkit and appropriate checklist in Chapter 9, “Migrations to OpenScape Voice V11”.

The new server (or servers) should be installed into the rack and prepared (for example: modify the SCSI RAID configuration, modify the BIOS settings, update firmware) for the migration before the maintenance window in which the migration shall be performed. **Server Installation details are provided in Chapter 3, “Installing the Hardware Platform”**.

7.2.3 Additional Servers for Migrations to Standard Duplex

Note: Integrated simplex or duplex migrations to standard duplex are performed using the migration toolkit and appropriate checklist in Chapter 9, “Migrations to OpenScape Voice V11”.

Migrations to standard duplex require that an external applications server is installed with the OpenScape Applications DVD version level and the SLES operating system level that is compatible with the OpenScape Voice software version and patch set level.

For Multiple Communications Server Admin deployments refer to Chapter 5, “Installing the OpenScape Applications” of this document.

For Standard Duplex Small or Standard Duplex Large deployments refer to the appropriate section(s) of the *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide (*where *x* is the software release version*)*.

After you perform the checklist steps to migrate to standard duplex, you then install/update this external applications server to the OpenScape Applications V10 USB level and the recommended SLES OS and SP distribution level as necessary.

Note: The Deployment Service (DLS) component might not be supported on the external OpenScape Applications server due to sizing limitations. A separate server running Microsoft Windows might be required for the DLS component. Please review the DLS release notes for sizing limitations when DLS is installed as a component of the external applications server.

Attention: If the integrated OSV system contains a DLS and migration of the DLS to an offboard server is planned, perform data collection on the source release (integrated) DLS before starting any Simplex to Standard Duplex migration procedure. Please refer to the DLS Release Notes for the data collection instructions.

7.3 Upgrade and Migration Scenarios

Note: Upgrades and Migrations to V11 are supported only from V9 and V10 systems. The Upgrade or Migration from a source system to a target system with both having the same release version (for example, from V11 to V11) is usually performed when the installed image is to be replaced with a newer image of the same release.

Attention: Ensure that SIP-Q connections are configured to use the TCP or TLS+MTLS transport before you begin the upgrade. For a SIP-Q GW (for example, HG3540): ensure the transport type = TCP or TLS+MTLS (no UDP). Please refer to INF-08-000789 on G-DMS for links to the solution configuration guides for additional details. Ensure that GW calls complete successfully (inbound and/or outbound) before you begin the upgrade if you update the configuration.

Attention: The functionality whether OSV will set up an MTLS connection to an endpoint has been split out from the MTLS transport type and shows up as a new checkbox in OSV Assistant named "Endpoint does not accept incoming TLS connections". At the same time, when setting the transport type to MTLS, it is now enforced that the connection must be served by SIPSM 3 or SIPSM 4. The consequence of this is that after the upgrade for backward compatibility reasons, an endpoint that was formerly configured to show MTLS transport type will now show TLS transport type (with the Endpoint does not accept incoming TLS connections checkbox not checked). If the craft wishes to enforce MTLS, then the craft must manually set the transport type to MTLS which will require the endpoint to send its messages on a mutually authenticated TLS connection served by SIPSM 3 or SIPSM 4.

7.3.1 Upgrade Scenarios

The following sections address both supported and not supported upgrades in addition to remote software upgrades.

7.3.1.1 Supported Upgrades

Refer to Chapter 8, “Upgrades to OpenScape Voice V11” for these upgrade scenarios (in each scenario the target system’s hardware server platform model, product type, subnet configuration, and deployment type [co-located nodes or geographically separated nodes] is kept the same as the source system).

The Outage Free toolkit upgrades, Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”, on page 483, is still supported for standard duplex systems if the customer cannot accept system downtime.

Note: The term native hardware refers to an OpenScape Voice system configuration that is not a virtual machine.

- V9/V10 simplex virtual machine to V11 simplex virtual machine. Refer to Section 8.5.1, “Overview”, on page 471.
- V9/V10 simplex native hardware to V11 simplex native hardware. Refer to Section 8.5.1, “Overview”, on page 471.
- V9/V10 standard duplex native hardware to V11 standard duplex native hardware. Refer to Section 8.6.1, “Overview”, on page 483.
- V9/V10 standard duplex virtual machine to a V11 standard duplex virtual machine. Refer to Section 8.6.1, “Overview”, on page 483.

Note: An alternative upgrade choice is the Remote Software Upgrade. For more information, refer to Section 7.3.1.3, “Remote Software Upgrade as an Alternative Upgrade Choice”, on page 426.

7.3.1.2 Upgrades Not Supported

Upgrades of integrated duplex systems are not supported. Integrated Duplex systems must migrate to a Standard Duplex configuration on HW supported in V11, refer to Chapter 9, “Migrations to OpenScape Voice V11”.

Low Cost systems are not supported. A Low Cost system in an older release must be migrated to a configuration supported in V11. Refer to Chapter 9, “Migrations to OpenScape Voice V11”.

7.3.1.3 Remote Software Upgrade as an Alternative Upgrade Choice

Remote Software Upgrades were introduced (Section 8.7, “Upgrade of an OSV System Using Remote SW Upgrade”, on page 491). This feature saves service cost by providing a procedure to perform major release upgrades without the cost of having a Service Technician on-site.

Remote Software Upgrades are applicable to:

- OSV Integrated Simplex
- OSV Standard Duplex (the OSV nodes only). Outage Free Toolkit Upgrade should be employed if an outage is not acceptable.
- OSV Virtual deployment (Standard Duplex)

7.3.2 Hardware Migrations

Note: Product type and node deployment changes are allowed as part of the hardware platform migration.

These migrations are performed using the migration toolkit and appropriate checklist in Chapter 9, “Migrations to OpenScape Voice V11”. Refer to Chapter 9, “Migrations to OpenScape Voice V11” for the following upgrades that include a hardware platform migration:

- V9/V10 simplex to V11 simplex
- V9/V10 simplex to V11 standard duplex (co-located nodes or geographically separated nodes)
- V9/V10 standard duplex (co-located nodes or geographically separated nodes) to V11 standard duplex (same node deployment as source)
- V9/V10 standard duplex (co-located nodes) to V11 standard duplex (geographically separated nodes)

7.3.3 Product/Node Deployment Migrations

Refer to Chapter 9, “Migrations to OpenScape Voice V11” for the following product type or node deployment migrations:

Note: In these product type and node deployment migrations, the existing OpenScape Voice server hardware is reused.

- V9/V10 simplex to V11 standard duplex (co-located nodes or geographically separated nodes)
- V9/V10 standard duplex (co-located nodes) to V11 standard duplex (geographically separated nodes)
- V9/V10 standard duplex native hardware (co-located nodes or geographically separated nodes) to V11 virtual machine (same node deployment as source). Knowledge of the VMware environment is a pre-requisite for this migration. If the hardware of the source release is reused for this migration scenario; before the OSV Image can be installed the ESXi must be installed and the virtual environment configuration built. This will extend the system down time.**Section 4.3, “Virtualization Environment Setup”, on page 241** should be referenced for details.

7.4 Completing the Upgrade/Migration to V11

Note: When migrating from a simplex to a standard duplex configuration or performing an upgrade that includes a node deployment migration, please consider the following;

- Basic TLS certificates are included in the image install. If custom certificates have been employed the migration from a simplex to a co-located duplex system should not require the generation of additional custom certificates for node 2 (because the network schema does not change). Migration to a geo-separated environment will require the generation of additional custom certificates because node 2 will have a different network schema than node 1. Node deployment migrations will require the generation of additional custom certificates for node 2 also.
- The external DNS will have to be administered with the node 2 IP address information.

Note: It is recommended that any USB drive(s) used during an OpenScape Voice Installation procedure be removed from the server(s) at this time.

Note: Ensure that all *OpenScape UC Application V10 Installation and Upgrade, Installation Guide* migrations steps have been addressed for Solution Upgrades that include a "Migration from Integrated to Small Applications deployment" or "Migration from Small to Large (or Very Large) Applications deployment" migration. This will prevent feature failures on the target solution.

As an example:
An OpenScape Voice "Simplex to Standard Duplex Product Migration" includes a migration from an Integrated Applications deployment to a Small Applications deployment. The Integrated Simplex OSV media server endpoint IP addresses should be updated to the IP of the offboard media server in the Standard Duplex OSV. Without these updates important functionality will be missing on the target solution; for instance the UC Conference portal.

Complete the upgrade to V11 by using the following steps:

1. The V11 target licenses should have already been installed on the OSV server and, if necessary, the offboard (external) Applications server. If the licenses were not installed please do so now.
   - For OSV license installation;

- For Integrated OSV systems and node 1 of a duplex OSV configuration refer to Section 9.12.1.2, “Customize Node 1”, on page 567.
- For node 2 of a duplex OSV configuration refer to Section 9.12.2.2, “Customize Node 2”, on page 570.

- If the Offboard (external) and Integrated Simplex Applications servers require license installation (e.g.; UC licenses), refer to the section titled "*Activating Licenses*" in the *OpenScape UC Application Configuration and Administration* documentation of your release.

2. If migration was performed with server(s) hardware change out, the IMM/iRMC user id and password are created with the default values (USERID/PASSW0RD where the "0" in PASSW0RD is zero, not the letter O) on the new server(s). If the old server(s) had non-default values for the user id and password, then update the IMM/iRMC user id and password on the new server(s) as described in Section 4.4.3, “Changing the User ID and Password for the IMM/iRMC/BMC Account”.
3. Carefully review the **OpenScape Applications V10 release notes** and download any materials the release note indicates that you will need to install any required workaround, hot fixes, or updates to the OpenScape Applications.
4. Carefully review the **OpenScape Voice V11 release notes** and download any materials the release note indicates that you will need to install any required workaround, patches, emergency patches, or updates to the OpenScape Voice system.
5. If the source release *hosts* file was copied and saved due to the Section 8.4.7, “Verify the Hosts File Configuration”, on page 465 procedure, rebuild the user-created entry list in the target release *hosts* file as follows:

Note: For duplex systems, both nodes need to be updated. The duplex system *hosts* files should be updated from the saved *hosts* file of that node. The stored *hosts* files should have been saved with names indicative of the node the *hosts* file was saved from (for example: *hosts_n1* and *hosts_n2*).

---

a) Open and copy the user-created entry list from the saved source release *hosts* file and paste the list below the new banner in the target release *hosts* file (new user-created entries can be added to the bottom of the list). For example, the *nmcsnmptrap* and *host_pc* are user-created entries copied and pasted into the target release *hosts* file:

```
10.235.54.10      rtp_com0_eth6
10.235.54.30      rtp_com1_eth6
########################################
# Please add new hosts under this line #
```

```
########################################
10.235.200.230    nmcsnmptrap
10.235.200.29     host_pc
```

b) Verify that all the user host´s entries were carried properly.

6. Restore the Cron tables for user ***root***.

   There are two Cron tables; One for user ***root*** and another for user ***srx***.

   The Cron tables are different on each node and for each of the above two users.

   a) On the first node, open file `crontab_root_node1` of the source release that was saved to an external location prior to the upgrade.

   b) Open/edit the Cron table for user ***root*** on the first node.
   `# crontab -u root -e` (u=user, e=edit cron table)

   c) For each entry in the source release file `crontab_root_node1`, determine whether the source release cronjob should be added to the target release crontab.

   d) Save the Cron table for user ***root***.

   e) For an OSV duplex system, repeat the above steps for user ***root*** on node 2. Remember that the saved Cron tab file of the source release of node 2 is `crontab_root_node2`.

7. Restore the Cron tables for user ***srx***.

   a) On the first node, open file `crontab_srx_node1` of the source release that was saved to an external location prior to the upgrade.

   b) Open/edit the Cron table for user ***srx*** on the first node.
   `# crontab -u srx -e` (u=user, e=edit cron table)

   c) For each entry in the source release file `crontab_srx_node1`, determine whether the source release cronjob should be added to the target release crontab.

   d) Save the Cron table for user ***srx***.

   e) For an OSV duplex system, repeat the above steps for user ***srx*** on node 2. Remember that the saved Cron tab file of the source release of node 2 is `crontab_srx_node2`.

8. CLM Settings file restoral.

   a) For an integrated simplex system, if CLM (Customer License Manager) is employed, the `ClmSettings.xml` file must be restored as follows:

   - Open the backed up file `ClmSettings.xml` with the CLM access configuration. This file contains the access configuration for the CLM.

- Execute the following commands to create a new file "`/enterprise/clm/ApacheTomcat/ClmSettings.xml`" and to update the database:

  ```
  # cd /enterprise/clm/
  # bash remoteAccess.sh <IP addr 1>,<IP addr 2>,<IP addr…>,<IP addr n>
  ```

Attention: All IP addresses listed in the `AllowedClients` field must be restored.

Example:

```
bash remoteAccess.sh
10.235.200.113,10.235.200.28,10.235.65.221
```

Attention: Make sure no blanks are entered between the IP addresses.

The backed up file `ClmSettings.xml` was in a directory "`/enterprise/clm/ApacheTomcat`". It is different from the one that includes the file `ClmSettings.xml` created here.

b) For a duplex configuration, if CLM (Customer License Manager) is installed, the `ClmSettings.xml` file must be restored as follows:

- Open the backed up file `ClmSettings.xml` with the CLM access configuration. This file contains the access configuration for the CLM.
- Execute the following commands to create a new file "`/opt/licenses/clm/ApacheTomcat/ClmSettings.xml`" and to update the database:

```
# cd /opt/licenses/clm
# bash remoteAccess.sh <IP addr 1>,<IP addr 2>,<IP
addr…>,<IP addr n>
```

Attention: All IP addresses listed in the `AllowedClients` field must be restored.

Example:

```
bash remoteAccess.sh
10.235.200.113,10.235.200.28,10.235.65.221
```

Attention: Make sure no blanks are entered between the IP addresses.

The backed up file `ClmSettings.xml` was in a directory "`/opt/siemens/clm/ApacheTomcat`". It is different from the one that includes the file `ClmSettings.xml` created here.

9. Executive Assistant file restoral.

a) For an integrated simplex system, if Executive Assistant feature is employed, the source release '.eag' files must be restored as follows:

- SFTP the '.eag' files that were saved to an external location prior to the upgrade to "`/enterprise/HiPathCA/WebSpace/Portal/webapps/eacockpit-osc/WEB-INF/groups`"

  These file contains the Executive Assistant configuration data.

- Restore file ownership and access rights as follows:

  ```
  # cd /enterprise/HiPathCA/WebSpace/Portal/webapps/
  eacockpit-osc/WEB-INF/groups
  # chown sym:sym eagroup*
  # chmod 664 eagroup*
  ```

b) For a duplex configuration, if Executive Assistant feature is employed, the source release '.eag' files must be restored as follows:

- SFTP the '.eag' files that were saved to an external location prior to the upgrade to `"/opt/siemens/HiPathCA/WebSpace/Portal/webapps/eacockpit-osc/WEB-INF/groups"`

  These file contains the Executive Assistant configuration data.

- Restore file ownership and access rights as follows:

  ```
  # cd /opt/siemens/HiPathCA/WebSpace/Portal/webapps/
  eacockpit-osc/WEB-INF/groups
  # chown sym:sym eagroup*
  # chmod 664 eagroup*
  ```

10. The following should be observed regarding media servers:

- There should be no need to re-provision/re-assign the MediaServer announcements, treatments or Prefix Access Code (PAC) data after completing the Upgrade/Migration. If problems with the media server are observed or suspected, refer to the following:
  - For media server announcement and treatments, refer to *OpenScape Voice Vx Administration, Administrator Documentation* (where *x is the software release version*), the section titled *Media Services.*
  - For media server hardware requirements, refer to *OpenScape Media Server Vx Administrator Documentation* (where *x is the software release version*).
  - For Prefix Access Code (PAC) information, refer to Section 14.2, “How to Add/Delete Default PACs for Vertical Services”, on page 598.
- The RadiSys Convedia media server is no longer supported.

Note: The Media Server SIP endpoint for Integrated Simplex deployments shall be associated with the non-standard port numbers 5062 (SIP) and 5063 (SIP-TLS) for the signaling between the OSV and the Media Server.

Verify the Integrated Media Server SIP listening ports are changed (via CMP) from 5060/5061 to 5062/5063 with the CMP. Navigate to **Configuration>Unified Communications>Configuration>Media Server**.

- Select the **Media Server Node**, then the **Edit** button. The **Node Administration** window is presented.

- From the **Node Administration** window select the **Providers** tab, the **IP Telephony (SIP)** radio button and then the **Edit** button. The **IP Telephony (SIP)** window is presented.

- In the **IP Telephony (SIP)** window verify the **Listening points for SIP networking** are **5062 (for UDP and TCP)** and **5063 (for TLS)**.

If you need to create a SIP endpoint for the MS, use ports 5062/5063 as well. Update the corresponding packet filter rules with the new port numbers.

Note: For specific information regarding the Media Server, e.g., Packet Filter Rule requirements, refer to the *Media Server Component Release Note* (found in the OpenScape UC Applications release Notes).
More details for PACs can be found in the *OpenScape Voice Vx Configuration Manual, System Configuration and Administration, Administrator Documentation* (where *x is the software release version*).

---

11. Refresh the CMP after completing the Upgrade/Migration procedure by logging into the CMP and navigating to the following menu:
Configuration > OpenScape Voice > General > Switches

    Select your switch and click on **Refresh Switch Data** button. In case some information is incorrect, you may use the **Edit** option to correct it.

Note: In some upgrade scenarios particularly of an integrated simplex system, the user cannot immediately refresh the CMP because the OSV is still locked and indicates "Upgrade in Progress".

To unlock the OSV from the Assistant, navigate to **Maintenance > Inventory > Applications**. The **OpenScape Voice** entry shows "Upgrade Version in progress". Click on the arrow at the end of the line on the right and select **Upgrade Version**. In the popup window, click the Cancel button at the bottom of the screen (not the X button in the upper corner). The OSV is now unlocked. However, the "Upgrade Version in progress" display remains until the CMP is refreshed.

The user must now refresh the CMP as indicated above this Note statement. After refreshing the CMP, the "Upgrade Version in progress" display is cleared.

If you can't login to the CMP, most likely symphonia was stopped during one of the upgrade or migration steps. Restart symphonia:

```
# /etc/init.d/symphoniad restart
```

After a few minutes, login to the CMP and refresh the switch data as indicated above.

12. If the source release initially had the SIP Session timer enabled and it was disabled by the user during the Pre-Maintenance Window Activities, Section 8.4.12, “Disable SIP Session Timer”, on page 469, then the initial setting needs to be restored using the Assistant as follows:
    - Login onto CMP
    - Click **Configuration** tab
    - Click **OpenScape Voice**
    - Select your switch
    - Click **Administration** > **General Settings** > **RTP**
    - From the dropdown menu of the "in" field, select Name
    - In the "Search for" field, enter: Srx/Sip/Session_Timer (case sensitive)
    - Click on the Srx/Sip/Session_Timer and change the value to **Yes**.
13. After upgrading the OpenScape Voice to V11, it must be verified that all voice mail Endpoints have the "Voice Mail Server" attribute provisioned. The V10 CMP/Assistant can be used to verify/set the "Voice Mail Server" attribute in the **Endpoints "Attribute"** tab.
14. After the successful Upgrade of (or Migration to) a virtual OpenScape Voice system, the resource allocation of the target system must be verified against Table 13 on page 251, "Virtualization Dimensioning Details " of the target release OpenScape Voice Installation and Upgrade Guide (IUG). The resource allocation of the target release virtual machine(s) must match the values listed in Table 13 of the target release IUG.

Attention: Some virtual machine resource changes require the machine be shut down (e.g., vCPU and Memory resources changes). This activity will cause a loss of service for the Integrated Simplex OSV and its Applications server.

If an outage is not allowed for the Standard Duplex virtual system, the Duplex system virtual resource allocation update must be performed by first shutting down one node (i.e.; node 1), updating that node's VM resource allocations, and then restoring that node to state 4. After one node is updated and restored to service, the partner node (i.e.; node 2) can be shut down, updated, and restored to state 4.

Normal operating procedures for updating a Integrated Simplex or Standard

Duplex system should apply too.

Questions should be addressed to your next level of support.

15. If there were scheduled CMP backup or export tasks recorded before the upgrade, you should recreate them now (see the administrator documentation *OpenScape Common Management Platform*), because backup unit names may get lost during an upgrade.
16. This step relates to Simplex OSV systems only.

    In some cases the following procedure will ensure "Presence" status changes are reflected in the client Fusion bar.

    a) Login to the CMP and navigate as follows;
    Maintenance > Inventory > Nodes & Applications > Nodes > <name of the OSC UC Applications server>

    b) This will present the Dashboard pop-up. In the Dashboard pop-up, under **Actions**, click the "**Show services status**" **Show** button.

    c) This will present the List of Components pop-up.

    d) In the pop-up **Filter** field enter "**Presence Service**" and click the **Go** button.

    e) The "Presence Service" component will be displayed. Click on the "**Presence Service**" component.

    f) An Edit Service Configuration pop-up for the **Presence Service** opens.

    g) Set the "**Eventing Backwards Compatible**" parameter value to **true**.

    h) Click the Edit Service Configuration pop-up **Save** button. Close the List of Components and Dashboard pop-ups.

    i) To complete the procedure, verify your Presence status changes are now reflected in the client Fusion bar.

Be sure to refer to Section 7.5, “Post Upgrade Actions”, on page 436 and perform the appropriate post upgrade procedures.

7.5 Post Upgrade Actions

After the upgrade/migrate procedure from V9/V10 to V11, the supervision timer values need to be aligned to the values of the response Timers from the external servers, as the receipt of the 100 Trying responses will not stop the Outgoing Call Supervision timer.

7.5.1 Create CLI Users

This step is necessary if customer created CLI accounts were not carried forward following a successful upgrade. If no customer created CLI accounts are missing, refer to Section 7.5.4, “Take File System and Database Backups”, on page 439.

Create users for each missing CLI account identified during the data collection phase.

Login to Node 1 as the user *srx* and start the RTP CLI:

- `> startCli`
- Select the following menu options:

  4 - Security Management

  1 - Users

  1 - Create User

Create each user with the role and password expiration criteria as identified in the data collection phase.

7.5.2 Create Linux Accounts for CLI Users

Note: Before proceeding with this procedure, be sure to review Section 17.2.3, “Change Default Password Policies for New Accounts”, on page 620.

This step is necessary if customer created Linux accounts were not carried forward following a successful upgrade. If no customer created Linux accounts are missing, refer to Section 7.5.4, “Take File System and Database Backups”, on page 439.

In order to access the CLI using a remote login, each CLI user must have its own Linux account. The following steps can be used to create Linux accounts for each CLI user:

All of the following commands must be executed as user root or srx on one node:

New users can be created from `account_admin` and `account_config` scripts.

`account_admin` - OSV user account administration

##

Usage:

```
account_admin accountAdd <user>'<password|hash>' <role>
<type>
```

Optional `<-role sysadm|secadm|guest*> (default sysadm)`

Optional `<-type temp|user*> (default user)`

User can change the Password of the new Account
`account_admin accountPwMod <user>'<password|hash>'`

User can verify the Password of the new Account
`account_admin accountVer <user> '<password>'`

User can delete the new Account (default accounts cannot deleted)
`account_admin accountDel <user>`

User can verify that new Account is created
`account_admin accountDsp <user>`

Description:

This script supports EZipAPI library user administration and maintenance.

It returns results from OSV account config utility: `account_admin`

Note: Password hash should be in single quotes.

Note: Password hash can't have single quote.

Options:

`-h, -help Print help.`

`account_config` - OSV user account administration

##

Usage:

```
account_config-add<username>-pwd'<string>'-role
<x> -type <x>
```

Optional `[-role sysadm|secadm|guest*] (default sysadm)`

Optional `[-type temp|user*] (default user)`

User can change the Password of the new Account
`account_config -modify <username> [-pwd '<string>']`

User can verify the Password of the new Account
`account_config -verify [username] [-pwd '<string>']`

User can delete the new Account (default accounts cannot deleted)
`account_config -delete <username> [-node n]`

User can verify that new Account is created
`account_config -display [username]`

Description:

This script supports EZipAPI library user administration and maintenance. It returns results from OSV account config utility: `account_config`

Note: Password hash should be in single quotes.

Note: Password hash can't have single quote.

Options:

```
-h, -help                Print help
```

##

Create each user with the role and password expiration criteria as identified in the data collection phase.

7.5.3 Modifying Node Names

If the upgraded nodes (or node) have names that do not meet node naming standards (For naming convention details, click this link to go to page 58), then the node names must be modified to meet the naming standards. Use the IFgui tool in Update mode to change the node names (or name).

Refer to the following:

- The section titled, *Important Information for "Easy IP Address Changing"* in the current release note for OpenScape Voice for information regarding the use of the IFgui tool.
- Appendix 13, "Updating the Node.cfg File (Also Known as EZIP)" for an overview and procedure for updating the node.cfg file.

If you have questions regarding the use of the IFgui tool, contact your next level of support.

7.5.4 Take File System and Database Backups

As described in the *OpenScape Common Management Platform Vx, Administrator Documentation* (where *x is the software release version*), in the *Backup and Restore Concept* section, perform the following:

- Create a database backup

Create a file system backup of each node.

7.5.5 Synchronize the OpenScape Voice Partitions

When satisfied that the upgrade has been successful, there is the potential to also synchronize the OpenScape Voice partitions. This activity can be accomplished as follows;

Warning: Once the upgrade completes successfully, it is noted that the active partition contains the latest fixes to a number of issues of the previous state of the system (e.g. bugs, vulnerabilities etc.), but the fallback partition still contains these issues. Therefore, and in order to eliminate any possibility of activating that fallback partition by mistake, it is strongly recommended to synchronize the active partition to the fallback one immediately after the successful upgrade or as close to it as possible.

Note: There is no need to execute a **Synchronize** action on node 1 and node 2 of a duplex OpenScape Voice deployment. The **Synchronize** action described here will synchronize the partitions in both nodes of a duplex OpenScape Voice.

- Log into the CMP.
- Click the **Maintenance** tab and navigate to **Inventory > Nodes & Applications > Nodes**.
- In the 'Nodes' display, click the OSV node. If this is a duplex system, then select node 1.
- In the OSV Dashboard, under **Actions**, click the **Synchronize** button.
- The 'Synchronize Versions' popup will be presented indicating the OSV partitions will be synchronized. Click the **OK** button to synchronize the partitions or click the **Cancel** button to return to the Dashboard without synchronizing the partitions.

  If you choose to click the **OK** button, the 'Synchronize Versions' popup will display the synchronization progress.

8 Upgrades to OpenScape Voice V11

Attention: When servers (e.g., media server or DLS) in the same network as one of the OSV subnets need to communicate with another of the OSV subnets, then changes to the network firewall are required to allow this communication. Any questions should be addressed to the next level of support.

Attention: Ensure that SIP-Q connections are configured to use the TCP or TLS transport before you begin the upgrade. For a SIP-Q GW (for example, HG3540): ensure the transport type = TCP or TLS (no UDP). Ensure that GW calls complete successfully (inbound and/or outbound) before you begin the upgrade if you update the configuration.

During an installation or an upgrade process, the hard disk drives for each node are divided into two partitions of equal size. These HDD partitions are referred to as the ‘Primary’ partition and the ‘Secondary’ partition.

The partition on which the running software resides is called the ‘Active’ partition (this could be either the ‘Primary’ or ‘Secondary’) and the other partition is called the ‘Fallback’ partition (also referred to as the ’standby’ partition).

Should the Active partition become unstable during the upgrade, one option is to recover by booting off of the Fallback partition that contains the backup (contact your next level of support for assistance).

Before upgrading, make sure that /tmp and / (rootfs) partitions have at least 700 MB of free disk space each. Furthermore, run RapidStat as it will produce warnings/errors/alarms and will give you a good overview of the system's condition and if an upgrade can be performed without any actions.

To determine the contents of the active and passive partitions, execute as user *root*;

 # /unisphere/srx3000/srx/bin/sync8k -v

Note: When upgrading to V11, copy the krb5.keytab file from the source release on a Windows machine and manually restore the file to the same folder on the target release as soon as the update is completed.

Warning: Once the upgrade completes successfully, it is noted that the active partition contains the latest fixes to a number of issues of the previous state of the system (e.g. bugs, vulnerabilities etc.), but the fallback partition still contains these issues. Therefore, and in order to eliminate any possibility of activating that

fallback partition by mistake, it is strongly recommended to synchronize the active partition to the fallback one immediately after the successful upgrade or as close to it as possible.

8.1 Procedure Descriptions

Attention: If you have not already done so, read Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11” before using the procedures in this chapter.

The procedures in this chapter provide instructions on how to upgrade the software from V9/V10 to V11. The procedures provide instructions to upgrade standard duplex and simplex systems.

The procedures require preparatory steps that need to be executed before performing the upgrade and detailed descriptions of the commands and outputs that are associated with the upgrade procedure. System outputs shown throughout the procedures are examples only and might deviate slightly from the actual output.

There is an operational impact as a result of the upgrade. For more details, see Section 8.1.5, “Outage Free Toolkit Upgrade (Live Upgrade) Operational Impacts”.

Review the actual upgrade procedure for tasks that may be performed prior to the upgrade maintenance window.

The actual upgrade as described in Section 8.5.2, “Upgrade Steps for an Integrated Simplex System”, on page 476, or Section 8.6.2, “Upgrade Steps for a Duplex System”, on page 486 is to be performed during a maintenance window.

The upgrade procedures include several fallback points. Fallback instructions are provided in Section 8.9, “Fallback Procedures”.

Note: The update and upgrade procedures of the Integrated OSV both apply to the simplex OSV server of the OpenScape Enterprise Express as well.

8.1.1 Applicable Upgrade Scenarios

Note: After you complete the applicable procedure for your scenario, refer to Section 7.4, “Completing the Upgrade/Migration to V11”, on page 428.

The procedures in this chapter apply to the following upgrade scenarios:

- Integrated simplex: V9/V10 single-node OSV with integrated V9/V10 Applications to V11 single-node OSV with integrated V10 OpenScape Applications.
- Standard duplex: V9/V10 redundant OSV with external V9/V10 Applications server to V11 redundant OSV with external V10 OpenScape Applications server.

8.1.2 Preparation Checklist

Note: Recommended practice for file transfer
1. If a checksum, md5sum or sha file is delivered with OpenScape software it is a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. When necessary, you can use third party software to calculate these values.

- Ensure that all items are available before you start the procedure.
- Read the release notes before you start the procedure.
- Read the entire procedure applicable to your scenario before you start the procedure.
- Ensure that the network configuration requirements for the system configuration type (co-located nodes or geographically separated nodes) are met before beginning the upgrade. Refer to Chapter 12 of the *OpenScape Voice, Design and Planning Manual, Volume 3, SIP Network Planning* for more information.

  Specifically, ensure that each of the bonded Ethernet pairs are assigned to a separate IP subnet (collision domain) within the reserved address range. The upgrade will fail if this requirement is not met.

The following task list describes all the required files and documents that have to be available before the start of an upgrade.

Item Number	Description	Available
1.	• OpenScape Voice V11 Image ISO • The capability to download files (i.e., OSV ISO image, Migration Toolkit, etc) to the /repository/upload folder of the OSV node(s).	
2.	**Note:** Applications are included in the Integrated Simplex OSV installation.	
3.	For Integrated Simplex upgrade or migration, you will be asked in one of the steps to copy and edit the Response file: /enterprise/servicetools/install/conf/responsefile.txt You need to know the Symphonia administrator password (parameter SI_SYMPHONIA_ADMIN_PASSWORD) and the Solid DB password (parameter SI_DB_LOGON_PASSWORD) because these passwords are encrypted in this file and they need to be changed to clear text. If you don't know these passwords, please contact your next level of support.	
4.	• SLES 15 OS and SP distribution approved for external Applications Server installations (if necessary). Please refer to the OpenScape Applications release notes for the latest approved Operation System SLES distribution, or • For VMs (external Application serve), ISO files of the SLES 15 OS and SP distribution.	
5.	Unless directed otherwise by Release Notes, the V11 target OpenScape Voice server should be at the latest patch level declared for General Availability Voice server should be at the latest patch level declared for General Availability.	

Table 17 Preparation Checklist

Item Number	Description	Available
6.	The latest source release patch sets downloaded from SWS. **It is recommended the source release be at the latest released patch set level before starting the upgrade**. Refer to the Release Notes of the target release for the minimum patch set level the source release should be updated to before the upgrade can take place.	
7.	OpenScape Voice V11 Release Notes	
8.	Latest Migration Toolkit rpm. Consult the Release Notes of the target release for the latest available version.	
9.	Documentation: Refer to Section 8.1.3, “Required Documents”.	

Table 17 Preparation Checklist

8.1.3 Required Documents

In addition to this document, the following documents are required to perform the upgrade.

- The *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide (w*here *x* is the current issue*)*
- The *OpenScape UC Application Vx Configuration and Administration, Administrator Documentation (w*here *x* is the current issue*)*
- The *OpenScape Voice Vx Service, Service Documentation (Vx equals the source release)*
- *OpenScape Voice Vx, Design and Planning Manual, Volume x, SIP Network Planning (w*here *x* is the current issue*)*
- *OpenScape Voice Vx Administration, Administrator Documentation (w*here *x* is the current issue*)*
- *OpenScape Media Server Vx Administrator Documentation (w*here *x* is the current issue*)*
- The *Solutions Upgrade Guide* in e-Doku.
- Release Notes for OpenScape Voice Server V11 Reference Image
- Release Notes for OpenScape Voice Vx Applications DVD

- Release Notes for applicable patch sets
- Any applicable MOPs (if needed)

Note: MOPs are included in the image file and installed automatically during image installation.

8.1.4 Outage Free Toolkit Upgrade (Live Upgrade) Overview

Attention: During an Outage Free Toolkit Upgrade (also known as Live Upgrade), the OpenScape Voice servers need to communicate via the Admin subnets of the nodes. Please be sure that the Admin subnets are functional.

The Outage Free Toolkit Upgrade method provides an upgrade procedure equivalent to the cluster replacement procedure, but without the need for separate cluster hardware.

This upgrade procedure allows upgrade without imposing interworking requirements between old and new versions of third party software, allowing third party upgrades which otherwise would have required a prolonged outage.

Additionally the upgrade procedure does not require the old and new versions of the software to interwork, which reduces development and test effort and simplifies upgrade between multiple release lines at different patch levels.

The Outage Free Toolkit Upgrade method is based on the fact that the cluster is made up of two individual nodes (two separate servers running in active/active mode).

The Outage Free Toolkit Upgrade procedure consists of three main phases: (In the example below, the cluster is running V9 and will be upgraded to V10).

Phase 1: The cluster is running V9 and the RTP is at run level 4.

Preconditions (see Figure 15):

- All processes are up.
- There are no HW alarms.
- All needed patch sets are installed.

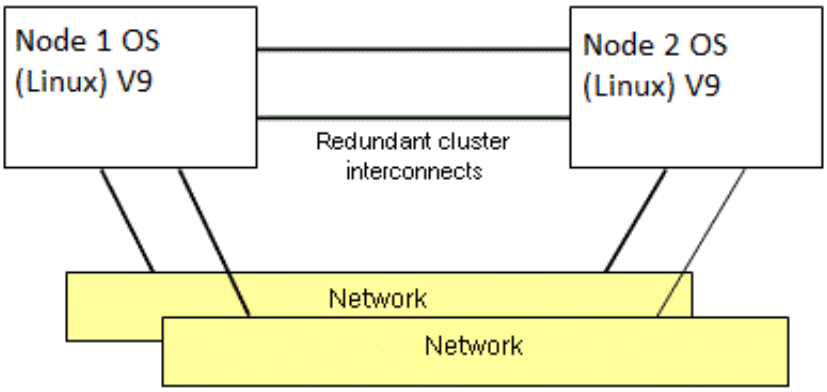


Figure 15 Initial Cluster Configuration

Phase 2: Upgrade Node 1

The interconnects between the nodes are disabled and Node 1 is temporarily isolated from the network. Node 1 is upgraded to the new release. See Figure 16.

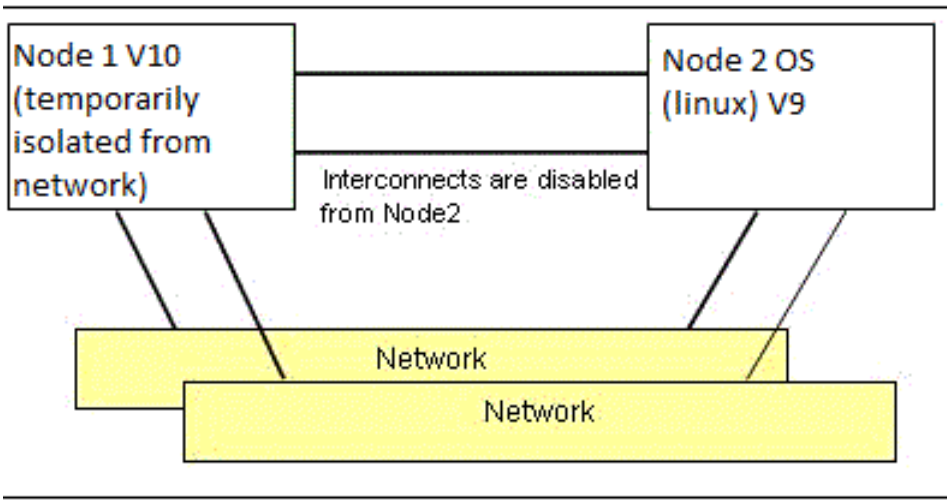


Figure 16 Cluster Configuration After Split

Phase 3: Upgrade Node 2

The redundant cluster interconnects between Node 1 and Node 2 are reestablished and Node 2 is upgraded to the new release. See Figure 17.

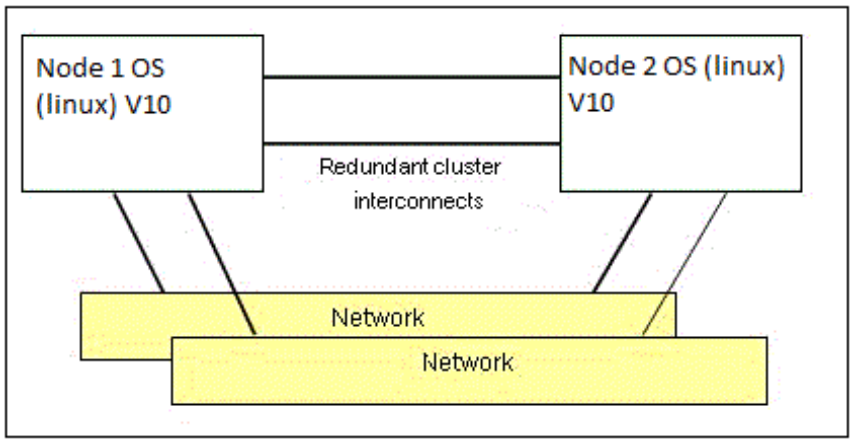


Figure 17 Cluster State after Restore of Node 2

8.1.5 Outage Free Toolkit Upgrade (Live Upgrade) Operational Impacts

8.1.5.1 Provisioning

#	Impact	Duration	Comment
1	Provisioning must be disabled for the period beginning when the database is backed up on Node 2, and ending when Node 1 takes over traffic from Node 2.	2 hours	Generally, no provisioning changes should be done after making backups of the database and file system.
2	Subscriber controlled input (* codes) is disabled after the database is backed up on Node 2, until Node 1 takes over traffic.	2 hours	Item #2 applies to the Outage Free Toolkit method only
3	Users & Resources:	n/a	

Table 18 Operational Impacts – Provisioning

8.1.5.2 Call Processing

Note: Table 19 applies to Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”.

Attention: For existing stable calls, a half call record will be generated when the traffic swings from node 2 to node 1 but no intermediate call records will be generated after the callp switchover to node 1. A call record will be generated when the call is released.

#	Impact	Duration	Comment
1	General Call Behavior - New Originations: During the switch of traffic from the 'old' release to the 'new' release, there will be a short duration where new dial tone will not be available and new calls will be rejected.	< 10 seconds	
2	General Call Behavior - Transient Calls: Calls in the process of being set up on the 'old' release will be lost.	< 10 seconds	
3	General Call Behavior - Mid-call Features: Mid-call features will not operate until the call is released & re-established.	Until all 'old' release calls complete	
4	SIP Calls - Registration data: Registration data that is updated after the database is backed up is lost following the upgrade.	60 minutes	Lost registrations are refreshed after 60 minutes, or when a new call is initiated from the endpoint.
5	SIP Calls - Keysets: Keyset information (stop hunt, make busy etc.) is lost and must be refreshed following the upgrade.	60 minutes	Refresh of keyset data occurs automatically via periodic SUBSCRIBE_NOTIFY
6	SIP Calls - Session Timers: SIP Session timing should be stopped on the source release prior to starting the upgrade to prevent the disruption of established calls during the upgrade. SIP Session timing is activated again after completing the upgrade.	Until call control is switched to the target release.	Calls established on the target release will use Session Timing (if RTP parameter Srx/Sip/ Session_Timer is set to YES)

Table 19 Operational Impacts – Call Processing

#	Impact	Duration	Comment
7	**TLS Subscribers during Upgrade or fallback scenarios:** In case of a controlled failover due to a maintenance procedure OpenScape Voice gracefully closes the TLS connections to all devices and the devices immediately take action and try to reestablish the TLS connection. Media connections are maintained for established calls, and call signaling to a device resumes as soon as the TLS connection for that device is reestablished to the partner OpenScape Voice node.	Until the next device re-registration.	New calls from the phone work properly without restrictions after a new registration from the phone.

Table 19 Operational Impacts – Call Processing

8.2 Prerequisites

8.2.1 System Information and Access Rights

The super user passwords for both cluster nodes will be required during the execution of the upgrade.

Consoles should be opened to each node for the duration of procedure execution.

Remote login as user *srx* or *root* is not permitted. Consequently, the system must be accessed using the default *sysad* user-id, followed by a subsequent login to the *srx* or *root* account, using the *su* command as shown below:

```
<< Logged in as 'sysad' >>
> su - srx
<< Logged in as srx >>
> exit
<< Return to 'sysad' >>
> su -
<< Logged in as 'root' >>
# exit
<< Return to 'sysad' >>
```

8.2.2 Logging

All actions should be logged via console log, the Linux *script* command or other mechanism.

8.2.3 Verify the 'fstab' File Permissions in Virtual OSV Deployments

The installation of VMWare tools may change the permissions of the file */etc/fstab* on the virtual machine. The */etc/fstab* file permissions should be;

```
-rw-r--r-- 1 root root 2558 Sep  7 13:39 /etc/fstab
```

If the permissions are not as indicated above, **as the root user,** change the file permissions with the following command (**be sure to execute the command on both nodes of a virtual Duplex OSV deployment**):

```
# chmod a+r /etc/fstab
```

This change will help prevent any unexpected behavior during an upgrade.

8.2.4 Change vNIC type from E1000 to VMXNET3

OpenScape Voice supports the use of VMXNET3 vNIC driver on all its network interfaces. The VMXNET3 is the latest, most efficient and best supported driver suggested by VMware.

Refer to Appendix 31, “Change E1000 to VMXNET3 network adapters” for information on how to change the driver type in existing installations.

Note: This will incur downtime on Integrated Simplex deployment. On a Standard Duplex deployment the change can be performed without downtime, but the actions still need to be performed within a maintenance window, prior to the upgrade of OSV to V11.

8.3 Preparation Phase

Run the following steps in preparation for the upgrade one week prior to the upgrade.

Note: If ‘route operations’ message windows are presented during the Node.cfg creation, the “OK” button should be selected. For more information regarding the Source Based Routing feature, refer to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11”.

The implementation or updating of source based routes during an upgrade will require the use of a Migration strategy (and therefore a system outage). Migration strategies are detailed in Chapter 9, “Migrations to OpenScape Voice V11”.

For duplex systems, if an OpenScape Voice system outage cannot be tolerated during the upgrade, then the Outage Free Toolkit method (Live Upgrade) will need to be performed. The Outage Free toolkit upgrade method is detailed in Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”, on page 483.

As a general rule, no changes to the OSV target release node.cfg are allowed during the three upgrade procedures detailed in Chapter 8, “Upgrades to OpenScape Voice V11”. After a Chapter 8 upgrade procedure is completed, the EZIP feature can be employed to establish source based routing (by specifying default gateway addresses). For more information regarding the EZIP feature, refer to Chapter 13, “Updating the Node.cfg File (Also Known as EZIP)”.

8.3.1 Create the Node.cfg for the Target System

8.3.1.1 Overview of Creating Node.cfg for the Target Release

The node.cfg file of the target release is automatically generated by the Upgrade/ Migration Toolkit rpm when it is installed on the node(s) of the source release. There is no need for using the NCPE tool to generate the node.cfg file of the target release.

Upon installing the Toolkit rpm on the node(s) of the source release, the conversion of the `node.cfg` file to the target release is automatically initiated by the Toolkit. A host of validation checks are performed on the current **/etc/ hiq8000/node.cfg** file of the source release (e.g., consistency and validity of nafo lines, consistency of networks in routing section with nafo section definitions, etc.). If the node.cfg file passes the validation checks, then versions of all future releases of the node.cfg file will be automatically generated under shared repository **/repository/config/<releaseNumber>**

The conversion is a stepwise process. To convert a node.cfg file from Release(n) to Release(n+2), the Toolkit first converts Release(n) **->** Release(n+1), validates Release(n+1), then converts Release(n+1) -> Release(n+2), etc.

All possible conversions up to the latest release will be attempted. For example, if the current node.cfg is a V9 then the V9, V10 and V11 node.cfg files are generated.

It should be noted that the conversion is also triggered during export of the database.

Handling of New Parameters

When a parameter is not in the current node.cfg file but was added to the node.cfg file of a future release, then the Toolkit stops the conversion and prompts the user to enter the desired value for the parameter. A default value is also presented to the user to use if he desires.

Handling of Deprecated Parameters

When a parameter is in the current node.cfg file but was deleted from the node.cfg file of a future release, then the Toolkit automatically moves the parameter to the Deprecated section in the node.cfg file of the future release.

8.3.1.2 Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release

---

Attention: Always use the latest available version of the Migration Toolkit. The latest version works across all OSV releases. It is independent of the source or the target OSV release version.

For an overview of generating the node.cfg file of the target release by the Migration Toolkit, refer to Section 8.3.1.1, “Overview of Creating Node.cfg for the Target Release”, on page 456.

The following are the detailed steps for generating the node.cfg file of the target release.

1. Remove older installed versions of the migration Toolkit rpm, if any.

   As user *root*:

   ```
   # rpm -qa | grep -i UNSPmigration
   ```

   If an old version of the migration toolkit software is found, then it should be removed with the following command:

   ```
   # rpm -e --allmatches UNSPmigration
   ```

2. Install the latest migration Toolkit rpm.

   As user *root*, download into the **/repository/upload** directory of the source system's nodes (or node for a simplex system) the latest Toolkit rpm (*UNSPmigration-<V#>.rpm)*.

   As user *root*, install the downloaded Toolkit rpm on the source system's nodes (or node for a simplex system):

```
# cd /repository/upload (directory where Toolkit rpm was copied to)
# rpm -ivh --replacefiles --replacepkgs UNSPmigration-<V#>.rpm
```

A node.cfg file for the target release is automatically created on each node's shared repository for all possible future target releases.

The file is: **`/repository/config/<TargetReleaseNumber>/node.cfg`**

3. For a duplex system, repeat steps 1 through 2 of this section on node 2.

Note: The Migration Toolkit tries its best to convert the node.cfg file in folder /etc/hiq8000 and generate a target release node.cfg. If the file has problems, a message is displayed instructing the user to convert the node.cfg to the target release manually.

Refer to Section 8.10, “Resolving Migration Toolkit node.cfg File Creation Issues”, on page 517 for options to resolve issues that prevent the Migration Toolkit from generating the target release node.cfg.

8.3.2 Prepare Files for the Upgrade

8.3.2.1 Prepare Upgrade Files in Repository of OSV Node(s)

Make sure that the directory upload under `/repository` is empty in both nodes, prior to any other action related to the upgrade, such as copy of the necessary files like toolkit, ISO etc. If it’s not empty, delete all existing files, making sure not to delete the directory itself, and then proceed to the following steps.

1. The node.cfg file(s) for the target system were created when the Migration Toolkit was installed on the source system's OSV nodes. The node.cfg file is:
   `/repository/config/<TargetReleaseNumber>/node.cfg`

   From OSV node 1 (or node in simplex), copy the above `node.cfg` file to **`/repository/upload`** folder and rename the file to **`node.cfg.primary`** as follows:

   ```
   # cd /repository/config/<TargetReleaseNumber>/
   # cp -p node.cfg /repository/upload/node.cfg.primary
   ```

   For a duplex OSV system, use command scp or sftp in **Binary** mode to transfer the generated node.cfg file above to **`/repository/upload`** folder of **node 2**. Rename the file to **`node.cfg.secondary`**. The reason for using the node.cfg file from node 1 is to have an exact `node.cfg` file in both nodes for the target release. For example:

   From node 1 of a Duplex OSV system, execute the following commands as user *root*:

   ```
   # cd /repository/upload
   # scp node.cfg.primary  <node2_name or node2_admin_IP_
   address>:/repository/upload/node.cfg.secondary
   ```

2. For an Integrated Simplex OSV system, the response file **`response.cfg.primary`** was copied, edited and saved on a local PC according to the instructions of Section 9.11, “Simplex System response.cfg.primary File Creation”, on page 562.

   After having created the *response.cfg.primary* file on a local PC, sftp the file from the local PC to the Integrated Simplex system and place it in directory **`/repository/upload`**. Then run the following commands as user *root*:

```
# cd /repository/upload
# chmod 600 response.cfg.primary
# chown root:root response.cfg.primary
# dos2unix response.cfg.primary
```

3. Place the OSV license file for the node into **`/repository/upload`** folder. Additionally, for an Integrated Simplex system, place the OpenScapeUC licenses (if UC services are being used) into **`/repository/upload`** folder.

Note: All OpenScape Voice licenses must have the keyword **OpenScape_Voice** in the license file name. Otherwise, the license will not be imported.

All OpenScapeUC licenses must have the keyword **OpenScape** in the license file name. Otherwise, the license will not be imported. The UC licenses only apply to an integrated simplex system.

If the target license file is invalid, it will not cause an automatic fallback but rather the new system will simply be unlicensed. You should obtain new licenses and apply them to the system to resolve the issue.

Note: During an upgrade from a point release to another point release (e.g., from V11 to V11R1) or an upgrade within the same release (e.g., V11 image 2 and/or patch set 4 to V11 image 4 and/or patch set 7), licenses are automatically transferred from the source release to the target release. In this case, new licenses for the target release are not required.

Generally, most upgrades are from one release to another release. In this case, new licenses have to be obtained for the target release as described in Section 8.3.4.

Note: In case of expired licenses, the renewed licenses should be installed to the server prior to the upgrade. License activation will fail, if the expired licenses are copied to the /repository/upload folder.

---

4. Place the latest Migration Toolkit rpm in the **`/repository/upload`** folder, if this has not already been done.

5. Place the patch sets and the emergency patch sets, including the SPA files, in the **`/repository/upload`** folder. Generally, **this means the needed tar files from the latest cumulative patch set and all the tar files of the latest cumulative emergency patch set.**

   For example, if the latest image is delivered with PS07.E02 and PS12.E05 is required as part of the image installation;

- Download all the zip files of cumulative PS12 including the associated SPA file.
- Download all the zip files of cumulative emergency PS12.E05 including the associated SPA file.
- Place all the downloaded tar files and SPA files in the **`/repository/upload`** folder.

Note: Including the SPA file in this step will trigger an md5sum check of the patch sets before they are installed. A patch set md5sum check failure will be reported to the console and the installation will abort. If cumulative patch sets are not available, tar files of the regular patch sets can be placed in the patch directory as well as the related tar files of the emergency patch sets. The standard naming convention of the patch sets must be maintained. **Remember to include the patch set SPA files in order to trigger the md5sum check during the installation.**

You can also place the .zip files that include the cumulative epatches without unzipping them under **`repository/upload`** and proceed with a live upgrade.

Note: The files can be named, for example, `epatchsets.zip` or `V11RX.X.zip`

---

6. Place the OSV image iso file in the **`/repository/upload`** folder.
7. Ensure that an ISO image DVD disk and USB memory stick are not inserted in the server.
8. For a duplex configuration, repeat steps 3 on page 459 through 7 on page 460 for the second node.

Note: In a duplex configuration, ensure that both nodes have the same number of files.

Additionally, ensure that the empty file dev.8kps is either present on both nodes or not present on both nodes. The file is created by the toolkit and it is not a mandatory file to be present.

8.3.3 Verify Prerequisites Met According to Release Notes

The release notes identify the order of the upgrades (Assistant, Media Server, etc.) and all prerequisites and dependencies before upgrading the system. Verify that the specified prerequisites are met. Also prepare any necessary files needed for Applications installation/upgrade (for example: response files, licenses).

Attention: The Response file of an OSV integrated system is built automatically as part of the installation process. A Response file no longer needs to be generated for images and is not required on the USB stick. If a Response file is found on the USB stick, that file will take precedence over the file that is automatically generated via the image installation.

Upgrade or Migration procedures that do require Response files will include a step in their task list indicating a response file should be generated and recommendations for generating the response file.

- For Applications without UC service refer to the appropriate section title in this document;
  - Response File for the Integrated Simplex Deployment
  - Response File for Media Server Standalone
  - Response File for Multiple Communications Server
- For Applications with UC service refer to the appropriate section title in the *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide (w*here *x* is the current version*)*;
  - Example of the Deployment Scenario Standard Duplex (small)
  - Example of the Deployment Scenario Standard Duplex (large)

8.3.4 Obtain Licenses for the Target Release

Before proceeding with the upgrade procedure, obtain licenses for the OSV target release. Additionally, for Applications server(s) obtain UC target release licenses (if UC service is being used on the system). This applies to OSV Integrated Simplex and offboard Applications server(s) with UC features.

Note: Refer to Section 2.2.3, “Backup License Recommendations”, on page 30.

Note: Since OpenScape Voice is an appliance, SW upgrades may include updates of the SUSE SLES operating system.

This requires an **active SUSE Update Subscription license** on the system (for Duplex systems: one per node).

For upgrades from OSV V11 to a future OSV V11 version, this license will also be checked while attempting to upgrade or update the system (major, minor, and fix releases).

Expired or missing **SUSE Update Subscription license** prevents further upgrades of the OpenScape Voice image.

Please check the license status while planning for upgrades / updates and order required licenses in time.

Note: For upgrades from OSV V11 to a future OSV V11 version **an active SSP (Software Support Plan) / SWA (Software Assurance) license** is required.

This license grants customers the right to use new software updates and upgrades, including major, minor, and fix releases, as well as hot fixes.

Expired or missing SSP (Software Support Plan) / SWA (Software Assurance) license prevents further updates / upgrades of the OSV image/hotfix.

Please check the license status while planning for upgrades / updates and order required licenses in time.

For more Information, please refer to Mitel Product Release Lifecycle Policy.

8.4 Pre-Maintenance Window Activities

The following steps must be run prior to the maintenance window to ensure that the system is ready to be upgraded.

8.4.1 Run RapidStat on Both Nodes and Analyze Output

For instructions for running *Rapidstat*, refer to the *RapidStat* chapter in *OpenScape Voice Vx, Service Manual, Service Documentation* (where *x is the software release version)*.

The possible ERRORS, displayed in the Rapidstat report, must be solved before the next OSV Upgrade due to a high risk of Upgrade failure.

8.4.2 Make Test Calls and Document Results

Make test calls and document results so that the result can be compared with the same test calls after the upgrade. Note that test calls for the upgrade may be different than what is required for normal maintenance.

8.4.3 Perform Any Customer Specific System Checks

Perform any customer specific system checks before you continue with the database and system backup.

The OSV system is purged of unused non-system accounts (for security reasons). In order to address this safely and completely it is necessary to document some pre-requisites before the upgrade process begins.

The customer site should determine if any of their custom accounts are in conflict with the "reserved" OSV accounts (and groups) listed below. If so, those customer accounts (or groups) should be removed prior to the upgrade.

Reserved OSV System Account IDs

Account Name	Account ID
reserved	501
sym	502
cdr	1001
srx	1522
solid	5000
superad	10000
sysad	10001
secad	10010
dbad	10011
reserved	10012
webad	10013

Reserved OSV Group IDs

Group Name	Group ID
rtpgrp	911
reserved	912
sym	913
dba	3020
cdrusers	3021
seclog	10001
reserved	10002

8.4.4 Verify Source Release Patch Set Level

Attention: Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability. If this is an integrated system ensure your applications server is updated with the latest released DVD/PatchSet/HotFix.

Based on the OpenScape Voice V11 Release Notes, ensure that the system is at the correct patch set level. If not, install the correct patch sets before starting the upgrade**.**

8.4.5 Perform a Database and File System Backup

For detailed instructions on the backup procedures;

- Refer to the *OpenScape Voice Vx, System Service Manual, Service Documentation* (where x is the release version.)

8.4.6 Verify the Ethernet Configuration of the External Applications Server

To determine which interface is currently being used, log on as *root* user to the external applications server using SSH or the console and enter the following command:

```
# ifconfig
```

If line “inet addr:<IP address of external server>” appears in the eth0 entry then eth0 is being used. If it appears in the eth1 entry then eth1 is being used.

Record this information as it will be needed if communications problems exist after a SLES OS installation/upgrade is completed.

8.4.7 Verify the Hosts File Configuration

Note: Contact your next level of support if you have any questions regarding this verification procedure.

Logic has been implemented for the */etc/hosts* file wherein a new banner, “Please add new hosts under this line”, indicates to OpenScape Voice tools that the *Ipaddress-hostname* entries that appear below the banner are created by the

user. Employing the banner as such allows OpenScape Voice to carry forward user-created entries in the *hosts* file during activities that require the *hosts* file to be rebuilt.

Verify the OpenScape Voice */etc/hosts* file (or files for duplex systems) configuration with the following commands (execute on both nodes in duplex system):

```
# cd /etc
# cat hosts
```

A truncated example of an */etc/hosts* file with the new banner (with no user-created entries) is as follows:

```
10.235.54.10      rtp_com0_eth6
10.235.54.30      rtp_com1_eth6
########################################
# Please add new hosts under this line #
########################################
```

Proceed as appropriate:

- No further action is necessary in the following cases:
  - The source release */etc/hosts* file does not contain user-created entries and the banner is not present (it will be present in the *hosts* file after the upgrade is completed).
  - The source release */etc/hosts* file does not contain user-created entries and the banner is present.
  - The source release hosts file does contain the new banner and all user-created entries **are below** the banner.
- Modify the source release *hosts* file (or files for duplex) if the file contains the new banner but all user-created entries **are not below** the new banner.

  For duplex systems, the */etc/hosts* file of both nodes needs to be updated. Duplicate entries in the */etc/hosts* file should be avoided.

  In the following example, the *nmcsnmptrap* and *host_pc* are user-created entries in the *hosts* file containing the new banner. If a user-created entry needs to be moved from above the banner, place it as the last line (bottom of the list below the banner) in the */etc/hosts* file. Remember to update both */etc/hosts* files in a duplex system.

  ```
  10.235.54.10      rtp_com0_eth6
  10.235.54.30      rtp_com1_eth6
  ########################################
  # Please add new hosts under this line #
  ########################################
  10.235.200.230    nmcsnmptrap
  10.235.200.29     host_pc
  ```

- Copy and save the source release */etc/hosts* file (or files for duplex) to a safe location (not on the OpenScape Voice server!) if it **does not** contain the new banner (as shown above) **and** it contains user-created entries.

Copy and save duplex system *hosts* files with names indicative of which node the *hosts* file is saved from (for example: *hosts_n1* and *hosts_n2*). After the upgrade is complete, the new banner will be present in the target release */etc/hosts* file of the OpenScape Voice server and you can use the source release *hosts* file (or files for duplex) you saved to rebuild the user-created entry list in the target release */etc/hosts* file.

Attention: When servers (e.g media server or DLS) in the same network as one of the OSV's subnets need to communicate with another of the OSV's subnets, then changes to the network firewall are required to allow this communication. Any questions should be addressed to the next level of support.

8.4.8 Verify Presence of IP Address and FQDN of External CMP

For a duplex OSV system, the IP address and FQDN of the external (offboard) CMP should be defined on both OSV nodes in files:

`/etc/security/access.conf`

and

`/etc/hosts`

to allow proper access to the OSV nodes by the CMP.

For verification and modification if required, refer to Section 4.5.2, “Verify Remote Access for srx Account in a Standard Duplex”, on page 339.

8.4.9 Save Cron Tables Data

1. There are two Cron tables; One for user ***root*** and another for user ***srx***.

   The Cron tables are different on each node and for each of the above two users.

   a) List and save the Cron table for user '*root*' on the first node.

   ```
   # crontab -u root -l          (u=user, l=list cron table)
   # crontab -u root -l > /tmp/crontab_root_node1
   ```

   Save file `/tmp/crontab_root_node1` to an external location.

   b) List and save the Cron table for user '*srx*' on the first node.

   ```
   # crontab -u srx -l           (u=user, l=list cron table)
   # crontab -u srx -l > /tmp/crontab_srx_node1
   ```

   Save file `/tmp/crontab_srx_node1` to an external location.

   c) List and save the Cron table for user '*root*' on the second node (only applies to an OSV duplex system).

   ```
   # crontab -u root -l          (u=user, l=list cron table)
   # crontab -u root -l > /tmp/crontab_root_node2
   ```

   Save file `/tmp/crontab_root_node2` to an external location.

   d) List and save the Cron table for user '*srx*' on the second node (only applies to an OSV duplex system).

   ```
   # crontab -u srx -l           (u=user, l=list cron table)
   # crontab -u srx -l > /tmp/crontab_root_node2
   ```

   Save file `/tmp/crontab_srx_node2` to an external location.

8.4.10 Save CLM Data for an Integrated Simplex System

For an integrated simplex system, if CLM (Customer License Manager) is installed, the ClmSettings.xml file must be saved prior to starting the upgrade and then restored after the upgrade is completed.

Save to an external location file `/enterprise/clm/ApacheTomcat/ClmSettings.xml`. This file contains the access configuration for the CLM.

Note: For a duplex configuration, the ClmSettings.xml file is stored on the offboard Application server and the upgrade steps of the offboard server mentions saving the file prior to starting the upgrade.

8.4.11 Executive Assistant with Cockpit

If your Applications employ the Executive - Assistant with Cockpit feature, the source release '.eag' files must be backed up to an external server for restoral after the upgrade.

The files are found on the Simplex OpenScape Voice Integrated Applications server at:

/enterprise/HiPathCA/WebSpace/Portal/webapps/eacockpit-osc/WEB-INF/groups

The files are found on the External Applications Server(OFFBoard) server at:

/opt/siemens/HiPathCA/WebSpace/Portal/webapps/eacockpit-osc/WEB-INF/groups

In the target release, these .eag files will be copied to the upgraded Applications server.

8.4.12 Disable SIP Session Timer

For Outage Free toolkit upgrade, the SIP Session timer needs to be disabled before starting the upgrade. Calls that were started before the SIP Session timer is disabled might be disconnected during the upgrade. Stable calls started after the SIP Session timer is disabled will continue unaffected by the upgrade.

The Upgrade/Migration toolkit disables the SIP Session timer when it starts the upgrade. However, calls started several minutes before starting the upgrade might get disconnected. Thus, disabling the SIP Session timer sometime before starting the upgrade ensures that stable calls initiated a short time before starting the upgrade are not affected by the upgrade.

You must remember the initial SIP Session timer setting because you must restore the setting after the Outage Free toolkit upgrade is completed.

StartCli has to be used to change the SIP Session timer setting as follows:

Using startCli:

- As user *srx*, type startCli
- Select option 1 - Configuration Management
- Select option 1 - Configuration Parameters
- Select option 2 - Get Parameter Info
- Enter parameter name: Srx/Sip/Session_Timer

If value = YES (enabled), then change the value to disable it

- Select option 3 - modifyParameter
- Enter parameter name: Srx/Sip/Session_Timer
- Enter value: NO

The SIP Session timer setting can be changed from startCli as indicated above or from Assistant as follows:

- Login onto CMP
- Click Configuration tab
- OpenScape Voice > Administration > General Settings > RTP
- From the dropdown menu of the "in" field, select Name
- In the "search" box, enter: Srx/Sip/Session_Timer
- Click on the Search button
- Click on the Srx/Sip/Session_Timer and change the setting to **NO**

8.4.13 List the Languages Installed on the Applications Server

Use the syntax appropriate for your Applications installation to list the installed language packages. Execute the command as the root user.

For Integrated Simplex systems;

```
# zypper se --match-any announ uc-tts uc-asr languagepack
```

For Offboard (external) Applications servers;

```
osc-setup --match-any announ uc-tts uc-asr languagepack
```

For Simplex systems, after the successful Upgrade or Migration, the English language will be installed by default. Any other languages will have to be installed. Store this command result for a reference of the required languages. If you have not already done so, review Appendix 28, “Guidelines for Language and Application Package adds to Simplex Systems” on page 783 for more details. To

expedite the installation of the additional language packages, it is recommended you know which language packages are necessary for installation after the successful Upgrade or Migration procedure is executed.

This process is not typically necessary for Offboard (external) Applications servers because language package upgrades should be included in the Offboard Applications server Upgrade. The list could be collected as a point of reference in case there are suspected issues after the successful Upgrade or Migration.

8.4.14 Record any Scheduled CMP Backup or Export Tasks

Before you upgrade, check whether there are scheduled CMP backup or export tasks (see the administrator documentation *OpenScape Common Management Platform*). Record any scheduled backup or export tasks. Backup unit names may get lost during an upgrade. Such scheduled tasks must be recreated after an upgrade.

8.5 Upgrade of an OSV Integrated Simplex System

8.5.1 Overview

Attention: If custom certificates, for example for WebClient secure access, have been stored under directories other than the default ones, back up these certificates prior to the upgrade and restore them to those specific directories after the upgrade. For certificates stored in their default locations, see information below on **Additional Certificate Backup Requirement.**

Additional Certificate Backup Requirement:

The following certificates must be backed up even when stored in their default locations, as they will be regenerated during the upgrade process:

- CMP HTTPS certificate

(/enterprise/common/conf/tomcat-keystore.p12)

- SPML responder HTTPS certificate

(/enterprise/common/conf/spmlresponder-keystore.p12)

To preserve these certificates:

1. Back up the certificate files from /enterprise/common/conf/
2. Back up the configuration file /enterprise/share/tomcat/conf/server.xml to preserve certificate passwords

After the upgrade, restore these files to their original locations.

Note: The WebClient certificate will be preserved during the upgrade process when stored in default locations. For other certificates (such as BCOM or Media Server certificates), please consult their respective component documentation for upgrade behavior.

Upgrading the Integrated Simplex system

There are four methods for upgrading an Integrated Simplex system. An outage occurs in all simplex upgrade methods because outage is inevitable with a single server. The upgrade methods are:

1. **Starting the upgrade from the CMP/Assistant (User Interface (UI) Method).**

   This upgrade method can be summarized as follows:

   - **The upgrade from the CMP/Assistant is the preferred upgrade method.**
   - This method can be used for upgrading a native or a virtual Integrated Simplex configuration.
   - **The user starts the upgrade from the CMP/Assistant.** The upgrade process continues without further user interaction. Both the OSV and the Applications are upgraded.
   - All the necessary files that are needed for the upgrade are stored on the repository of the node.
   - The upgrade duration of an Integrated Simplex system using the CMP/Assistant is approximately 1:30 hours with system downtime of approximately 1:15 hours. The time duration may differ depending on the database size or the number/size of the additional patch sets.
   - At the end of a successful upgrade, the Migration Toolkit automatically collects the log files and places them in a single compressed file named `"data-<clusterName>.tar.gz"` in the `/log` directory.
   - The CMP/Assistant displays a status that upgrade is in progress in several screens ensuring that other users know the status of the OSV system. Also, another OSV upgrade cannot be started while an upgrade is already in progress. Additionally, the OSV nodes on the CMP's dashboard are grayed out thus disabling any action on the OSV nodes while the upgrade is in progress.

- If an error occurs during the upgrade, the system automatically falls back to the source release. Additionally, the user can initiate the collection of data files from the Assistant for the analysis of the error.

For this type of upgrade, refer to Section 8.5.2, “Upgrade Steps for an Integrated Simplex System”, on page 476.

2. **Starting the upgrade from the node's console or VM console with upgrade files on node's repository**

   This upgrade method can be summarized as follows:

   - This method can be used for upgrading a native or a virtual Integrated Simplex configuration.
   - The user starts the upgrade by entering a line command on the node's console or VM console. The upgrade process continues without further user interaction. Both the OSV and the Applications are upgraded.
   - All the necessary files that are needed for the upgrade are stored on the repository of the node.
   - The upgrade duration of an Integrated Simplex system using this method is approximately 1:30 hours with system downtime of approximately 1:25 hours. This includes upgrading the OSV and the applications. The time duration may differ depending on the database size or the number/size of the additional patch sets.
   - If an error occurs during the upgrade, the system automatically falls back to the source release. Additionally, the system automatically collects logs and data files for the analysis of the error.

   For this type of upgrade, refer to Section 8.5.2, “Upgrade Steps for an Integrated Simplex System”, on page 476.

3. **Starting the upgrade from the node's console with upgrade files on external media**

   This upgrade method can be summarized as follows:

   - This method can be used for upgrading a native Integrated Simplex configuration only.
   - The user enters a line command on the node's console to export the data to the USB memory stick. The user then enters a command on the console to start the upgrade. The upgrade only upgrades the target software using the target ISO image but does not import the data of the source release. After the upgrade, the user logs into the console and may install Applications' Hotfixes, if required. The user then enters a command to import the data of the source release.
   - All the necessary files that are needed for the upgrade are stored on external media like a USB memory stick.
   - The upgrade duration of an Integrated Simplex system using the Console method (data export, image install, and data import) takes approximately 1:10 hours with a system downtime of approximately 1:00 hour. The time duration may differ depending on the database size or the number/size of the additional patch sets.

- If an error occurs during the upgrade, the user must initiate fall back to the source release. Additionally, the user must also initiate the collection of log and data files for the analysis of the error.

For this type of upgrade, refer to Section 8.5.2, “Upgrade Steps for an Integrated Simplex System”, on page 476.

4. **Starting the Upgrade Remotely (Remote Software Upgrade)**

   This upgrade method can be summarized as follows:

   - This method can be used for upgrading a native or a virtual Integrated Simplex configuration.
   - This method does not require service personnel to be present at the customer's site to perform the upgrade. The RSA interface is utilized for a native system while the Virtual Machine (VM) console is utilized for a virtual system.
   - The user uses SFTP file transfer in **Binary** mode to transfer the upgrade files (i.e., OSV image, node.cfg, license file, Migration Toolkit rpm and additional patches) to the /repository/upload folder. External media like a DVD disk and a USB memory stick are not needed.
   - The user starts the upgrade by entering a line command on the node's console via the RSA interface or the VM console.
   - The upgrade duration of an Integrated Simplex system using Remote Software Upgrade takes approximately 1:30. The time duration may differ depending on the database size or the number/size of the additional patch sets.
   - If an error occurs during the upgrade, the user must initiate fall back to the source release. Additionally, the user must also initiate the collection of log and data files for the analysis of the error.

   For this type of upgrade, refer to Section 8.7.2, “Upgrade Steps for Remote SW Upgrade”, on page 493.

8.5.2 Upgrade Steps for an Integrated Simplex System

Attention: When servers (for example, media server or DLS) in the same network as one of the OSV's subnets need to communicate with another of the OSV's subnets, then changes to the network firewall are required to allow this communication. Any questions should be addressed to the next level of support.

Attention: No modifications to the voice server hardware, product type or deployment are expected in this procedure. If the voice server hardware, product type or deployment is to be changed a procedure from Chapter 9, “Migrations to OpenScape Voice V11”, should be employed for the upgrade.

Attention: When you have an integrated simplex and the UC version of the source has been upgraded to a higher version than the one of the target, then perform the steps from Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11”.

Table 20 on page 477 describes the upgrade procedure. Some steps describe specifications to be performed by the user depending on the upgrade method that is chosen. Checklist tasks 1to 7, on pages 531 to 642 can be performed, prior to the upgrade maintenance window.

Hint: When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader tool bar. This will ease the navigation between the checklists and associated sections of the IUG.

After executing a checklist task, select the ‘Previous View’ icon in the Reader toolbar to return to the checklist.

The task list below describes the upgrade steps.

.

Task	Description
1.	Refer to Section 8.1.2, “Preparation Checklist”, on page 445 and Section 8.1.3, “Required Documents”, on page 447.
2.	Refer to Section 8.2.1, “System Information and Access Rights”, on page 454 and Section 8.2.2, “Logging”, on page 454.
3.	Refer to Section 8.3.3, “Verify Prerequisites Met According to Release Notes”, on page 461 and Section 8.3.4, “Obtain Licenses for the Target Release”, on page 462. **Note:** During an upgrade from a point release to another point release or an upgrade within the same release licenses are automatically transferred. In this case, new licenses are not required. Most upgrades are from one release to another release (e.g., from V10 to V11). In this case, new licenses have to be obtained as described in Section 8.3.4
4.	Refer to Section 8.4, “Pre-Maintenance Window Activities”, on page 463. Perform all the activities in the subsections of Section 8.4 that may apply to your configuration.
5.	Copy the krb5.keytab file from the source release on a Windows machine.
6.	Create the node.cfg file for the target system by downloading and installing the latest Migration Toolkit rpm on the source system which automatically generates the node.cfg file for the target system. Refer to Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457.

Table 20 Simplex Upgrade

Task	Description
7.	Prepare the upgrade files using one of the methods below. It is very helpful to mark the method that you are going to select to refer back to it in later steps: a) **For a native or a virtual Integrated Simplex system**, the upgrade files are stored on the node's repository (i.e., without using external media like DVD disk and USB memory stick), prepare the upgrade files as described in Section 8.3.2.1, “Prepare Upgrade Files in Repository of OSV Node(s)”, on page 458. **This is the preferred method.** Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability.
8.	Run RapidStat on the source system prior to the upgrade. Errors and/or Warnings must be reviewed and corrected as necessary before continuing.
9.	For virtual machines only, the resource allocation of target release virtual machines must be verified against Table 13 on page 251, "Virtualization Dimensioning Details " of the target release OpenScape Voice Installation and Upgrade Guide (IUG). The resource allocation of the virtual machine(s) must be adjusted to the values listed in Table 13 on page 251, of the target release IUG before the upgrade begins. --- **Attention:** Some virtual machine resource changes require the machine be shut down (e.g. vCPU and Memory resources changes). This activity will cause a loss of service for the Integrated Simplex OSV and its Applications server. If an outage is not allowed for the Standard Duplex virtual system; the Duplex system virtual resource allocation update must be performed by first shutting down one node (i.e.; node 1), updating that node's VM resource allocations, and then restoring that node to state 4. After one node is updated and restored to service the partner node (i.e.; node 2) can be shut down, updated, and restored to state 4. Normal operating procedures for updating a Integrated Simplex or Standard Duplex system should apply too. ---

Table 20 Simplex Upgrade

Task	Description
10.	**For virtual machines only**, execute the following command on the OSV node of a simplex deployment: **`# ls -l /mnt`** Verify the *cdrom* directory is NOT listed on the OSV node of a Simplex deployment. An example result with the *cdrom* directory listed follows: **`root@bocast4a:[~] #164`** **`# ls -l /mnt`** **`total 4`** **`drwx------ 2 root root 4096 Nov 20 17:13 cdrom`** **`root@bocast4a:[~] #165`** **`#`** IF the *cdrom* directory IS NOT PRESENT, THEN proceed to step 11 on page 479 now. IF the *cdrom* directory IS PRESENT, THEN execute the following command (as the root user); `# rmdir /mnt/cdrom` You can verify your work by executing the ***`ls -l /mnt`*** command once more. After removing the *cdrom* directory, proceed to step 11 on page 479.
11.	**For virtual machines only**; the installation of VMWare tools may change the permissions of the file */etc/fstab* on the virtual machine. The */etc/fstab* file permissions should be; `-rw-r--r-- 1 root root 2558 Sep  7 13:39 /etc/fstab` If the permissions are not as indicated above, **as the root user,** change the file permissions with the following command (**be sure to execute the command on both nodes of a virtual Duplex OSV deployment**): **`# chmod a+r /etc/fstab`** This change will help prevent any unexpected behavior during an upgrade.

Table 20 Simplex Upgrade

Task	Description

12.	Manually restore the file to the same folder on the target release as soon as the update is completed.
	run as user root
	`chown sym:sym  krb5.keytab`
	`chmod 777 krb5.keytab`

13.	Start the upgrade using one of the following methods: **a) Start the upgrade from the CMP/Assistant (UI Method):** This method applies to native or virtual Integrated Simplex configuration. Outage will occur since it is inevitable with a single server. This method requires that the user had selected option a) in step 7 on page 478. This is the preferred upgrade method. The user starts the upgrade from the CMP/Assistant. Both the OSV and the Applications are upgraded with minimal input from the user. If an error occurs during the upgrade, the system automatically falls back to the source release with minimal prompts to the user. To invoke this upgrade method, refer to Section 8.8.1, “Simplex Configuration: Invoke Upgrade from the CMP/Assistant (UI Method)”, on page 498.

Table 20 Simplex Upgrade

Task	Description
	b) **Start the upgrade from the node's console or VM console with the upgrade files on the node's repository:** This method applies to native or virtual Integrated Simplex configuration. Outage will occur since it is inevitable with a single server. **This method requires that the user had selected option a) in step 7 on page 478.** The user starts the upgrade by entering a line command on the node's console. Both the OSV and the Applications are upgraded with minimal input from the user. If an error occurs during the upgrade, the system automatically falls back to the source release with minimal prompts to the user. To invoke this upgrade method, refer to Section 8.8.2, "Simplex Configuration: Invoke Upgrade from Console or VM Console with Upgrade Files on Node's Repository", on page 500. c) You can perform an upgrade through the OpenScape Composer also. For detailed information please consult the document *OpenScape Composer Vx Administration, Administrator Manual,* chapter **Software Updates**.

14.	Reconfigure the web client in an integrated simplex.
	
	`# /etc/init.d/symphoniad stop`
	
	`#/enterprise/HiPathCA/bin/reconfiguration.sh`
	
	`# /etc/init.d/symphoniad start`

15.	An integrated system should ensure that the Applications server is updated to the latest released DVD/PatchSet/HotFix. If an Applications PatchSet (Update) or HotFix is required, please refer to Section 5.2.3.5, "Update/Upgrade of Integrated Applications", on page 310 or Section 5.2.3.6, "Installing a HotFix - Integrated Apps server", on page 313.

Table 20 Simplex Upgrade

Task	Description
16.	Add additional languages. For an Integrated Simplex system, after the successful Upgrade, the English language will be installed by default. Any other languages will have to be installed by the user. As a part of the pre-maintenance window preparation of Section 8.4.13, “List the Languages Installed on the Applications Server”, a list of required languages should have been collected. Reference Appendix 28, “Guidelines for Language and Application Package adds to Simplex Systems”, on page 783 for more details.
17.	Run RapidStat after a successful upgrade. Verify there are no issues and that the system is functioning correctly. **Note:** If it is determined that the upgrade of the system is unsatisfactory, fall back to the source release. Refer to Section 8.9.3, “Manual Fallback on Failed Upgrade”, on page 509.
18.	Remove the Migration Toolkit software (UNSPmigration-<V#>.rpm) from the target system. Refer to Section 9.7, “Remove the Migration Toolkit Software from the Target System”, on page 554.
19.	Complete the upgrade. Refer to Section 7.4, “Completing the Upgrade/ Migration to V11”, on page 428.
20.	After the upgrade, the Openfire server has to be reconfigured. For detailed information, see chapter "Configuring the Connection to the Openfire Server" of *OpenScape UC Application, Installation and Upgrade, Installation Guide*.

Table 20 Simplex Upgrade

Configuring the parameter XMPP Server Name

After re-configuration of the Openfire server, the parameter **XMPP Server Name** is empty and you must configure it. Follow the steps below:

1. Log in to the IP of the Integrated Simplex via the CMP
2. Navigate to **Maintenance > Inventory > Nodes**

   The list of Nodes is displayed.
3. Click the node name of the Simplex
4. A pop-up window appears. In the **Actions** field, click **Show:** Services status
5. A pop-up window **List of components** appears. In the **Filter** box, type "Presence XMPP Integration - Connector" and click **Go**.
6. Click the component **Presence XMPP Integration - Connector**

7. The **Edit Service Configuration** pop-up window appears
8. Configure the parameter **XMPP Server Name** with the XMPP-domain name.
9. Click **Save**

8.6 Upgrade of an OSV Duplex System Using Live Upgrade

8.6.1 Overview

There are three methods for Live Upgrade (also known as Outage Free Upgrade) of a duplex OSV system. They are:

1. **Starting the upgrade from the CMP/Assistant.**

   This upgrade method can be summarized as follows:

   - **The upgrade from the CMP/Assistant is the preferred upgrade method.**
   - This method can be used for upgrading a native or a virtual duplex OSV configuration.
   - The user starts the upgrade from the CMP/Assistant. Node 1 is upgraded first, the calls are switched to node 1 and then node 2 is upgraded. All these steps are performed sequentially without stoppage and without any input from the user.
   - All the necessary files that are needed for the upgrade are stored on the repository of each node.
   - The upgrade duration of an OSV duplex system using the CMP/Assistant is approximately 1:25 hours. The time duration may differ depending on the database size or the number/size of the additional patch sets.
   - Upgrading the Applications of a UC Standard Duplex Small deployment takes additional 1:20 hours.
   - At the end of a successful upgrade, the Migration Toolkit automatically collects the log files and places them in a single compressed file named "`data-<clusterName>.tar.gz`" in the `/log` directory. The single compressed file contains data from both nodes and is placed in the `/log` directory of **node 1.**
   - From the same CMP, it is possible to initiate an upgrade of more than one OSV system simultaneously.
   - The CMP/Assistant displays a status that an upgrade of the OSV is in progress in several screens ensuring that other CMP users know the status of the OSV system. Also, another OSV upgrade of the same OSV

cannot be started while an upgrade is already in progress. Additionally, the OSV nodes on the CMP's dashboard are grayed out thus disabling any action on the OSV nodes while the upgrade is in progress.

- If an error occurs during the upgrade, the system automatically falls back to the source release. Additionally, the user can initiate the collection of log and data files from the Assistant for the analysis of the error.

For this type of upgrade, refer to Section 8.6.2, “Upgrade Steps for a Duplex System”, on page 486.

2. **Starting the upgrade from node 1's console or VM console with upgrade files on nodes' repository.**

   This upgrade method can be summarized as follows:

   - This method can be used for upgrading a native or a virtual duplex OSV configuration.
   - The user starts the upgrade by entering a line command on node 1's console or VM Console. Node 1 is upgraded first; the calls are switched to node 1, and then node 2 is upgraded. All these steps are performed sequentially without stoppage and without any input from the user.
   - All the necessary files that are needed for the upgrade are stored on the repository of each node. Thus, the use of DVD disks and USB memory sticks is eliminated.
   - The upgrade duration of an OSV duplex system using the Console method is approximately 1:25 hours. The time duration may differ depending on the database size or the number/size of the additional patch sets.
   - Upgrading the Applications of a UC Standard Duplex Small deployment takes additional 1:20 hours.
   - If an error occurs during the upgrade, the system automatically falls back to the source release. Additionally, the system automatically collects log and data files for the analysis of the error.

   For this type of upgrade, refer to Section 8.6.2, “Upgrade Steps for a Duplex System”, on page 486.

3. **Performing Remote Software Upgrade**

   This upgrade method can be summarized as follows:

   - This method can be used for upgrading a native or a virtual duplex configuration.

- **This method is another upgrade method but it is not actually Live upgrade because this method causes an outage. This upgrade method takes less time because both nodes are upgraded simultaneously.** The Applications server(s) are upgraded before the OSV servers as part of the upgrade procedure.
- This method does not require service personnel to be present at the customer's site to perform the upgrade. The RSA interface is utilized for a native system while the Virtual Machine (VM) console is utilized for a virtual system.
- The user uses SFTP file transfer in **Binary** mode to transfer the upgrade files (i.e., OSV image, node.cfg, license file, Migration Toolkit rpm and additional patches) to the /repository/upload folder of each node. External media like DVD disks and USB memory sticks are not needed.
- The user starts the upgrade by entering a line command on node 1's console via the RSA interface or the VM console.
- The upgrade duration of a duplex system using Remote Software Upgrade takes approximately 1:00 hour. The time duration may differ depending on the database size or the number/size of the additional patch sets.
- If an error occurs during the upgrade, the user must initiate fall back to the source release. Additionally, the user must also initiate the collection of log and data files for the analysis of the error.

For this type of upgrade, refer to Section 8.7.2, “Upgrade Steps for Remote SW Upgrade”, on page 493.

8.6.2 Upgrade Steps for a Duplex System

Attention: When servers (e.g., media server or DLS) in the same network as one of the OSV's subnets need to communicate with another of the OSV's subnets, then changes to the network firewall are required to allow this communication. Any questions should be addressed to the next level of support.

Attention: No modifications to the voice servers' hardware, product type or deployment are expected in this procedure. If the voice servers' hardware, product type or deployment is to be changed, a procedure from Chapter 9, “Migrations to OpenScape Voice V11” should be employed for the upgrade.

Attention: If the OSV uses a media server resident on an external Applications server, that media server will not be available during the upgrade of the external Applications server. Announcements and conferences will not be available during the Applications upgrade until the latest DVD/Hotfix level of the target release is applied and the Applications server is started.

Table 21 describes the upgrade procedure. Some steps describe specific actions to be performed by the user depending on the upgrade method that is chosen. At the discretion of the user, checklist tasks 1 on page 486 through 4 on page 487 may be performed prior to the upgrade maintenance window.

Checklist task 5 on page 487 which upgrades the external Applications server can be performed prior to the upgrade maintenance window or during the upgrade maintenance window depending on the local company's policy.

A successful Applications server upgrade is necessary before proceeding with the OSV upgrade.

Hint: When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader tool bar. This will ease the navigation between the checklists and associated sections of the IUG.

After executing a checklist task, select the 'Previous View' icon in the Adobe Reader tool bar to return to the checklist.

The task list below describes the upgrade steps.

Task	Description
1.	Refer to Section 8.1.2, “Preparation Checklist”, on page 445 and Section 8.1.3, “Required Documents”, on page 447.

Table 21 Live Upgrade of Duplex OSV System

Task	Description
2.	Refer to Section 8.2.1, “System Information and Access Rights”, on page 454 and Section 8.2.2, “Logging”, on page 454.
3.	Refer to Section 8.3.3, “Verify Prerequisites Met According to Release Notes”, on page 461 and Section 8.3.4, “Obtain Licenses for the Target Release”, on page 462. **Note:** During an upgrade from a point release to another point release or an upgrade within the same release, licenses are automatically transferred. In this case, new licenses are not required. Most upgrades are from one release to another release (e.g., from V10 to V11). In this case, new licenses have to be obtained as described in Section 8.3.4
4.	Refer to Section 8.4, “Pre-Maintenance Window Activities”, on page 463. Perform all the activities in the subsections of Section 8.4 that may apply to your configuration.
5.	For an OSV duplex system, the external Applications server must be upgraded first to the latest target release. Install/update the OpenScape Applications onto the external applications server as follows: • Upgrading the External Applications Server (OffBoard). Direct update from these Applications server(s) levels to the V10 Applications level is supported: • V9Rx DVD Build, Hotfix level to V10 DVD Build level. The Build level of the source and target are specified in the V11 Release Notes. **For Multiple Communications Server Admin** deployments, refer to Section 5.7, “Upgrade of Offboard (External) Apps Server”, on page 376 and Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377. **For Standard Duplex Small, Standard Duplex Large and Standard Duplex Very Large** deployments, refer to the *OpenScape UC Application V10 Installation and Upgrade, Installation Guide*, section titled *“Updating, Upgrading and Migrating”.* **Note:** The DLS component can also be installed on the external OpenScape Applications server; review the DLS release notes for sizing limitations if the DLS component is to be installed on the external OpenScape Applications server. **A successful applications server upgrade is necessary before proceeding with the OSV upgrade.** If the upgrade fails, contact your next level of technical support for assistance.

Table 21 Live Upgrade of Duplex OSV System

Task	Description
6.	Create the node.cfg file for the target system by downloading and installing the latest Migration Toolkit rpm on the source system which automatically generates the node.cfg file for the target system. Refer to Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457.
7.	Prepare the upgrade files using one of the methods below. It is very helpful to mark the method that you are going to select to refer back to it in later steps: a) **For a native or a virtual OSV system**, if the upgrade files are to be stored on the nodes' repository (i.e., without using external media like DVD disks and USB memory sticks), prepare the upgrade files as described in Section 8.3.2.1, “Prepare Upgrade Files in Repository of OSV Node(s)”, on page 458. Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability.
8.	Run RapidStat on the source system prior to the upgrade. Errors and/or Warnings must be reviewed and corrected as necessary before continuing.
9.	For virtual machines only, the resource allocation of target release virtual machines must be verified against Table 13 on page 251, "Virtualization Dimensioning Details " of the target release OpenScape Voice Installation and Upgrade Guide (IUG). The resource allocation of the virtual machine(s) must be adjusted to the values listed in Table 13 on page 251, of the target release IUG before the upgrade begins. Some virtual machine resource changes require the machine be shut down (e.g. vCPU and Memory resources changes). This activity will cause a loss of service for the Integrated Simplex OSV and its Applications server. If an outage is not allowed for the Standard Duplex virtual system; the Duplex system virtual resource allocation update must be performed by first shutting down one node (i.e.; node 1), updating that node's VM resource allocations, and then restoring that node to state 4. After one node is updated and restored to service the partner node (i.e.; node 2) can be shut down, updated, and restored to state 4. Normal operating procedures for updating a Integrated Simplex or Standard Duplex system should apply too. **Questions should be addressed to your next level of support.**

Table 21 Live Upgrade of Duplex OSV System

Task	Description
10.	**For virtual machines only**; execute the following command on each node of a duplex deployment: **# ls -l /mnt** Verify the *cdrom* directory is NOT listed on the OSV nodes of a Duplex deployment. An example result with the *cdrom* directory listed follows: **root@bocast4a:[~] #164** **# ls -l /mnt** **total 4** **drwx------ 2 root root 4096 Nov 20 17:13 cdrom** **root@bocast4a:[~] #165** **#** IF the *cdrom* directory IS NOT PRESENT, THEN proceed to step 11 on page 489 now. IF the *cdrom* directory IS PRESENT, THEN execute the following command (as the root user); # rmdir /mnt/cdrom You can verify your work by executing the ***ls -l /mnt*** command once more. Remember to perform the check on both nodes of a duplex deployment. After removing the *cdrom* directory, proceed to step 11 on page 489.
11.	**For virtual machines only**; the installation of VMWare tools may change the permissions of the file */etc/fstab* on the virtual machine. The */etc/fstab* file permissions should be; -rw-r--r-- 1 root root 2558 Sep 7 13:39 /etc/fstab If the permissions are not as indicated above, **as the root user,** change the file permissions with the following command (**be sure to execute the command on both nodes of a virtual Duplex OSV deployment**): **# chmod a+r /etc/fstab** This change will help prevent any unexpected behavior during an upgrade.

Table 21 Live Upgrade of Duplex OSV System

Task	Description
12.	Start the upgrade using one of the following methods: a) **Duplex Configuration: Live Upgrade using the CMP/Assistant** This method is outage free and applies to native or virtual duplex configuration. This method requires that the user had selected option a) in step 7 on page 488. **This is the preferred upgrade method.** The user starts the upgrade from the CMP/Assistant. Node 1 is upgraded first, the calls are switched to node 1 and then node 2 is upgraded. Once the upgrade is started, all these steps are performed sequentially without stopping and without any input from the user. If an error occurs during the upgrade, the system automatically falls back to the source release with minimal prompts to the user. To invoke this upgrade method, refer to Section 8.8.4, “Duplex Configuration: Invoke Live Upgrade from the CMP/Assistant”, on page 503. b) **Duplex Configuration: Live Upgrade using the console or VM console with the upgrade files on the nodes' repository** This method is outage free and applies to a native duplex configuration. **This method requires that the user had selected option a) in step 7 on page 488.** The user starts the upgrade by entering a line command on node 1. Node 1 is upgraded first and the calls are switched back to node 1. At this point, depending on the command options used for the upgrade the process either: • proceeds with node 2 upgrade automatically, without waiting for any input from the user, or • stops, giving the user the opportunity to verify the integrity of node 1's upgrade. Once satisfied, the user enters a line command on node 1 to commit the upgrade. The upgrade resumes and node 2 is upgraded. If an error occurs during the upgrade, the user must manually initiate fall back to the source release with minimal prompts to the user. To invoke this upgrade method, refer to Section 8.8.5, “Duplex Configuration: Invoke Live Upgrade from Console or VM Console with Upgrade Files on Nodes' Repository”, on page 505. **Note:** When the OSV is a geographically separated duplex with Admin and Signaling interfaces shared, then the traffic switch, after the upgrade has finished on node1, does not affect the established calls/connections. This means that those calls will remain established on node2 until this node reboots to get upgraded as well. c) You can perform an upgrade through the OpenScape Composer also. For detailed information please consult the document *OpenScape Composer Vx Administration, Administrator Manual,* chapter **Software Updates**

Table 21 Live Upgrade of Duplex OSV System

Task	Description
13.	Execute RapidStat after a successful upgrade. Verify there are no issues and that the system is functioning correctly. **Note:** If it is determined that the upgrade of the system is unsatisfactory, fallback both nodes to the source release. Refer to Section 8.9.2, “Fallback Procedure 2 for Outage Free Toolkit”, on page 508. You do not need to return back to this section.
14.	Remove the upgrade/migration toolkit software (UNSPmigration-<V#>.rpm) from the target system. Refer to Section 9.7, “Remove the Migration Toolkit Software from the Target System”, on page 554.
15.	Complete the upgrade. Refer to Section 7.4, “Completing the Upgrade/Migration to V11”, on page 428.

Table 21 Live Upgrade of Duplex OSV System

8.7 Upgrade of an OSV System Using Remote SW Upgrade

8.7.1 Overview

This upgrade method was created to reduce service cost of upgrading an OpenScape Voice system by having the service technician upgrade the system remotely without having to be present at the customer's site.

This upgrade method can be summarized as follows:

- This method can be used for upgrading a native or a virtual OpenScape system. Additionally, it works for an Integrated Simplex configuration or a Standard Duplex configuration.
- **For a Standard Duplex configuration, this upgrade method causes an outage.** However, this upgrade method takes less time than Live upgrade of a Standard Duplex configuration because both OSV nodes are upgraded simultaneously.

  For an Integrated Simplex configuration, this upgrade method causes an outage just like other upgrade methods since outage is inevitable in a single node system.
- This method does not require the service personnel to be present at the customer's site to perform the upgrade. The RSA interface is utilized for a native system while the Virtual Machine (VM) console is utilized for a virtual system. The VM console is accessed from the Console tab of the virtual machine's vSphere client.

- For a Standard Duplex configuration, the Applications server(s) must be upgraded prior to starting the Remote SW Upgrade of the OpenScape Voice servers.

  For an Integrated Simplex system, the Remote SW Upgrade upgrades the OpenScape Voice server and the applications.

- The user uses SFTP file transfer in **Binary** mode to transfer the upgrade files (i.e., OSV image, node.cfg, license file, Migration Toolkit rpm and additional patches) to the /repository/upload folder of each node. The use of external media like DVD disks and USB memory sticks is eliminated.

- The user starts the upgrade by entering a line command on node 1's console via the RSA interface or the VM console.

- **The user may login to the node via an SSH session** to start the upgrade rather than logging into the console via the RSA interface or the VM console. However, the user should be aware of the following when an SSH session is used:

  – The user will not be able to monitor the upgrade progress.

  – When an upgrade failure occurs, the system tries to fallback to the source release automatically. However if the automatic fallback fails, the user must use the console or VM console to manually restore the system.

  – The user will have to wait some time until the upgrade is completed before being able to login onto the node(s) via an SSH session and verify the upgrade status. The user must understand it may appear that he/she gets the login prompt for an SSH session but the login fails with invalid password because the system has been installed, but the import of the data has not finished and the passwords from the source system have not yet been imported to the target system.

  – For a virtual system, it may take a while longer to synchronize the image if the Storage Array Network (SAN) is slow.

- The upgrade duration of a duplex system using Remote Software Upgrade takes approximately 1:00 hour.

  The upgrade duration of an Integrated Simplex system using Remote Software Upgrade takes approximately 1:30 hours.

  The time duration may differ depending on the database size or the number/size of the additional patch sets.

- When an error occurs during the upgrade, the system tries to fallback to the source release automatically. However if the automatic fallback fails, the user must initiate fall back to the source release. Additionally, the user must also initiate the collection of log and data files for the analysis of the error.

For this type of upgrade, refer to Section 8.7.2, “Upgrade Steps for Remote SW Upgrade”, on page 493.

8.7.2 Upgrade Steps for Remote SW Upgrade

Prerequisites:

1. Adequate administrative permissions.
2. Fully functional system.
3. For a Standard Duplex configuration, the Applications server(s) will be upgraded prior to starting the Remote SW Upgrade of the OpenScape Voice servers.

Note: For an Integrated Simplex system, the Remote SW Upgrade procedure also upgrades the applications.

Note: The RSA applies to a native machine upgrade. For the case of a virtual machine upgrade, any references to the native hardware RSA should be interpreted to mean the virtual machine (VM) console. The VM console is accessed from the Console tab of the virtual machine's vSphere client.

The task list below describes the upgrade steps.

Task	Description
1.	Refer to Section 8.1.2, “Preparation Checklist”, on page 445 and Section 8.1.3, “Required Documents”, on page 447.
2.	Refer to Section 8.3.4, “Obtain Licenses for the Target Release”, on page 462. **Note:** During an upgrade from a point release to another point release or an upgrade within the same release licenses are automatically transferred. In this case, new licenses are not required. Most upgrades are from one release to another release (e.g., from V10 to V11). In this case, new licenses have to be obtained as described in Section 8.3.4
3.	Refer to Section 8.4, “Pre-Maintenance Window Activities”, on page 463. Perform all the activities that apply in the subsections of Section 8.4.
4.	For a duplex OSV system, the external Applications server must be upgraded first to the latest target release. Install/update the OpenScape Applications onto the external applications server as follows: • Upgrading the External Applications Server (OffBoard). Direct update from these Applications server(s) levels to the V10 Applications level is supported: – V9Rx DVD Build, Hotfix level to V10 DVD Build level. The Build level of the source and target are specified in the V11 Release Notes. **For Multiple Communications Server Admin** deployments, refer to Section 5.7, “Upgrade of Offboard (External) Apps Server”, on page 376 and Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377. **For Standard Duplex Small, Standard Duplex Large and Standard Duplex Very Large** deployments, refer to the *OpenScape UC Application V10 Installation and Upgrade, Installation Guide*, section titled “Updating, Upgrading *and Migrating*”. **Note:** The DLS component can also be installed on the external OpenScape Applications server; review the DLS release notes for sizing limitations if the DLS component is to be installed on the external OpenScape Applications server. **A successful applications server upgrade is necessary before proceeding with the OSV upgrade.** If the upgrade fails, contact your next level of technical support for assistance.

Table 22 Upgrade SW Remotely

Task	Description
5.	Login onto the RSA or the VM console for remote access. For a Standard Duplex configuration, login onto both nodes. **Note:** Alternatively, the user may login onto the nodes via an SSH session. However, the user should be aware that the upgrade progress cannot be continuously monitored by the service technician when an SSH session is used. For more details, refer to Section 8.7.1, “Overview”, on page 491.
6.	Create the node.cfg file for the target system by downloading and installing the latest upgrade/migration Toolkit rpm on the source system which automatically generates the node.cfg file for the target system. Refer to Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457.
7.	If this is a Duplex OSV Remote Software Upgrade, proceed to step 8 on page 495 of this task list. If this is an Integrated Simplex Remote Software Upgrade, create the response.cfg.primary file for the Integrated Simplex system. Refer to Section 9.11, “Simplex System response.cfg.primary File Creation”, on page 562.
8.	Prepare the upgrade files. Refer to Section 8.3.2.1, “Prepare Upgrade Files in Repository of OSV Node(s)”, on page 458.
9.	Run RapidStat. Errors and/or Warnings must be reviewed and corrected as necessary before continuing.

Table 22 Upgrade SW Remotely

Task	Description
10.	For virtual machines only, the resource allocation of target release virtual machines must be verified against Table 13 on page 251, "Virtualization Dimensioning Details " of the target release OpenScape Voice Installation and Upgrade Guide (IUG). The resource allocation of the virtual machine(s) must be adjusted to the values listed in Table 13 on page 251 of the target release IUG before the upgrade begins. **Attention:** Some virtual machine resource changes require the machine be shut down (e.g. vCPU and Memory resources changes). This activity will cause a loss of service for the Integrated Simplex OSV and its Applications server. If an outage is not allowed for the Standard Duplex virtual system; the Duplex system virtual resource allocation update must be performed by first shutting down one node (i.e.; node 1), updating that node's VM resource allocations, and then restoring that node to state 4. After one node is updated and restored to service the partner node (i.e.; node 2) can be shut down, updated, and restored to state 4. Normal operating procedures for updating a Integrated Simplex or Standard Duplex system should apply too. **Questions should be addressed to your next level of support.**
11.	**For virtual machines only**; Execute the following command on the OSV node of a simplex deployment or each node of a duplex deployment; **# ls -l /mnt** Verify the *cdrom* directory is NOT listed on the OSV node of a Simplex deployment or nodes of a Duplex deployment. An example result with the *cdrom* directory listed follows: **root@bocast4a:[~] #164** **# ls -l /mnt** **total 4** **drwx------ 2 root root 4096 Nov 20 17:13 cdrom** **root@bocast4a:[~] #165** **#** IF the *cdrom* directory IS NOT PRESENT, THEN proceed to step 12 on page 497 now. IF the *cdrom* directory IS PRESENT, THEN execute the following command (as the root user); # rmdir /mnt/cdrom You can verify your work by executing the ***ls -l /mnt*** command once more. Remember to perform the check on both nodes of a duplex deployment. After removing the *cdrom* directory, proceed to step 12 on page 497.

Table 22 Upgrade SW Remotely

Task	Description

12.	**For virtual machines only**; the installation of VMWare tools may change the permissions of the file */etc/fstab* on the virtual machine. The */etc/fstab* file permissions should be;
	`-rw-r--r-- 1 root root 2558 Sep 7 13:39 /etc/fstab`
	If the permissions are not as indicated above, **as the root user**, change the file permissions with the following command (**be sure to execute the command on both nodes of a virtual Duplex OSV deployment**):
	`# chmod a+r /etc/fstab`
	This change will help prevent any unexpected behavior during an upgrade.

13.	Start the upgrade. As user root on node 1: `# cd /root; upgrade8k -quiet` --- **Note:** If an error occurs during the upgrade, the system automatically falls back to the source release. For certain errors, the system might not be able to automatically fallback or automatically come up on the source release then manual fallback to the source release has to be initiated by the user. Refer to Section 8.9.5, “Fallback Due to Failure During Installation for Remote SW Upgrade”, on page 512 and Section 8.9.6, “Fallback Due to Failure During Import for Remote SW Upgrade”, on page 513, as needed. ---

14.	If the upgrade was started from an SSH session rather than a console or VM console, it is important to verify that the upgrade has completed because monitoring the upgrade was not possible in an SSH session.
	Login onto node 1 via an SSH session after giving the system ample time to complete the upgrade. Verify that the upgrade has finished by checking the upgrade status as follows:
	`# upgrade8k -s`
	As an example, when the upgrade is completed, the following messages are seen at the end of the output of the above command:
	`: : :`
	`05/02/13 15:56:16 DataCollect`
	`05/02/13 16:03:06 NoError`

15.	Execute RapidStat. Verify there are no issues and that the system is functioning correctly. --- **Note:** If it is determined that the upgrade of the system is unsatisfactory, fallback both nodes (or node for simplex) to the source release. Refer to Section 8.9.6, “Fallback Due to Failure During Import for Remote SW Upgrade”, on page 513. ---

Table 22 Upgrade SW Remotely

Task	Description
16.	Remove the upgrade/migration toolkit software (UNSPmigration-<V#>.rpm) from the target system. Refer to Section 9.7, “Remove the Migration Toolkit Software from the Target System”, on page 554.
17.	Complete the upgrade. Refer to Section 7.4, “Completing the Upgrade/Migration to V11”, on page 428.

Table 22 Upgrade SW Remotely

8.8 Invoking Upgrade

Attention: Your upgrade should not be started from the subsections of this section. The upgrade should be started from one of the upgrade tables like Table 20, Table 21 or Table 22 etc. One of the steps in these tables would refer you to one of the subsections in this section.

8.8.1 Simplex Configuration: Invoke Upgrade from the CMP/Assistant (UI Method)

This method is run from the CMP/Assistant. The upgrade files should have already been placed in folder `/repository/upload` of the node.

1. Login to RSA or the Console (native OSV/VM) for remote access. This allows the user to monitor the upgrade progress because the CMP/Assistant connection will be lost during the upgrade.

   Note: The RSA applies to a native machine upgrade. For the case of a virtual machine upgrade, any references to the native hardware RSA should be interpreted to mean the virtual machine (VM) console. The VM console is accessed from the Console tab of the virtual machine's vSphere client.

2. Ensure that an ISO image DVD disk and USB memory stick are not inserted in the server.
3. Login to the CMP and navigate to **Maintenance > Inventory > Applications**

   Note: In some cases particularly after fallback to the source release, "Upgrade Version in progress" might be displayed for the OpenScape Voice entry of your switch under the **Active version** column. To clear this indication, do the following:

Click on the arrow at the end of the line on the right and select **Upgrade Version**. In the popup window, click the **Finish Upgrade** button at the bottom of the screen. The window is closed and now the OpenScape Voice entry under the **Active version** does not show "Upgrade Version in progress" anymore.

4. For the corresponding OSV system, click on the arrow at the end of the line on the right and select **Upgrade Version …**

   A window opens showing the contents of directory /repository/upload of the node.

   Note: Start the upgrade from the RSA connection by entering the following command on the node as user *root*:

   ```
   # cd /root; upgrade8k –quiet –live
   ```

   No further interactions are required by the user other than agreeing to continue with the upgrade after preliminary checks are made. The user uses the RSA connection to monitor the status of the upgrade.

   If you have entered the command above, then go to step 6 on page 500 of this task list and wait for the upgrade process to complete.

5. Click on the **Start Upgrade** button to initiate the upgrade. The status of the upgrade is displayed on the Assistant.

   Note: After the upgrade is started, a message is displayed on the Assistant indicating that the screen will not be updated anymore. Therefore, the user must use the RSA connection or the Console (native OSV/VM) connection to monitor the status of the upgrade.

6. When the upgrade process completes, the login prompt is displayed on the console.

Note: At the final step of the upgrade, the Toolkit automatically collects the log files and places them in a single compressed file named `"data-<clusterName>.tar.gz"` in the `/log` directory.

For example: `/log/data-BOCASTRESS1.tar.gz`

Note: Timing information regarding the upgrade is available on the node in file: `/repository/upgrade8k-timing`

Fallback on Error

If an error occurs during the upgrade, fallback to the source release is automatically initiated by the system. The Toolkit automatically collects the log files and places them in a single compressed file named `"data-<clusterName>.tar.gz"` in the `/log` directory.

Also, check file /log/prepare8k.log for clues about the failure.

After investigating and fixing the problem, it shall be possible to initiate another upgrade.

8.8.2 Simplex Configuration: Invoke Upgrade from Console or VM Console with Upgrade Files on Node's Repository

This method can only be run from the console or VM console. The upgrade files should have already been placed in folder /repository/upload of the node.

1. Ensure that an ISO image DVD disk and USB memory stick are not inserted in the server.
2. Login to the console or VM console of the node as user *root*.
3. As user *root,* enter the following command from the console or VM console:

Note: The order of options in the following command cannot be changed.

```
# cd /root; upgrade8k –quiet –live
```

No further interactions are required by the user other than agreeing to continue with the upgrade after preliminary checks are made.

4. When the upgrade process completes, the login prompt is displayed on the console.

Note: At the final step of the upgrade, the Toolkit automatically collects the log files and places them in a single compressed file named "data-<clusterName>.tar.gz" in the /log directory.

For example:

/log/data-BOCASTRESS1.tar.gz

Note: Timing information regarding the upgrade is available on the node in file:

/repository/upgrade8k-timing

Fallback on Error

If an error occurs during the upgrade, fallback to the source release is automatically initiated by the system. The Toolkit automatically collects the log files and places them in a single compressed file named "data-<clusterName>.tar.gz" in the /log directory.

Also, check file /log/prepare8k.log for clues about the failure.

After investigating and fixing the problem, it shall be possible to initiate another upgrade.

8.8.3 Simplex Configuration: Invoke Upgrade from the Console with Upgrade Files on External Media

This method can only be run from the console of a native Integrated Simplex configuration. The upgrade files should have already been placed on a DVD disk and a USB memory stick and inserted in the native Integrated Simplex server.

1. Login to the console of the node as user *root*. You may also login to the RSA of the node as user *root*.
2. Delete all the files in folder /repository/upload
3. Insert the USB memory stick labeled **node.cfg.primary** into the node.
4. Insert the USB stick that contains the OSV image of the target system. In case of a virtual environment, connect the virtual CD/DVD ISO.
5. Export the data to the USB memory stick by entering the following command as user *root:*

```
# export8k
```

The above procedure creates file: `patch/export.tar` on the USB memory stick. The following message is displayed at the end indicating a successful export:

```
:    :    :
Export completed: <date>
Elapsed time:     <time>
```

Note: Do not remove the USB memory stick from the node.

---

6. Configure the node to Rtp state 2. This will also stop the applications (symphonia):

   ```
   # /unisphere/srx3000/srx/startup/srxctrl 2 0
   ```

   Enter **y** to continue, if prompted.

7. Reboot the system:

   ```
   # reboot
   ```

8. When the boot screen presents the options below, select the second option to install the Softswitch with the image of the target release. The options are:

   - Boot from Hard Disk
   - **Install Softswitch - Va_Rb_c.d_ee** (Select this option and then press **Enter**)

9. Review and accept the EULA by selecting **Done** and selecting **Yes** on the following screen.

   Select **Done** again if you are satisfied with the presented Network Information.

10. When prompted with the following options:

    ```
    Note: Typing yes or format will erase all data from
    unlocked partition on the disk.
    : yes - Erases data from the first unlocked image.
    : no - Aborts installation.
    : format - Reformats harddisk, user loses all the data
    : lockprim - Erases data from the secondary partition
    : locksec - Erases data from the primary partition
    : verify - verify hardware
    Do you want to continue with installation (enter yes/no/
    format/lockprim/locksec)?
    ```

    Type: **lockprim** if the source software was on the primary partition

    or

Type: **locksec** if the source software was on the secondary partition.

Note: Format and repartition are necessary for fresh installation.

Note: No further user interactions are required until the image installation ends and the login prompt is presented to the user.

---

11. After the image installation ends, login to the node as user *sysad* (default password: "1clENtk="). After the first login, the *sysad* password has to be changed. Change it to any value (e.g., !Q2w3e4r). This doesn't matter because the password from the source release will be restored in the next few steps.

12. Switch to user *root* and verify the success of the installation as follows:

    `# su - root` (Default password: "T@R63dis")

    `# srxqry -v` (System should be in state 4 & all processes in PROCESS_READY state)

    `# su - srx -c "pkgversion -ps"` (latest target patch set is installed)

13. Download the Migration Toolkit software (UNSPmigration-<V#>.rpm) and install it onto the target system. Refer to Section 9.5, "Downloading and Installing the Migration Toolkit Software to the Target System", on page 551.

14. Import the data of the source system from the USB memory stick labeled **node.cfg.primary** to the target by entering the following command:

    `# import8k`

Fallback on Error

If an error occurs during the upgrade, fallback to the source release is automatically initiated by the system. The Toolkit automatically collects the log files and places them in a single compressed file named: "data-<clusterName>.tar.gz" in the /log directory.

Also, check file /log/prepare8k.log for clues about the failure.

After investigating and fixing the problem, it shall be possible to initiate another upgrade.

8.8.4 Duplex Configuration: Invoke Live Upgrade from the CMP/Assistant

This method is run from the CMP/Assistant. The upgrade files should have already been placed in folder /repository/upload of each node.

1. Ensure that an ISO image DVD disk and USB memory stick are not inserted in the server.
2. Login to the CMP and navigate to **Maintenance > Inventory > Applications**

Note: In some cases particularly after fallback to the source release, "Upgrade Version in progress" might be displayed for the OpenScape Voice entry of your switch under the **Active version** column. To clear this indication, do the following:

Click on the arrow at the end of the line on the right and select **Upgrade Version**. In the popup window, click the **Finish Upgrade** button at the bottom of the screen. The window is closed and now the OpenScape Voice entry under the **Active version** does not show "Upgrade Version in progress" anymore.

---

3. For the corresponding OSV system, click on the arrow at the end of the line on the right and select **Upgrade Version …**

   A window opens showing the contents of directory /repository/upload of the nodes.
4. Click on the **Start Upgrade** button to initiate the upgrade.

   The status of the upgrade is displayed on the Assistant. No further interaction is required by the user.
5. When the upgrade process completes, an appropriate message is displayed on the Assistant.

Note: At the final steps of node 2's upgrade, the Toolkit automatically collects the log files **from both nodes** and places them in a single compressed file named `"data-<clusterName>.tar.gz"` in the `/log` directory of **node 1.**

For example:
`/log/data-BOCASTRESS1.tar.gz`

Note: Timing information regarding the upgrade is available on node 1 in the following file:

`/repository/upgrade8k-timing`

Note: Click this link to return to step 13 on page 491 in Table 21, "Live Upgrade of Duplex OSV System".

.**Fallback on Error**

If an error occurs during the upgrade, fallback is automatically initiated by the system. In this case, the user is informed and an option to **Download Logs** button is presented to the user.

After the user clicks on the button and downloads the logs, the user should click on the **Finish Upgrade** button. At this point, the OSV system reverts back to the source release.

Also, check file `/log/prepare8k.log` for clues about the failure.

After investigating and fixing the problem, it shall be possible to initiate another upgrade.

Note: In case of a more extreme error where automatic fallback to the source release is not initiated by the system, manual fallback should be performed. Refer to Section 8.9.3, “Manual Fallback on Failed Upgrade”, on page 509. You do not need to return back to this section.

8.8.5 Duplex Configuration: Invoke Live Upgrade from Console or VM Console with Upgrade Files on Nodes' Repository

This method is run from the console or VM console. The upgrade files should have already been placed in folder /repository/upload of each node.

1. Ensure that an ISO image DVD disk and USB memory stick are not inserted in the servers.
2. Login to the console or VM console of node 1 as user *root*.
3. As user *root*, enter the following command from the console or VM console of node 1:

    1. For a completely automated Upgrade enter the following command from the console or VM console of node 1 as user root:

    Note: The order of the options in the following command cannot be changed.

    ```
    # cd /root; upgrade8k –quiet –live
    ```

    The '*quiet*' option enables complete automation of the Upgrade. No further interactions are required by the user other than agreeing to continue with the upgrade after preliminary checks are made. For instance when prompted as follows, do nothing. The upgrade will automatically proceed without user input;

```
-----------------------------------------------------
After logging in as root, type one of the following:
 1. upgrade8k -commit   (start node#2 upgrade).
 2. upgrade8k -fallback (fallback to source release).
-----------------------------------------------------
```

2. For a controlled Upgrade, verify first the integrity of node 1 and then proceed with node 2 upgrade by entering the following command from the console or VM console of node 1 as user root:

```
# cd /root; upgrade8k -live
```

Here the process stops after the Upgrade has finished on node 1 giving the user the opportunity to verify the integrity of the node after the upgrade. Depending on the results, the user can either select to commit the upgrade or fallback to the source release. When prompted as follows provide your input accordingly;

```
-----------------------------------------------------
After logging in as root, type one of the following:
 1. # cd /root; upgrade8k -commit (start node#2
upgrade)
 2. # cd /root; upgrade8k -fallback (fallback to
source release)
-----------------------------------------------------
```

4. When the upgrade process is completed, the login prompt is displayed on the console.

Note: At the final steps of node 2's upgrade, the Toolkit automatically collects the log files **from both nodes** and places them in a single compressed file named "`data-<clusterName>.tar.gz`" in the `/log` directory of **node 1.**

For example:
`/log/data-BOCASTRESS1.tar.gz`

Note: Timing information regarding the upgrade is available on node 1 in file:
`/repository/upgrade8k-timing`

Note: Click this link to return to step 13 on page 491 in Table 21, "Live Upgrade of Duplex OSV System"

Note: OSV Duplex solidDB diagnostics are also collected by default during upgrade. At the end of the Upgrade you can find the log files under the /log directory of each node with the name `ss_debug_upgrade.tar`

For example:
`/log/ss_debug_upgrade.tar`

To turn off this functionality the `-nosoliddebug` flag can be used in the upgrade8k command so as the user root can enter either:
`# cd /root; upgrade8k -quiet -nosoliddebug -live`
or
`# cd /root; upgrade8k -nosoliddebug -live`

You must not change the order of the flags (the -live flag must always be at the end)

Fallback on Error

If an error occurs during the upgrade, fallback to the source release is automatically initiated by the system. The Toolkit automatically collects the log files from both nodes and places them in a single compressed file named "data-<clusterName>.tar.gz" in the `/log` directory of **node 1**.

Also, check file `/log/prepare8k.log` for clues about the failure.

After investigating and fixing the problem, it shall be possible to initiate another upgrade.

Note: In case of a more extreme error where automatic fallback to the source release is not initiated by the system, manual fallback should be performed. Refer to Section 8.9.3, "Manual Fallback on Failed Upgrade", on page 509. You do not need to return back to this section.

8.9 Fallback Procedures

If a decision to Fallback is made, the priorities are to return the system to the source release, verify functionality and then execute the data collection. The data collection software is delivered with the toolkit. Data will be collected from both partitions of each node. The resulting data collection is stored in a zipped tar file. The following subsections have additional information about data collection.

If the fallback procedures listed in Section 8.9.1 through Section 8.9.6 do not succeed, then use the fallback procedure in Section 8.9.7, "Fallback using File System Restore", on page 515 as a last resort but only after contacting your next level of support.

8.9.1 Fallback Procedure 1 for Outage Free Toolkit

When an error occurs during the installation of node 1 or after finishing the installation of node 1 and realizing that the OSV system is not functioning correctly, fallback to the source release should be initiated as follows:

1. Login onto **node 1** as user *root* and enter the following:

   ```
   # cd /root; upgrade8k -fallback
   ```

   When prompted if you want to continue, enter **yes**

   Node 1 is rebooted and comes up on the other partition that contains the source release software. For a duplex system, the cluster is joined and both nodes will be operational with the source release software.

   Note: The log files are automatically collected from both nodes (or node in simplex) and placed in a single compressed file named `"data-<clusterName>.tar.gz` in the `/log` directory of **node 1**.

   For example: `/log/data-BOCASTRESS1.tar.gz`

   ---

2. For integrated simplex only, the OSV might still be locked and indicates "Upgrade in Progress". To unlock the OSV:
   - Login onto the CMP.
   - Navigate to **Maintenance > Inventory > Applications**.
   - If the **OpenScape Voice** entry shows "Upgrade Version in progress", then do the following:
     – Click on the arrow at the end of the line on the right and select **Upgrade Version**.
     – In the popup window, click **Finish Upgrade**. The OSV is now unlocked.

8.9.2 Fallback Procedure 2 for Outage Free Toolkit

Attention: During the manual fallback there will be an outage of approximately 9 minutes while the OpenScape Voice source release is restored.

When an error occurs during the installation of node 2 of a duplex OSV system or after finishing the upgrade in a simplex or duplex OSV system and realizing that the OSV system is not functioning correctly, fallback to the source release should be initiated as follows:

1. Login onto **node 1** as user *root* and enter the following command to fall back to the source release:

   ```
   # /unisphere/srx3000/srx/bin/activate8k -auto
   ```

   Both Nodes are rebooted and come up on the partition that contains the source release software. The cluster is joined and both nodes will be operational with the source release software. An outage will occur in this case for approximately 9 minutes until the two nodes come up to RTP state 4 4 on the source release.

2. From node 1, collect data for analysis after the system is restored as follows:

   ```
   # cd /root; upgrade8k -collect
   ```

   The command is only executed from node 1. However, it collects data **from both nodes** and places them in a single compressed file named "`data-<clusterName>.tar.gz`" in the `/log` directory of **node 1**.

   For example:

   ```
   /log/data-BOCASTRESS1.tar.gz
   ```

8.9.3 Manual Fallback on Failed Upgrade

Attention: During the manual fallback there will be an outage of approximately 9 minutes while the OpenScape Voice source release is restored.

In most cases when an error occurs during the upgrade or migration process, the fallback to the source release is initiated automatically and data is collected automatically for analysis of the error. In case an automatic fallback is not initiated by the system, the user can initiate the fallback manually.

If the upgrade fails, contact your next level of technical support for assistance.

To manually initiate fallback:

1. Login to the console (native OSV/VM) or the RSA interface.
2. As user *root*, enter the following command on node 1:

   ```
   # /unisphere/srx3000/srx/bin/activate8k -auto
   ```

   Note: In an extreme error case, if the console (native OSV/VM) or the RSA interface freezes and commands cannot be entered, refer to Section 8.9.4, “Fallback when Console is not Responsive”, on page 510. You do not need to return back to this section.

   ---

3. The above step will reboot the system and bring it up to state 4 (or state 4 4 for a duplex system) on the source release. The Toolkit automatically collects the log files (from the node in simplex or from both nodes in duplex) and places them in a single compressed file named `"data-<clusterName>.tar.gz"` in the `/log` directory of node 1.

   Also, check file `/log/prepare8k.log` for clues about the failure.

4. For integrated simplex only, the OSV might still be locked and indicates "Upgrade in Progress". To unlock the OSV:

   - Login onto the CMP.
   - Navigate to **Maintenance > Inventory > Applications**.

     If the **OpenScape Voice** entry shows "Upgrade Version in progress", then do the following:

     – Click on the arrow at the end of the line on the right and select **Upgrade Version**.

     – In the popup window, click **Finish Upgrade**. The OSV is now unlocked.

After investigating and fixing the problem, it shall be possible to initiate another upgrade.

Attention: If the fallback was for a standard duplex configuration (with an external Applications server), then fallback may have to be performed on the external Applications server. Refer to the appropriate Fallback instruction for your deployment:

- For Multiple Communications Server Admin and Media Server Stand Alone deployments, refer to the appropriate subsection of Section 5.7.2, “Fallback During Upgrade Procedure”, on page 382.

- For all other Applications server deployments (i.e.; Standard Duplex Small or Standard Duplex Large deployments, refer to the *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide* (where *x* is the current version), section "Fallback after aborted Upgrade".

8.9.4 Fallback when Console is not Responsive

Attention: During the manual fallback there will be an outage of approximately 9 minutes while the OpenScape Voice source release is restored.

In extreme upgrade failure scenarios, if the console (native OSV/VM) or the RSA interface freezes and commands cannot be entered, the following manual procedure can be used:

1. Remove any exterior media (e.g., DVD disc(s) and USB memory stick(s)) from the server(s).
2. From the console, reboot both nodes (or node in simplex) by pressing the restart button or turning off each server and then turning it on. The server can also be rebooted from the RSA interface or the VM console.
3. From the boot menu that will be displayed, select the load of the source release.
4. After the system is brought up to state 4 (or state 4 4 for a duplex system) on the source release, collect data for analysis of the error as follows:

   Login onto node 1 as user *root* and enter the following command:

   ```
   # cd /root; upgrade8k -collect
   ```

   The Toolkit automatically collects the log files (from the node in simplex or from both nodes in duplex) and places them in a single compressed file named `"data-<clusterName>.tar.gz"` in the `/log` directory of node 1.

   Also, check file `/log/prepare8k.log` for clues about the failure.

   After investigating and fixing the problem, it shall be possible to initiate another upgrade.
5. For integrated simplex only, the OSV might still be locked and indicates "Upgrade in Progress". To unlock the OSV:
   - Login onto the CMP.
   - Navigate to **Maintenance > Inventory > Applications**.

     If the **OpenScape Voice** entry shows "Upgrade Version in progress", then do the following:
     - Click on the arrow at the end of the line on the right and select **Upgrade Version**.
     - In the popup window, click **Finish Upgrade**. The OSV is now unlocked.

Attention: If the fallback was for a standard duplex configuration (with an external Applications server), then fallback may have to be performed on the external Applications server. Refer to the appropriate Fallback instruction for your deployment:

- For Multiple Communications Server Admin and Media Server Stand Alone deployments, refer to the appropriate subsection of Section 5.7.2, “Fallback During Upgrade Procedure”, on page 382.

- For all other Applications server deployments (i.e.; Standard Duplex Small or Standard Duplex Large deployments), refer to the *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide* (where *x* is the current version), section "Fallback after aborted Upgrade".

8.9.5 Fallback Due to Failure During Installation for Remote SW Upgrade

Attention: During the manual fallback there will be an outage of approximately 9 minutes while the OpenScape Voice source release is restored.

If for any reason the upgrade fails during installation, then reboot nodes (or node for integrated Simplex system) and select to boot from the source partition on each node as described in details below.

Prerequisites:

Adequate administrative permissions

Step by step:

1. Login to RSA or VM console for remote access (must log on to each node).
2. Reboot both nodes:

   ```
   # reboot
   ```

3. During the reboot, on each node a menu is displayed (GRUB menu) asking the user to select the source load or the target load (i.e., if the user wants to bring the system up on the partition containing the source load or on the partition containing the target load). **The user must select the source load.**
4. If the system (that comes up on the source release) does not reach state 4, run the following command on both nodes (or node for simplex system):

   ```
   # /unisphere/srx3000/srx/bin/activate8k -done
   ```

5. Check the system:
   - If both nodes (or node in simplex) work normally:
     – Go to step 7.

     Note: Under certain conditions it is possible that the installation could fail e.g. due to a bad `node.cfg`. If for some reason the remote upgrade menus are not reset, continue with step 6.

6. If for some reason (e.g., a bad node.cfg) the remote upgrade menus are not reset then the user can run the following command in order to reset the remote upgrade setup enter as user root:

   ```
   # cd /root; upgrade8k -reset
   ```

7. Contact your next level of support in order to investigate the cause that led to the upgrade failure.

   Once the problem is solved, the Remote SW Upgrade procedure can be started again.

8.9.6 Fallback Due to Failure During Import for Remote SW Upgrade

If for any reason the upgrade fails during import, then run the commands described in details below in order to activate the fallback partition (source release).

Attention: During the manual fallback there will be an outage of approximately 9 minutes while the OpenScape Voice source release is restored.

Prerequisites:

Adequate administrative permissions

Step by step:

1. For a Standard Duplex system, login to node 1's RSA (for a native system) or VM console (for a virtual system).

   For an Integrated Simplex system, login to the node's RSA (for a native system) or VM console (for a virtual system).

2. Run the following command:

   ```
   # /unisphere/srx3000/srx/bin/activate8k -auto
   ```

3. For integrated simplex only, after the OSV comes up to state 4, the OSV might still be locked and indicate "Upgrade in Progress". To unlock the OSV:

   - Login onto the CMP.
   - Navigate to **Maintenance > Inventory > Applications**.

     If the **OpenScape Voice** entry shows "Upgrade Version in progress", then do the following:

     – Click on the arrow at the end of the line on the right and select **Upgrade Version**.

– In the popup window, click **Finish Upgrade**. The OSV is now unlocked.

4. Contact your next level of support in order to investigate the failure.

8.9.7 Fallback using File System Restore

Attention: This procedure should not be performed unless advised to do so by your next level of support.

Note: If the upgrade data collection has not already been executed ("upgrade8k -collect"), it is recommended to perform this data collection before the file system restore. Be sure to save the resulting file to a server other than the OpenScape Voice switch (because disk formatting is part of the file system restore process and all data will be lost).

The data collection software is delivered with the Toolkit. The data is collected from both partitions of each node. Data collection can be initiated as follows:

Login onto node 1 as user *root* and enter the following command:

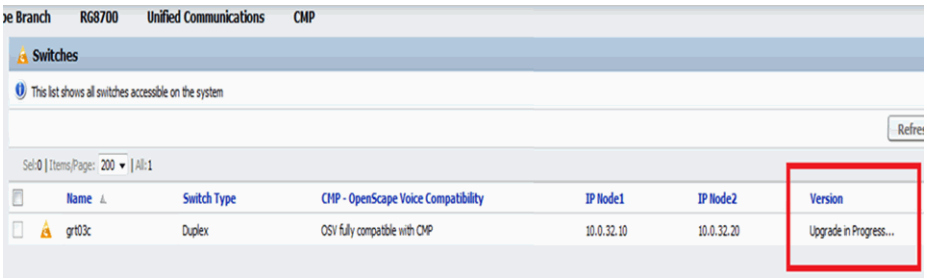
```
# cd /root; upgrade8k -collect
```

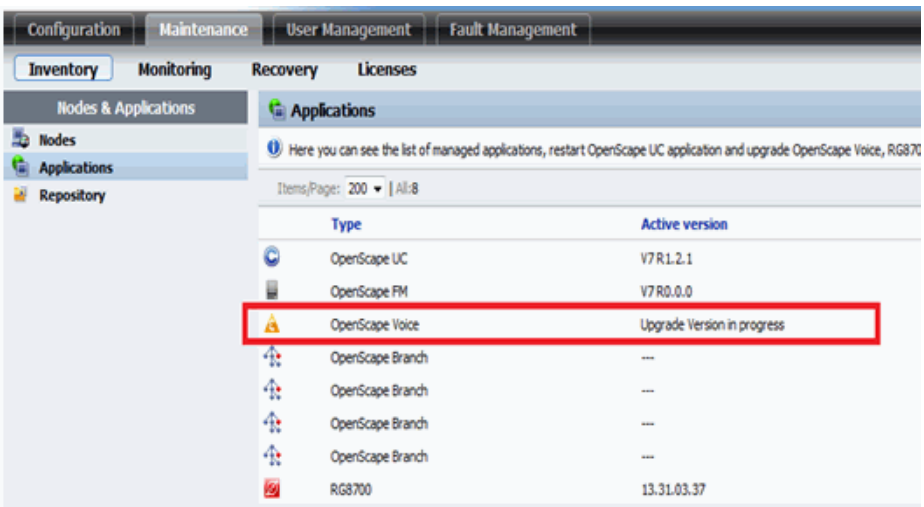
The command is only executed from node 1. However, it collects data **from both nodes** and places them in a single compressed file named "`data-<clusterName>.tar.gz`" in the `/log` directory of **node 1**.

For example:
`/log/data-OSVNODENAME.tar.gz`

Save the resulting file to a server other than the OpenScape Voice switch (because disk formatting is part of the file system restore process and all data will be lost).

1. In the very rare case that an automatic fallback fails then the user should utilize the file system restore procedures. Refer to the "*OpenScape Voice Vx Service, Service Documentation*" (Vx equals the source release), section titled "*Serviceability - B&R, Import/Export, SW Maintenance*".
2. OpenScape Voice Assistant maintains locally (stores) the Upgrade status of the OpenScape Voice system. So after the file system restore, the OpenScape Voice switch may not be available from the CMP because the upgrade status remains in progress. Additionally, the OSV node(s) on the CMP's dashboard are grayed out thus disabling any action on the OSV node(s).





Change the switch state to idle in the CMP

3. Ensure that remote access for node 1 and node 2 are configured correctly and use the pam_tally2 command to resolve "srx user access violations". As user *root* on node 1, query the pam_tally2 count. For example:

   # pam_tally2
   User srx (1522) has 31

   If the pam_tally2 reports 5 or more counts for user srx, reset the pam_tally2 count for the srx user. For example:

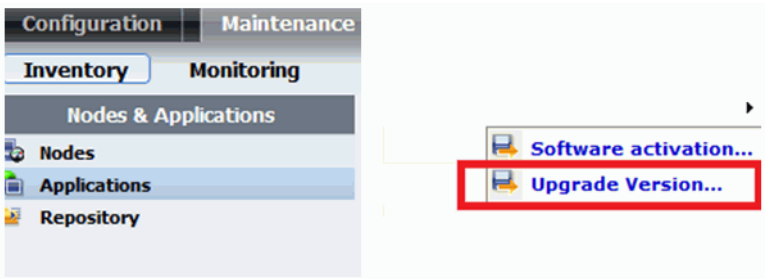
   # pam_tally2 --user srx --reset

   Query the pam_tally2 count again to ensure there are no pam_tally2 errors for the srx user. For example:

   # pam_tally2

4. Repeat the commands of step 3 on node 2.

5. Login to the CMP and navigate to **Maintenance > Inventory > Applications**. For the corresponding OSV system, click on the arrow at the end of the line on the right and select **Upgrade Version** …



6. A window opens showing the contents of directory /repository/upload of the node(s).
7. Click on Cancel button in order to close the window. The Switch becomes idle again.

8.10 Resolving Migration Toolkit node.cfg File Creation Issues

Use one of the following two methods to resolve Migration Toolkit node.cfg file creation issues:

1. Use the IFGUI Update (EZIP). **This is the recommended method.** Refer to Section 8.10.1, “Correct the node.cfg using the IFGUI Update (EZIP)”, on page 518.
2. If time or other constraints prevent the use of the EZIP method, use the create_node.cfg.pl script to generate a node.cfg of the source release. Refer to Section 8.10.2, “Correct the node.cfg using the create_node.cfg.pl Script”, on page 518.

If the target node.cfg file build is successful, links back to the Upgrade/Migration procedures are provided in Section 8.10.3, “Links to the Upgrade/Migration Procedures”, on page 519.

Attention: If the target node.cfg build is not successful, contact your next level of support.

Attention: When you upgrade to OSV V11, you will see two disabled parameters: **osv_emergency_mode** and **osv_esinet_esrp_mode**. These parameters are viable only for customers who have acquired the ESRP license, so ignore them and continue with the upgrade.

8.10.1 Correct the node.cfg using the IFGUI Update (EZIP)

Attention: If the OSV system contains invalid or unused configuration elements (e.g.; snmp servers), that info will be built into the node.cfg file. For this reason the IFGUI Update (EZIP) is the recommended method to resolve node.cfg issues. During the "Edit System Configuration" step of the EZIP process these invalid or unused configuration elements can be removed or updated as necessary.

Attention: Any questions should be addressed to the next level of support.

1. For details, refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”.
2. After the successful EZIP, use the ZEN tool to manually generate the node.cfg of the target release as follows:

   ```
   # zen upgrade node.cfg
   ```

   - **If the end result is "Exception", contact your next level of support.**
   - If the end result shows text indicating the conversion was successful, then the target release node.cfg file is stored in:

     `/repository/config/<TargetReleaseNumber>/node.cfg`
3. If this procedure is successful, continue the Upgrade/Migration procedure. Refer to Section 8.10.3, “Links to the Upgrade/Migration Procedures”, on page 519.

8.10.2 Correct the node.cfg using the create_node.cfg.pl Script

If time or other constraints prevent the use of the EZIP method, use the method suggested below.

Attention: The create_node.cfg.pl script will create a node.cfg file based on the actual configuration of the OSV. If the OSV system contains invalid or unused configuration elements (e.g.; snmp servers), that info will be built into the

generated node.cfg file. For this reason the IFGUI Update (EZIP) is the recommended method to resolve node.cfg issues. With EZIP, these invalid or unused configuration elements can be removed or updated as necessary.

Attention: Any questions should be addressed to the next level of support.

Use the create_node.cfg.pl script to generate a node.cfg of the source release. Then convert the source release node.cfg to the target release format. The step-by-step instructions are as follows:

1. Log on to **Node 1** as user *root*.
2. Create the source release node.cfg file. Enter the following commands to collect system information and create the source release node.cfg:

   ```
   # cd /opt/unisphere/srx3000/ifw/bin/
   # ./create_node_cfg.pl
   ```

   Upon successful execution of the script, this message will be displayed:
   `Generated node.cfg file`

   The source release node.cfg file will be saved in the "**`/opt/unisphere/srx3000/ifw/bin/`**" path as `cfgen_node.cfg`.
3. Copy the `cfgen_node.cfg` to `/tmp/node.cfg as follows`:

   ```
   # cp -p /opt/unisphere/srx3000/ifw/data/cfgen_node.cfg /tmp/node.cfg
   ```
4. Use the ZEN tool to manually generate the node.cfg of the target release as follows:

   ```
   # zen upgrade /tmp/node.cfg
   ```

   - **If the end result is "Exception", contact your next level of support.**
   - If the end result shows text indicating the conversion was done successfully, then the target release node.cfg file is stored in:

     `/repository/config/<TargetReleaseNumber>/node.cfg`
5. If this procedure is successful, continue the Upgrade/Migration procedure. Refer to Section 8.10.3, “Links to the Upgrade/Migration Procedures”, on page 519.

8.10.3 Links to the Upgrade/Migration Procedures

Follow the appropriate link to return to the tasklist of your Upgrade/Migration procedure.

If you arrived here from Table 19, return to step 7 on page 642

If you arrived here from Table 20, return to step 7 on page 545

If you arrived here from Table 21, return to step 7 on page 554

9 Migrations to OpenScape Voice V11

Attention: In Migration scenarios the source system can be on V9 or V10. If the source system is V11, make sure that the **PatchSet** level of the target system after the Image installation is at least equal or greater than the one of the source. Migrations to a lower PatchSet level are not supported.

Attention: For migration strategies where the Hardware Platform changes, install the toolkit rpm on the target release to automatically generate a node.cfg file for the target release as described in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457. Then use this generated target node.cfg as a guide to build the actual target release node.cfg using the NCPE or CDC tool that meets the requirements of your particular migration scenario.

Attention: If you have not already done so, read Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11” before using the checklists in this chapter as well as checking Table on page 417 for the supported hardware servers for migration.

When the target system is a Virtual Machine this migration procedure does detail specifics regarding the node.cfg creation, data export (from the source system) and restore (for the target system) but assumes the virtual environment is ready at the time the OSV Image is to be installed.

Knowledge of the VMware environment is a pre-requisite. If the hardware of the source release is reused as the virtual machine host(s) for this migration scenario; before the OSV Image can be installed the ESXi must be installed and the virtual environment configuration built on the servers. This will extend the system down time. Section 4.3, “Virtualization Environment Setup” should be referenced for details.

If the migration includes a move to different server(s) acting as host(s) for the virtual machines the virtual environment configuration should be built in advance. Section 4.3, “Virtualization Environment Setup” should be referenced for details.

If a Fallback is required the source release servers will have to be restored to an on-line state.

- If the virtual machines were created on the original native hardware then a file system restore will be required to restore the source release.
- If the virtual machines were created on hosts other than the original native hardware the native hardware will have to be brought to an online state.

Any questions should be addressed to your next level of support before proceeding.

Attention: When servers (for example, media server or DLS) in the same network as one of the OSV's subnets need to communicate with another of the OSV's subnets, then changes to the network firewall are required to allow this communication. Any questions should be addressed to the next level of support.

The migration (data export, image install, and data import) takes approximately 130 minutes to complete with a system downtime of approximately 100 minutes.

Perform only the task indicated and then return to the checklist. As an example; if the checklist indicates Section 7.3.1, “Upgrade Scenarios”should be performed, follow the link to Section 7.3.1, “Upgrade Scenarios”, perform that task, and return to the checklist.

When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader toolbar. This will ease the navigation between the checklists and associated sections of the IUG.

After executing a checklist task, select the ‘Previous View’ icon in the Reader tool bar to return to the checklist.

Upgrades that include one or more of the following must use the checklists in this chapter:

Attention: These migrations are performed using the migration toolkit and appropriate checklist.

- Hardware platform migration (product type and node deployment changes are allowed).

  Refer to Section 9.1, “Migration Scenarios”, on page 523.

- Node deployment migration (existing OpenScape Voice server hardware reused):

  Change the system from co-located nodes to geographically separated nodes.

- The following notes have to be considered:

Note: A node deployment migration or any migration to a Voice Server target release with a different network schema than the source release may require the external DNS be administered to reflect the new IP addresses of the Voice Server node(s). TLS certificates (including custom TLS certificates) should be reviewed and generated as required for these cases.

9.1 Migration Scenarios

These migrations are performed using the migration toolkit and appropriate checklist.

Before starting the Migration, ensure that the hardware servers to be used for the target release are supported for migration. For details, refer to Table on page 417.

The supported upgrade paths for hardware platform migration scenarios are as follows:

- Simplex to simplex migration: Refer to Section 9.1.1, “Simplex to Simplex Migration”.
- Simplex to standard duplex migration: Refer to Section 9.1.2, “Simplex to Standard Duplex Migration”.
- Standard duplex to standard duplex migration (Node deployment changed): Refer to Section 9.1.3, “Standard Duplex to Standard Duplex Migration”

9.1.1 Simplex to Simplex Migration

Use Table 23 to monitor the migration when the target is a native hardware system or when it is a Virtual Machine. Perform only the task indicated and then return to the checklist. As an example; if the checklist indicates Section 7.3.1 should be performed, follow the link to Section 7.3.1, perform that task, and return to the checklist.

Hint: When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader toolbar. This will ease the navigation between the checklists and associated sections of the IUG.

After executing a checklist task, select the ‘Previous View’ icon in the Reader tool bar to return to the checklist.

Task	Target is Native HW	Target is VM
1.	If the integrated OSV system contains a DLS and migration of the DLS to an offboard server is planned, perform data collection on the source release (integrated) DLS before starting any migration procedure. Please refer to the DLS Release Notes for the data collection instructions.	
2.	Refer to Section 8.1.2, “Preparation Checklist”, on page 445 and Section 8.1.3, “Required Documents”, on page 447.	
3.	Refer to Section 8.2.1, “System Information and Access Rights”, on page 454 and Section 8.2.2, “Logging”, on page 454.	

Table 23 Simplex to Simplex Migration

Task	Target is Native HW	Target is VM
4.	Refer to Section 8.3.3, “Verify Prerequisites Met According to Release Notes”, on page 461 and Section 8.3.4, “Obtain Licenses for the Target Release”, on page 462.	
5.	Refer to Section 8.4, “Pre-Maintenance Window Activities”, on page 463.	
6.	Create the initial node.cfg file for the target system by downloading and installing the Toolkit rpm on the source system which automatically generates the node.cfg file for the target system. Refer to Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457. This procedure provides an initial target release node.cfg file which can be used as a guide to create the final target release node.cfg file (**in Task 6)**.	
7.	Adapt the parameters from the node.cfg collected in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 to build the final node.cfg for the target system. Use Section 9.2, “Create the Node.cfg for the Target System”. This file will be used during the installation of the OSV Image on the Simplex native or virtual machine.	

Table 23 Simplex to Simplex Migration

Task	Target is Native HW	Target is VM
8.	Copy the node.cfg.primary file for the target system to a USB memory stick and label the stick node.cfg.primary. Refer to Section 4.2.3.2, “Image installation/System Restore USB/Service System Image Write” Remember to include the response.cfg.primary file along with the node.cfg (node.cfg.primary) when creating the installation ISO. **Note:** Patch sets and emergency patch sets may be loaded onto the USB memory stick (or sticks - depending on the system configuration) for automatic installation during the image install. Refer to Section 2.7, “Including Patch Sets and License files on the USB Memory Stick(s)”, for details.	Create the node.cfg installation file as an ISO image because this image can contain the node.cfg, license file, and the latest release patch sets all of which will be automatically updated to the OSV node (nodes in the case of a duplex system); removing the need for manual license file transfer and a post-installation rolling upgrade. This practice also results in installation time savings. Remember to include the response.cfg.primary file along with the node.cfg (node.cfg.primary) when creating the installation ISO. Create a Installation ISO file from the node.cfg file. Refer to Section 4.3.4.2, “Saving the node.cfg, license and patch sets to an Installation ISO Image” for direction.
9.		After preparing the Installation ISO image, transfer the Installation ISO files and the OSV Image ISO file to the datastore. Use steps 1 through 4 of Section Section 4.3.5.2, “Uploading a File to the Datastore” as a guide for uploading the file to the datastore. To make the OSV ISO Image and Installation ISO files available from CD/DVD drives see Section Section 24.3, “Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration”
10.	Run RapidStat. Errors and/or Warnings must be reviewed and corrected as necessary before continuing.	

Table 23 Simplex to Simplex Migration

Task	Target is Native HW	Target is VM
11.	Export the data of the source system. Refer to Section 9.4, “Exporting Source System Data”. Remove the USB stick(s) from the old hardware as they will be needed for the OSV image installation of the new hardware.	Export the data of the source system. Since the created export file will be imported to a virtual system, refer to Section 9.4, “Exporting Source System Data”.
12.	Disconnect all cables from the nodes, relocate to the geographically separate locations and reattach the cables as appropriate.	The resource allocation of target release virtual machines must be verified from the latest document OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide of the target release OpenScape Voice Installation and Upgrade Guide (IUG). The resource allocation of the virtual machine(s) must be adjusted to the values listed in the latest document OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide of the target release IUG before the upgrade begins. Some virtual machine resource changes require the machine be shut down (e.g. vCPU and Memory resources changes). This activity will cause a loss of service for the Integrated Simplex OSV and its Applications server. Questions should be addressed to your next level of support.

Table 23 Simplex to Simplex Migration

Task	Target is Native HW	Target is VM
13.	Install the OpenScape Voice V11 image onto the target system.Refer to Chapter 4, “Installing the OpenScape Voice Reference Image”.	**Note:** Knowledge of the VMware environment is a prerequisite. If the hardware of the source release is reused for this migration scenario; before the OSV Image can be Installed the ESXi must be installed and the virtual environment configuration built. This will extend the system down time. Section 4.3, “Virtualization Environment Setup” should be referenced for details. If the hardware is being reused it should be configured for the virtual environment now. Install the OpenScape Voice V11 image onto the target system. Refer to Section 24.5, “Install the OpenScape Voice V11 Image onto the Upgrade VM Target System”.
14.	Customize node 1. If the OSV licenses were not included on the Installation USB (Non VM) or the Installation ISO (VM), download the licenses to the OpenScape Voice nodes. Refer to Section 9.12.1.2, “Customize Node 1”, on page 567. **Note:** Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability.	
15.	An integrated system should ensure the applications server is updated with the latest released DVD/PatchSet/HotFix. If an Applications PatchSet (Update) or HotFix is required, please refer to Section 5.2.3.5, “Update/Upgrade of Integrated Applications”, on page 310 or Section 5.2.3.6, “Installing a HotFix - Integrated Apps server”, on page 313.	

Table 23 Simplex to Simplex Migration

Task	Target is Native HW	Target is VM
16.	Add additional languages. For Simplex systems, after the successful Upgrade or Migration, the English language will be installed by default. Any other languages will have to be installed. As a part of the pre-maintenance window preparation of Section 8.4.13, “List the Languages Installed on the Applications Server”, a list of required languages should have been collected. Reference Appendix 28, “Guidelines for Language and Application Package adds to Simplex Systems”", onpage 783 for more details.	
17.	Download the migration toolkit software (*UNSPmigration-<V#>.rpm*) and install it onto the target system. Refer to Section 9.5 on page 551.	
18.	Import the data of the source system. Refer to Section 9.6 on page 552.	
19.	Remove the migration toolkit software (*UNSPmigration-<V#>.rpm*) from the target system. Refer to Section 9.7 on page 554.	
20.	Execute RapidStat and place test calls to verify there are no issues and that the system is functioning correctly.	
21.	Refresh the CMP after completing the Upgrade/Migration procedure by logging into the CMP and navigating to the following menu: **Configuration > OpenScape Voice > General > Switches** Select your switch and click on Refresh Switch Data button. In case some information is incorrect, you may use the Edit option to correct it, for example IP address of node 1.	
22.	Complete the upgrade. Refer to Section 7.4, “Completing the Upgrade/Migration to V11”.	

Table 23 Simplex to Simplex Migration

9.1.2 Simplex to Standard Duplex Migration

At the discretion of the technician checklist tasks 1 through 8 may be performed prior to the upgrade maintenance window.

Use Table 25 to monitor the migration to the new hardware servers or VMs in which the node deployment of the target system is kept the same as it was in the source system. Perform only the task indicated and then return to the checklist. As an example; if the checklist indicates Section 7.3.1 should be performed, follow the link to Section 7.3.1, perform that task, and return to the checklist.

Hint: When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader toolbar. This will ease the navigation between the checklists and associated sections of the IUG.

After executing a checklist task, select the ‘Previous View’ icon in the Reader tool bar to return to the checklist.

Tasks	Target is Native HW	Target is VM
1.	If the integrated OSV system contains a DLS and migration of the DLS to an offboard server is planned, perform data collection on the source release (integrated) DLS before starting any migration procedure. Please refer to the DLS Release Notes for the data collection instructions.	
2.	Refer to Section 8.1.2, “Preparation Checklist”, on page 445 and Section 8.1.3, “Required Documents”, on page 447.	
3.	Refer to Section 8.2.1, “System Information and Access Rights”, on page 454 and Section 8.2.2, “Logging”, on page 454.	
4.	Refer to Section 8.3.3, “Verify Prerequisites Met According to Release Notes”, on page 461 and Section 8.3.4, “Obtain Licenses for the Target Release”, on page 462.	
5.	Refer to Section 8.4, “Pre-Maintenance Window Activities”, on page 463.	
6.	Create the initial node.cfg file for the target system by downloading and installing the Toolkit rpm on the source system which automatically generates the node.cfg file for the target system. Refer to Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457. This procedure provides an initial target release node.cfg file which can be used as a guide to create the final target release node.cfg file (**in Task 6)**.	

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM
7.	Adapt the parameters from the node.cfg collected in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 to build the final node.cfg for the target system. Use Section 9.2, “Create the Node.cfg for the Target System”. This file will be used during the installation of the OSV Image on the Simplex native or virtual machine.	
8.	Copy the node.cfg.primary file for the target system to a USB memory stick and label the stick node.cfg.primary; copy the node.cfg.secondary file for the target system to another USB memory stick and label that stick node.cfg.secondary. Refer to Section 4.2.3.2, “Image installation/System Restore USB/Service System Image Write” Remember to include the response.cfg.primary file along with the node.cfg (node.cfg.primary) when creating the installation ISO. --- **Note:** Patch sets and emergency patch sets may be loaded onto the USB memory stick (or sticks - depending on the system configuration) for automatic installation during the image install. Refer to Section 2.7, “Including Patch Sets and License files on the USB Memory Stick(s)”, for details. ---	Create the node.cfg installation file as an ISO image because this image can contain the node.cfg, license file, and the latest release patch sets all of which will be automatically updated to the OSV node (nodes in the case of a duplex system); removing the need for manual license file transfer and a post-installation rolling upgrade. This practice also results in installation time savings. Remember to include the response.cfg.primary file along with the node.cfg (node.cfg.primary) when creating the installation ISO. Create an Installation ISO file from the node.cfg file. Refer to Section 4.3.4.2, “Saving the node.cfg, license and patch sets to an Installation ISO Image” for direction.

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM
9.	Ensure that the required network components are installed (for example: additional Ethernet switches, L2/L3 routers to support the geographically separated nodes) **Note:** Section 2.3, “Guidelines for Geographically Separated Nodes”details the requirements for network separated systems. If this section has not already been reviewed please do so now.	After the Installation ISO image is prepared, transfer the Installation ISO files and the OSV Image ISO file to the data store. Use steps 1 through 4 of Section 4.3.5.2, “Uploading a File to the Datastore”as a guide for uploading the file to the data store. To make the OSV ISO Image and Installation ISO files available from CD/DVD drives see Section 24.3, “Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration”
10.	Ensure that the new hardware servers for OpenScape Voice have been installed. In case of Virtual Machines, ensure that the Virtual Machines have been created. For example: BIOS/RAID is configured, firmware updated, and remote console function is configured. Ethernet cables should not be connected at this time. If the servers have not been installed, refer to the appropriate checklist for the server type and install them now.	
11.	Run RapidStat. Errors and/or Warnings must be reviewed and corrected as necessary before continuing.	
12.	Export the data of the source system. Refer to Section 9.4, “Exporting Source System Data”. Remove the USB stick(s) from the old hardware in case of native HW as they will be needed for the OSV image installation of the new hardware.	

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM
13.	For the external Applications server(s) monitoring the Voice Server system to be updated; • If the external Applications server is deployed as a Multiple Standard Duplex Communication Server remove the Voice server system to be updated from the external Applications server List of Switches. Do not add the Voice Server to the external Applications server until instructed to do so in task 14of this procedure. • If the external Applications server is monitoring this system only, i.e. Applications servers deployed in a "Standard Duplex - Small Deployment", stop symphoniad. The symphoniad process will be restarted as part of the external Applications server Installation/update process. `# /etc/init.d/symphoniad stop` **Attention:** Removing an OpenScape Voice server from a Standard Duplex (Large or Small) UC Applications deployment will result in the loss of UC application data (e.g.; OpenScape Users/Resources). Any questions should be addressed to your next level of support before proceeding.	

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM

14.	Install/update the OpenScape Applications onto the external applications server as follows:
	
	Note: Do NOT execute the actions described in Section 9.8, “Configure the OpenScape Applications Server for Access to the Nodes” until task 21 is completed.
	
	• Upgrading the External Applications Server (OffBoard). Direct update from these Applications server levels to the V10 Applications level is supported:
	  • V9 DVD Build, Hotfix level to V10 DVD Build level. The Build level of the source and target are specified in the V11 Release Notes.
	
	For Multiple Communications Server Admin deployments refer to Section 5.7, “Upgrade of Offboard (External) Apps Server” of this document and the following subsection for the appropriate procedure;
	  • Section 5.7.1, “Upgrade of V8R1 Offboard Applications to V10”, on page 377
	
	For Standard Duplex Small or Standard Duplex Large deployments refer to the *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide (*where *x* is the software release version*)*, Section “Updating, Upgrading and Migrating”.
	
	Note: The DLS component can also be installed on the external OpenScape Applications server; review the DLS release notes for sizing limitations if the DLS component is to be installed on the external OpenScape Applications server.
	
	• Configure the external OpenScape Applications server for access to the nodes. Refer to Section 9.8, “Configure the OpenScape Applications Server for Access to the Nodes” for instructions.	

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM
15.	Disconnect all cables from the nodes, relocate to the geographically separate locations and reattach the cables as appropriate.	The resource allocation of target release virtual machines must be verified from the latest document OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide of the target release OpenScape Voice Installation and Upgrade Guide (IUG). The resource allocation of the virtual machine(s) must be adjusted to the values listed in the latest document OpenScape Solution Set Virtual Machine Resourcing and Configuration Guide of the target release IUG before the upgrade begins. Some virtual machine resource changes require the machine be shut down (e.g. vCPU and Memory resources changes). This activity will cause a loss of service for the Integrated Simplex OSV and its Applications server.

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM
16.	Install the OpenScape Voice V11 image onto the target system.Refer to Section , “Installing the OpenScape Voice Reference Image”.	**Note:** Knowledge of the VMware environment is a prerequisite. If the hardware of the source release is reused for this migration scenario; before the OSV Image can be Installed the ESXi must be installed and the virtual environment configuration built. This will extend the system down time. Section 4.3, “Virtualization Environment Setup” should be referenced for details. If the hardware is being reused it should be configured for the virtual environment now. Install the OpenScape Voice V11 image onto the target system. Refer to Section 24.5, “Install the OpenScape Voice V11 Image onto the Upgrade VM Target System”.
17.	Log in to node 1. Refer to Section 9.12.1.1, “Log In to Node 1”	
18.	Customize node 1. If the OSV licenses were not included in the Installation USB (Non VM) or the Installation ISO (VM), download the licenses to the OpenScape Voice nodes. Refer to Section 9.12.1.2, “Customize Node 1”	
19.	Log in to node 2. Refer to Section 9.12.2.1, “Log In to Node 2”.	
20.	Customize node 2. If the OSV licenses were not included on the Installation USB (Non VM) or the Installation ISO (VM), download the licenses to the OpenScape Voice nodes. Refer to Section 9.12.2.2, “Customize Node 2”.	

Table 24 Simplex to Duplex Migration

Tasks	Target is Native HW	Target is VM
21.	If the latest patchsets or emergency patch sets for the target release were not included as part of the Installation ISO; the OSV nodes must be updated to the latest patchset or emergency patchset. Refer to the Release Notes for the target release. **Note:** Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability.	
22.	Download the migration toolkit software (*UNSPmigration-<V#>.rpm*) and install it onto the target system. Refer to Section 9.5, “Downloading and Installing the Migration Toolkit Software to the Target System”.	
23.	Import the data of the source system. Refer to Section 9.6, “Importing the Source System Data to the Target System”.	
24.	Remove the migration toolkit software (*UNSPmigration-<V#>.rpm*) from the target system. Refer to Section 9.7, “Remove the Migration Toolkit Software from the Target System”.	
25.	Execute RapidStat and place test calls to verify there are no issues and that the system is functioning correctly.	
26.	Migrate the UC data to the external OpenScape Applications server for access to the nodes. Refer to *OpenScape UC Application V10, Installation and Upgrade, Installation Guide*.	
27.	Complete the upgrade. Refer to Section 7.4, “Completing the Upgrade/Migration to V11”.	

Table 24 Simplex to Duplex Migration

9.1.3 Standard Duplex to Standard Duplex Migration

At the discretion of the technician checklist tasks 1 through 9 may be performed prior to the upgrade maintenance window.

Use Table 25 to monitor the migration to the new hardware servers or VMs in which the co-located node deployment of the source system is changed to a geographically separated node deployment in the target system. Perform only the task indicated and then return to the checklist. As an example; if the checklist indicates Section 7.3.1 should be performed, follow the link to Section 7.3.1, perform that task, and return to the checklist.

Hint: When viewing the Installation and Upgrade Guide (IUG) with Adobe Reader add the “Previous View” icon to the Reader tool bar. This will ease the navigation between the checklists and associated sections of the IUG.

After executing a checklist task, select the ‘Previous View’ icon in the Reader tool bar to return to the checklist.

Tasks	Target is Native HW	Target is VM
1.	Refer to Section 8.1.2, “Preparation Checklist” and Section 8.1.3, “Required Documents”	
2.	Refer to Section 8.2.1, “System Information and Access Rights” and Section 8.2.2, “Logging”	
3.	Refer to Section 8.3.3, “Verify Prerequisites Met According to Release Notes” and Section 8.3.4, “Obtain Licenses for the Target Release”	
4.	Refer to Section 8.4, “Pre-Maintenance Window Activities”.	
5.	Create the initial node.cfg file for the target system by downloading and installing the Toolkit rpm on the source system which automatically generates the node.cfg file for the target system. Refer to Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”. This procedure provides an initial target release node.cfg file which can be used as a guide to create the final target release node.cfg file (in **Task 6**).	
6.	Create the final node.cfg file for the target system. Refer to Section 9.2, “Create the Node.cfg for the Target System”	

Table 25 Standard Duplex to Standard Duplex Migration

Tasks	Target is Native HW	Target is VM
7.	Copy the node.cfg.primary file for the target system to a USB memory stick and label the stick `node.cfg.primary`; copy the `node.cfg.secondary` file for the target system to another USB memory stick and label that stick node.cfg.secondary. Refer to Section 4.2.3.2, "Image installation/System Restore USB/Service System Image Write" **Note:** Patch sets and emergency patch sets may be loaded onto the USB memory stick (or sticks - depending on the system configuration) for automatic installation during the image install. Refer to Section 2.7, "Including Patch Sets and License files on the USB Memory Stick(s)", for details.	Create the node.cfg installation file as an ISO image because this image can contain the node.cfg, license file, and the latest release patch sets all of which will be automatically updated to the OSV node (nodes in the case of a duplex system); removing the need for manual license file transfer and a post-installation rolling upgrade. This practice also results in installation time savings. Create an Installation ISO file from the node.cfg file. Refer to Section 4.3.4.2, "Saving the node.cfg, license and patch sets to an Installation ISO Image" for direction. Repeat the procedure for node 2 of a duplex system.
8.	If Node Deployment is changed ensure that the required network components (for example: additional Ethernet switches, L2/L3 routers) to support the geographically separated nodes are installed. **Note:** Section 2.3, "Guidelines for Geographically Separated Nodes"details the requirements for network separated systems. If this section has not already been reviewed please do so now.	After the Installation ISO image is prepared, transfer the Installation ISO files and the OSV Image ISO file to the datastore. Use steps 1 through 4 of Section 4.3.5.2, "Uploading a File to the Datastore" as a guide for uploading the file to the datastore. Remember to repeat the procedure for the node 2 Installation ISO of a duplex system. To make the OSV ISO Image and Installation ISO files available from CD/DVD drives see Section 24.3, "Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration"

Table 25 Standard Duplex to Standard Duplex Migration

Tasks	Target is Native HW	Target is VM
9.	Ensure that the new hardware servers for OpenScape Voice have been installed. In case of Virtual Machines, ensure that the Virtual Machines have been created. For example: BIOS/RAID is configured, firmware updated, remote console function is configured, and Ethernet cables are attached. If the servers have not been installed, refer to the appropriate checklist for the server type and install them now.	
10.	Run RapidStat. Errors and/or Warnings must be reviewed and corrected as necessary before continuing.	
11.	Download the migration toolkit software (*UNSPmigration-<V#>.rpm*) and install it onto the target system. Refer to Section 9.5, “Downloading and Installing the Migration Toolkit Software to the Target System”	
12.	Export the data of the source system. Refer to Section 24.4, “Export Source System Data”.	
13.	For the external Applications server(s) monitoring the Voice Server system to be updated: • If the external Applications server is deployed as a Multiple Standard Duplex Communication Server, remove the Voice server to be migrated from the external Applications server List of Switches. Do not add the Voice Server to the external Applications server until instructed to do so in task 22 of this procedure. • If the external Applications server is only monitoring this Voice Server, i.e. the Applications server is deployed in a “Standard Duplex, Small Deployment”, then stop symphoniad on the Applications server. The symphoniad process will be restarted later as part of the external Applications server Installation/ update process. Enter the following command on the Applications server to stop the symphoniad process: `# /etc/init.d/symphoniad stop` **Attention:** Removing an OpenScape Voice server from a Standard Duplex (Large or Small) UC Applications deployment will result in the loss of UC application data (e.g.; OpenScape Users/Resources). Any questions should be addressed to your next level of support before proceeding.	

Table 25 Standard Duplex to Standard Duplex Migration

Tasks	Target is Native HW	Target is VM

14.	Install/update the OpenScape Applications on the external applications server as follows:
	
	Note: Do NOT execute the actions described in Section 9.8, "Configure the OpenScape Applications Server for Access to the Nodes" until task 21 is complete.
	
	• Upgrading the External Applications Server (OffBoard).
	  • V9 DVD Build, Hotfix level to V10 DVD Build level. The Build level of the source and target are specified in the V11 Release Notes.
	  For Multiple Communications Server Admin deployments refer to Section 5.7, "Upgrade of Offboard (External) Apps Server" of this document and the following subsection for the appropriate procedure;
	  • Section 5.7.1, "Upgrade of V8R1 Offboard Applications to V10", on page 377
	• **For Standard Duplex Small or Standard Duplex Large deployments refer** to the *OpenScape UC Application Vx, Installation and Upgrade, Installation Guide (*where *x* is the software release version*)*, Section "Updating, Upgrading and Migrating".
	
	Note: The DLS component can also be installed on the external OpenScape Applications server; review the DLS release notes for sizing limitations if the DLS component is to be installed on the external OpenScape Applications server.	

Table 25 Standard Duplex to Standard Duplex Migration

Tasks	Target is Native HW	Target is VM
15.	Disconnect all cables from the nodes, relocate to the geographically separate locations and reattach the cables as appropriate: If Node Deployment is unchanged swap the cables from the old system to the new system. Refer to Chapter 3, “Installing the Hardware Platform” and locate the subsection that describes each platform's cable connections.	The resource allocation of target release virtual machines must be verified, according toSection 4.3.3.2, “Virtual Machine Configuration Parameters Overview” Some virtual machine resource changes require the machine be shut down (e.g. vCPU and Memory resources changes). This activity will cause a loss of service for Applications servers.
16.	Install the OpenScape Voice V11 image onto the target system.Refer to Chapter 4, “Installing the OpenScape Voice Reference Image”.	Knowledge of the VMware environment is a pre-requisite. If the hardware of the source release is reused for this migration scenario; before the OSV Image can be Installed the ESXi must be installed and the virtual environment configuration built. This will extend the system down time. Section 4.3, “Virtualization Environment Setup” should be referenced for details. If the hardware is being reused it should be configured for the virtual environment now. Install the OpenScape Voice V11 image onto the target system. Refer to Section 24.5, “Install the OpenScape Voice V11 Image onto the Upgrade VM Target System”
17.	Log in to node 1. Refer to Section 9.12.1.1, “Log In to Node 1”	
18.	Customize node 1. If the OSV licenses were not included in the Installation USB (Non VM) or the Installation ISO (VM), download the licenses to the OpenScape Voice nodes. Refer to Section 9.12.1.2, “Customize Node 1”	
19.	Log in to node 2. Refer to Section 9.12.2.1, “Log In to Node 2”.	
20.	Customize node 2. If the OSV licenses were not included on the Installation USB (Non VM) or the Installation ISO (VM), download the licenses to the OpenScape Voice nodes. Refer to Section 9.12.2.2, “Customize Node 2”.	

Table 25 Standard Duplex to Standard Duplex Migration

Tasks	Target is Native HW	Target is VM
21.	If the latest patchsets or emergency patch sets for the target release were not included as part of the Installation ISO; the OSV nodes must be updated to the latest patchset or emergency patchset. Refer to the Release Notes for the target release. **Note:** Unless directed otherwise by Release Notes, the target OpenScape Voice server should be at the latest patch level declared for General Availability.	
22.	Download the migration toolkit software (*UNSPmigration-<V#>.rpm*) and install it onto the target system. Refer to Section 9.5, “Downloading and Installing the Migration Toolkit Software to the Target System”.	
23.	Import the data of the source system. Refer to Section 9.6, “Importing the Source System Data to the Target System”.	
24.	Remove the migration toolkit software (*UNSPmigration-<V#>.rpm*) from the target system. Refer to Section 9.7, “Remove the Migration Toolkit Software from the Target System”.	
25.	Execute RapidStat and place test calls to verify there are no issues and that the system is functioning correctly.	
26.	Configure the external OpenScape Applications server for access to the nodes. Refer to Section 9.8, “Configure the OpenScape Applications Server for Access to the Nodes” for instructions. Refresh the CMP after completing the Migration procedure by logging into the CMP and navigating to the following menu: **Configuration > OpenScape Voice > General > Switches** Select your switch and click on Refresh Switch Data button. In case some information is incorrect, you may use the Edit option to correct it, for example **IP address of node 1** and **IP address of node 2**.	
27.	Complete the upgrade. Refer to Section 7.4, “Completing the Upgrade/Migration to V11”.	

Table 25 Standard Duplex to Standard Duplex Migration

9.2 Create the Node.cfg for the Target System

Attention: This procedure is NOT intended for;

Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”
If you are performing the Outage Free toolkit upgrade method, then employ

Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457.

All other migrations should employ this procedure.

Note: If ‘route operations’ message windows are presented during the Node.cfg creation, the “OK” button should be selected. For more information regarding the Source Based Routing feature, refer to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11”.
The implementation or updating of source based routes during an upgrade will require the use of a Migration strategy (and therefore a system outage). Migration strategies are detailed in Chapter 9, “Migrations to OpenScape Voice V11”.
For duplex systems, if an OpenScape Voice system outage cannot be tolerated during the upgrade, then the Outage Free toolkit upgrade will need to be performed. The Outage Free toolkit upgrade method is detailed in Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”, on page 483.
As a general rule, no changes to the OSV target release node.cfg are allowed during the three upgrade procedure detailed in Chapter 8, “Upgrades to OpenScape Voice V11”. After a Chapter 8 upgrade procedure is completed, the EZIP feature can be employed to establish source based routing (by specifying default gateway addresses). For more information regarding the EZIP feature, refer to Chapter 13, “Updating the Node.cfg File (Also Known as EZIP)”.

Attention: For the migration scenarios, it is recommended that the user create the node.cfg from scratch using the NCPE. Specify the new IP configuration using the appropriate tabs. The node.cfg collected in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 may be used as a reference for external server IP addresses (e.g., Name (DNS), NTP, CSTA, SNMP, License, Billing, SNMP and Misc. Host servers.)

If it is decided to create the target release node.cfg from scratch (while employing the node.cfg collected in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 as a template); steps 1, 3a), 3b), and 3c) do not apply in this case. Open the node.cfg, step 2), and proceed to step 3d). Before sure to employ the latest target release NCPE.

Use the latest version of the OffLineWizard software indicated in the release notes for the target release.

Note: X-channel and CIGroup references apply to virtual duplex deployments.

Attention: Read Section 9.10, “Restrictions for Migrations In Which The Network Configuration Is Changed”, on page 559 before proceeding. A link back to this section will be provided.

---

1. Transfer the node.cfg file of the target release generated in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 to a Windows/Linux machine that can run the OfflineWizard.

   Note: If necessary, refer to the OpenScape Voice base software release note on G-DMS for the link to SWS to download the Installation Wizard zip file.

   Recommended practices for file transfer and burning of CD/DVD media;
   1. If a checksum, md5sum or sha file is delivered with OpenScape software it is a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. **If necessary, third party software can be used to calculate these values.**
   2. When burning a file to a CD/DVD media use a lower burning speed (i.e.; 4x).
   3. Use the 'verify' option of the burning application to ensure data integrity after the DVD burning is complete.

   Unzip the downloaded file. Now there should be a parent directory named 'ncpe-OfflineWizard-<version_number>'. Change to the bin path located one level below 'ncpe-OfflineWizard-<version_number>'.

   Attention: Use WinZIP to extract the ncpe zip file, as other tools will not work.

   ---

2. Start the OffLineWizard.

   a) Change directory to ncpe-OfflineWizard-<version_number>'\bin path.

   For Windows systems open (double click) the file named ifgui.cmd.

For Linux systems; open the file named ifgui.

Note: For Linux users, if needed, export the DISPLAY of the output to your PC by entering "export DISPLAY=<IP address>:0", where the IP address of the destination of the DISPLAY is to be sent is used. This step is done as the root user.

---

b) Select **Install** on the first screen, click **Next**, then select **Expert Mode** on the next screen.

Attention: In the Expert mode of the NCPE, page IP Configuration (1/5); Updating the Management subnets or netmasks will impact the Signaling, Billing, Cluster, and Remote Administration IP settings. If the Management subnet or netmask IP addresses are changed please review/verify the Signaling, Billing, Cluster, and Remote Administration settings before proceeding to another page of the NCPE.

Note: Some node.cfg files may report 'Invalid Data' related to IPV6 addressing. As a general rule; If IPV6 addressing is not needed, remove all IPV6 addresses. If IPV6 addressing is needed, all IPV6 address parameters must be populated.

IPV6 address parameters are located at:

- IP Configuration 1/5 in the Signaling tab
- IP Configuration 2/5 IPv6 Configuration
- IP Configuration 5/5 Node 1 and Node 2 IPv6 Routes tables

---

3. From the NCPE GUI:

   a) Under "File", open the target release file node.cfg that was created in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 and generate the final node.cfg for the target release.

   b) Enter "OK" and the click "OK" to the Warning window to accept new parameters added to the node.cfg.

      The Configuration and Hardware (1/1) screen contains a parameter; " **Preferred Node to Takeover** ". This parameter indicates which node reacts first to an x-channel failure. The value defaults to node 2. If the x-channel fails, node 2 will be the first to call the shutdown agents in order to "kill" node 1.

      The Configuration and Hardware (1/1) screen contains a new parameter; "**Cluster Timeout**". This parameter indicates how long the cluster cross channel (AKA x-channel and cluster interconnect) can be down before

the Cluster Manager declares "Changed cross channel state to DOWN" and initiates shutdown agent activity to prevent a split brain condition. The default value is 15 seconds for all OpenScape voice deployments. If a node to node connection failure is less likely than a server failure (e.g.; in a co-located configuration) the timeout should be set to 10 seconds. If the likelihood of short term connection failures is higher, values of up to 15 seconds are recommended.

Reference Chapter 6, “Survival Authority and IPMI Shutdown Agents” for further details of the shutdown agents operation.

c) Under “Configuration and Hardware (1/1)” **make sure that the “Installation mode” is set to “normal”**. As appropriate, specify all new parameters for the new configuration of the target system.

Note: This section is intended for the procedures of the following sections: Section 8.5, Section 8.7, Section 9.1.1.

Note: If you arrive at Section 9.2, step 3d from Section 8.5 or Section 8.7, no modifications to the voice server hardware, product type or deployment are allowed. You should be employing a procedure from Chapter 9, “Migrations to OpenScape Voice V11” (if the Voice Server hardware, product type or deployment is to be changed). Only the changes indicated in steps 3b, 3c, and 3e through 3i are allowed if you arrived at Section 9.2, step 3d from Section 8.5 or Section 8.7.

---

d) Software Build ID: Select appropriate software build for your installation.

Answer ‘OK’ to Messages indicating ‘route operations’ have been performed.

e) Select the “IP Configuration (4/5)” screen.

If Static/Source Routes exist please verify there are **NO** duplicate routes. Duplicate routes will result in Image installation failures. Duplicate routes should be deleted using the Delete button (X) provided with each table. A method to verify the existence of duplicate routes is to employ the Preview mode, which is accessed by selecting the Preview icon in the NCPE menu bar (or by selecting the File menu and then Preview).

The NCPE defaults to the signaling subnet gateway as the default route subnet. If servers have been added to the node.cfg and these servers must communicate over a subnet other than the default route subnet; add these static routes at this time. Examples of servers that may require static routes;

- A Billing Server may need a static route to transfer data over the billing subnet.

- A SNMP server may need a static route to transfer data (snmp traps) over the administration subnet to a Network Operations Center.

The following info would be required to add this static route;

- The destination server IP address.
- The destination IP address netmask (typically 255.255.255.255).
- For the subnet gateway IP address, refer to IP Configuration page 1/5.
  - For the SNMP server example the Administration subnet gateway IP address would be employed.
  - For the Billing server example the Billing subnet gateway IP address would be employed.
- The Nafo ID is automatically populated based on the subnet gateway.

This same exercise should be performed in the “IP Configuration (5/5)” screen as required.

Attention: Ensure that any static routes manually added to the OpenScape Voice server (not added with the EZIP feature) are included in the static route table.
For more info regarding the EZIP refer to Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)” of this document.

---

f) The IP Configuration (3/6) page contains the **Assistant/CMP** parameter. For the **Assistant/CMP** value enter the IP address of the CMP/external Applications server associated with the OpenScape Voice system. This will trigger the installation scripts to add the IP address to the /etc/security/access.conf file. The **Assistant/CMP** parameter is intended for the IP address of an external (offboard) Applications server. It is recommended the CMP FQDN be included in the access.conf file access list. Refer to Section 4.5.2, “Verify Remote Access for srx Account in a Standard Duplex”, on page 339 for more details on this configuration.

No Assistant/CMP IP address is required for Simplex systems because the Applications server is integrated into the OpenScape Voice system.

g) Check and correct all errors/warnings (all red marked items). There is an exception: the user may disregard the warning about node names that contain an "underscore". This will happen if the node name of the old release contains an underscore and, by design, the same node name has to be carried over to the new release.

h) Select “File”, “Save As”, set “File of Type” to “**All Files**”, and enter File name: **node.cfg.primary** for a simplex system or node 1 of a duplex system. Click ‘Save’, make note of the path to which the file was saved and then click ‘OK’.

Note: Ensure that the file was not saved with a name that has a *.cfg* extension (for example: *node.cfg.primary.cfg*). The file name should be without the second *.cfg* extension (in fact: *node.cfg.primary*).

---

i) If this is a simplex system, go to step 4. For a duplex system, continue to the next step.

j) Select “File”, “Save As”, set “File of Type” to “**All Files**”, and enter File name: **node.cfg.secondary** for the second node of a duplex system. Click ‘Save’, make note of the path to which the file was saved and then click ‘OK’.

Note: Ensure the file was not saved with a name that has a *.cfg* extension (for example: *node.cfg.secondary.cfg*). The file name should be without the second *.cfg* extension (in fact: *node.cfg.secondary*).

---

4. Exit the NCPE. Select “File”, “Exit”, “Yes”, and “Finish”.

9.3 Download and Install the Migration Toolkit Software to the Source System

---

Attention: Always use the latest available version of the Migration Toolkit. The latest version works across all OSV releases. It is independent of the source or the target OSV release version.

As user *root*, verify that old Migration Toolkit software does not exist on the system. For a duplex system, execute the commands on both nodes:

```
# rpm -qa | grep -i UNSPmigration
```

If an old version of the migration toolkit software is found, then it should be removed with the following command:

```
# rpm -e --allmatches UNSPmigration
```

As user *root*, download to the /tmp directory and install the latest *UNSPmigration-<V#>.rpm* to the nodes (or node for a simplex system) as follows:

```
# cd /tmp          (directory where toolkit was copied to)
# rpm -ivh --replacefiles --replacepkgs UNSPmigration-<V#>.rpm
```

Example given;

```
# rpm -ivh --replacefiles --replacepkgs UNSPmigration-1.05-29.rpm
```

After some seconds, messages similar to the following will be displayed:

```
Preparing... ########################################### [100%]
1:UNSPmigration
########################################### [100%]
Checking for shared repository.
: : :
csv/simplex/
csv/simplex/12.00.02.ALL.15.csv
csv/simplex/V4.00.01.ALL.40.csv
csv/simplex/V5.00.01.ALL.11.csv
csv/simplex/V6.00.01.ALL.05.csv
csv/simplex/V7.00.01.ALL.07.csv
Valid node.cfg found. Invoking auto conversion.
Auto conversion successfull.
Converted node.cfg are found under /repository/config
Check /repository/config for converted node.cfg.
Migration tools installed successfully.
```

Similar messages appear when installing the Toolkit rpm on the second node of a duplex system.

As can be seen from the output above, a node.cfg file for the target release is automatically created on each node's shared repository. The file is:

/repository/config/<releaseNumber>/node.cfg

9.4 Exporting Source System Data

The `toolkit export8k` command with the 'cfg' option is used to export the data of the source system. The 'cfg' option is useful for Virtual systems where USBs are not available.

When using the 'cfg' option, the data is exported to a local path specified by <path to export>.

Path requirements

- The fully qualified path name must be provided.
- This path must **NOT** already exist.
- Must be located under `/repository/upload/`
- Must be consistent and accessible on all nodes in a duplex system.

Export the source system data as follows:

a) As user *root* on node 1 of the system, enter the following command:

Note: Execute this command from node 1 only.

```
# export8k -cfg <path to export>
```

Example:

```
# export8k -cfg /repository/upload/toolkit_Db_export
```

The command exports all user configurations of the node (both nodes of a duplex system) to the specified path.

Note: For the V9/V10 simplex to V11 standard duplex migration scenario, if the external application server is running UC V10, include the `-ucdbexp` option. For example:

```
# export8k -cfg <path to export> -ucdbexp
```

If the external applications server is at UC V10 or below this is not needed.

---

b) Ensure the process is completed successfully:

After approximately 10 minutes and upon successful completion, messages will be displayed ending with a message similar to:

```
[*] Export completed: <date>
```

The following file is created on each node: **<path to export>/patch/export.tar**.

Example location:

```
/repository/upload/toolkit_Db_export/patch/export.tar
```

c) After the successful export8k, the following prerequisites must be met before proceeding with the import or migration, as described in Section 9.6, “Importing the Source System Data to the Target System”:

- Save the data under <path to export> to an external server for safekeeping: Copy the entire export directory (e.g., toolkit_Db_export) along with all its subdirectories.

Attention: For duplex systems, perform this step for both nodes.

Attention: Do not modify or tamper with the exported data.

- When preparing for import or migration, ensure the same directory is restored under `/repository/upload/` on the target system, with identical contents on all nodes.
- For duplex systems, ensure the data is clearly separated per node to allow correct restoration during import. For example, the external server could employ **db_export_n1** and **db_export_n2** folders to hold the data.

9.5 Downloading and Installing the Migration Toolkit Software to the Target System

---

Attention: Always use the latest available version of the Migration Toolkit. The latest version works across all OSV releases. It is independent of the source or the target OSV release version.

As user *root*, verify that old Migration Toolkit software does not exist on the system. For a duplex system, execute the commands on both nodes:

```
# rpm -qa | grep -i UNSPmigration
```

If an old version of the migration toolkit software is found, then it should be removed with the following command:

```
# rpm -e --allmatches UNSPmigration
```

As user *root*, download to the /tmp directory and install the latest *UNSPmigration-<V#>.rpm* to the nodes (or node for a simplex system) with the command:

```
# cd /tmp          (directory where toolkit was copied to)
# rpm -ivh --replacefiles --replacepkgs UNSPmigration-<V#>.rpm
```

Example given;

```
# rpm -ivh --replacefiles --replacepkgs UNSPmigration-1.05-29.rpm
```

After some seconds, messages similar to the following will be displayed:

```
Preparing... ########################################## [100%]
1:UNSPmigration
########################################### [100%]
Checking for shared repository.
: : :
csv/simplex/
csv/simplex/12.00.02.ALL.15.csv
csv/simplex/V4.00.01.ALL.40.csv
csv/simplex/V5.00.01.ALL.11.csv
csv/simplex/V6.00.01.ALL.05.csv
csv/simplex/V7.00.01.ALL.07.csv
Valid node.cfg found. Invoking auto conversion.
Auto conversion successfull.
```

```
Converted node.cfg are found under /repository/config
Check /repository/config for converted node.cfg.
Migration tools installed successfully.
```

Similar messages appear when installing the Toolkit rpm on the second node of a duplex system.

9.6 Importing the Source System Data to the Target System

There are two command variants for restoring data:

- **import8k**
- **migrate8k**

The use of either **import8k** or **migrate8k** depends by the upgrade/migration procedure being performed. The applicable command variant is described within the corresponding upgrade or migration procedure.

Attention: By default, the source release passwords for system-defined OpenScape Voice accounts (for example, srx, and root) are imported to the target release.

Prerequisites for Import/Migration

Before starting the import or migration, ensure the following conditions are met:

1. The data exported in Section 9.4, “Exporting Source System Data”, must have been transferred back to the nodes (or to the single node in the case of a simplex system).
   - Ensure that this directory structure has been restored under `/repository/upload/` and is available on all nodes, with contents identical on all nodes.
   - Ensure the exported data were stored to an external server for safekeeping, as outlined in Section 9.4, “Exporting Source System Data”. The complete export directory (for example, toolkit_Db_export), including all subdirectories, must have been preserved without any modification.
2. For duplex systems, ensure that the data has been clearly separated per node on the external server and correctly restored so that each node receives its corresponding data, as described in Section 9.4, “Exporting Source System Data”.
3. For the V9/V10 simplex to V11 standard duplex migration scenario, ensure that the exported data from the Integrated Simplex system has been copied to node 2 of the target system under the same directory structure, with the file `node.cfg.primary` duplicated and renamed to `node.cfg.secondary`.

4. Ensure the target system is installed with the latest available patch set, unless otherwise specified in the Release Notes.

   - For integrated systems, ensure the application server is updated to the latest released DVD, Patch Set, or HotFix level.

9.6.1 Restore the data of the VM source

To restore the data of the source system the `toolkit` command with the 'cfg' option is used. The 'cfg' option is particularly useful for virtual systems where USB devices are not available.

When using the 'cfg' option, the data is imported from a local path specified by <path to import>.

Any questions concerning the *import* step should be addressed to your next level of support before proceeding.

For system upgrades or migrations:

- If the network configuration remains the same, follow step a).

  Note: This should apply to Section 8.7, “Upgrade of an OSV System Using Remote SW Upgrade”, on page 491.

- If the network configuration changes (with or without hardware migration), follow step b).

  a) **Import without network changes**:

  As user *root*, run the following command **from node 1 only**:

  ```
  # import8k -cfg <path to export>
  ```

  The export directory must not be placed under `/tmp`. It must be located under `/repository/upload/` on all nodes.

  Example:

  ```
  # import8k -cfg /repository/upload/toolkit_Db_export
  ```

  Go to step c.)

  b) **Migration with network changes** (e.g. Simplex -> Duplex):

  As user *root*, run the following command **from node 1 only**:

  Note: Ensure that **node.cfg** is correct and there are no cyclic or duplicate IP mappings before running the command.

  ```
  migrate8k -cfg <path to export> -config
  ```

– The export directory must be located under `/repository/upload/` (not under `/tmp`)

– The directory must exist on both nodes

– The content must be identical on both nodes

Example:

```
migrate8k -cfg /repository/upload/toolkit_Db_export -
config
```

Go to step c)

c) Ensure the process is completed successfully::

The time required to import the configuration varies based on the size of the imported database.

Messages similar to the following at the end of the list indicate a successful import:

```
prepare8k:Data imported successfully.
[*] Migrate completed: <date>
```

9.7 Remove the Migration Toolkit Software from the Target System

As user *root*, remove the Migration Toolkit software from the system. For a duplex system, execute the command on both nodes:

```
# rpm -e UNSPmigration
```

Messages similar to the following will be displayed:

```
Info: Checking rsync package : rsync-<version #>
Migration tools uninstalled successfully.
```

9.8 Configure the OpenScape Applications Server for Access to the Nodes

Configure the external OpenScape Applications server for access to the two nodes as follows:

1. Allow remote access for srx account on both nodes. Refer to Section 5.2.6.7, “Remote Access for srx Account”, on page 337 for instructions.
2. Log in (use the same password for the CMP of the previous release) to the Common Management Platform.

3. Select the **OpenScape Voice** tab**, List of Switches**, and select **Switches** from the drop down menu.

Note: It may take some time to display the switch list.

---

4. Refresh or Add the OpenScape Voice Server in the Applications server List of Switches.

   If you reached this step from one of the following sections, click **Edit**.

   - Section 8.7, “Upgrade of an OSV System Using Remote SW Upgrade”
   - Section 9.1.1, “Simplex to Simplex Migration”
   - Section 9.1.2, “Simplex to Standard Duplex Migration”
   - Section 9.1.2, “Simplex to Standard Duplex Migration”
   - Section 9.1.2, “Simplex to Standard Duplex Migration”
   - Section 9.1.3, “Standard Duplex to Standard Duplex Migration”

   In case the switch IP has been changed, it is required to restart the Applications services with:

   ```
   /etc/init.d/symphoniad restart
   ```

   For all other scenarios, click **Add**.

Attention: Removing an OpenScape Voice server from a Standard Duplex (Large or Small) UC Applications deployment will result in the loss of UC application data (e.g.; OpenScape Users/Resources).

---

5. Ensure that the required information is correct (e.g. srx password, Node 1 and 2 management IP addresses, and so on). Enter the correct information as necessary.

   If you need to change the switch IP, click on **Change IP Address** and enter the correct information.

6. Click **Test Connection**.

   This step might fail due to “srx user access violations”.

   If it does, ensure that remote access for Node 1 (or Node 2) is configured correctly and use the `pam_tally2` command to resolve the “srx user access violations” before you repeat the step.

   As user *root* on Node 1, query the *pam_tally2* count. For example:

   ```
   root@bocast4a:[~] #99
   # pam_tally2
   User srx        (1522)  has 25
   ```

If the *pam_tally2* reports 5 or more counts for user *srx*, reset the *pam_tally2* count for the *srx* user. For example:

```
root@bocast4a:[~] #100
# pam_tally2 --user srx --reset
User srx        (1522)  had 25
```

Query the *pam_tally2* count again to ensure there are no *pam_tally2* errors for the *srx* user. For example:

```
root@bocast4a:[~] #101
# pam_tally2
root@bocast4a:[~] #102
```

7. If the above test is successful, click **Save** at the bottom of the form.

Attention: Saving the switch configuration may not be successful the first time with a `Configuration Failed` message given due to install key. If this happens, close the window of the error message and click **Save** again. The switch configuration will be successfully saved the second time.

---

8. If the migration procedure involved OSV IP subnet address changes that included the Signaling Managers (the CSTA SM in particular);

   a) Navigate the CMP UI to **Configuration>OpenScape Voice>Administration>Signaling Management>CSTA**. Here the OSV CSTA Signaling IPs should be presented in the **Signaling Manager** tab of the **CSTA Settings** window. These IPs will be verified against the IPs listed in step 8b).

   b) Next, the user should navigate to **Configuration>Unified Communications>Configuration>Connections>OS Voice**. Verify the **OpenScape Voice Connection** IPs match the IPs listed in step 8a). If necessary, edit the **OpenScape Voice Connection** IPs to match those of step 8a).

   c) The user should restart the Applications services with:
   # /etc/init.d/symphoniad restart

9.9 Create the Node.cfg for the Target System (Source system = Low Cost)

Attention: This procedure is intended for the Low Cost to Standard Duplex Migration and Low Cost Native Hardware to Virtual Integrated Simplex Migration.

Any other migrations should employ Section 9.2, “Create the Node.cfg for the Target System”, on page 542.

Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade” should employ Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457.

Note: If ‘route operations’ message windows are presented during the Node.cfg creation, select the **OK** button. For more information regarding the Source Based Routing feature, refer to Chapter 7, “Overview of Upgrades and Migrations to OpenScape Voice V11”.

For duplex systems, if an OpenScape Voice system outage cannot be tolerated during the upgrade, then the Outage Free toolkit upgrade will need to be performed. The Outage Free toolkit upgrade method is detailed in Section 8.6, “Upgrade of an OSV Duplex System Using Live Upgrade”, on page 483.

Attention: For the Low Cost to Standard Duplex Migration and Low Cost Native Hardware to Virtual Integrated Simplex Migration scenarios, it is recommended that the user create the node.cfg from scratch using the NCPE. Specify the new IP configuration (if necessary) using the appropriate tabs. The node.cfg collected in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 may be used as a reference for external server IP addresses (e.g., Name (DNS), NTP, CSTA, SNMP, License, Billing, SNMP and Misc. Host servers.)

If it is decided to create the target release node.cfg from scratch (while employing the node.cfg collected in Section 8.3.1.2, as a template); steps 1, 3a), 3b) and 3c) do not apply in this case. Open the node.cfg, step 2), and proceed to step 3d). Before sure to employ the latest target release NCPE.

Attention: Read Section 9.10, “Restrictions for Migrations In Which The Network Configuration Is Changed”, on page 559 before proceeding. A link back to this section will be provided.

Use the latest version of the OffLineWizard software indicated in the release notes for the target release.

1. Transfer the node_<node-name>.cfg file generated in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 to a Windows/Linux machine that can run the OfflineWizard.

   Note: If necessary, refer to the OpenScape Voice base software release note on G-DMS for the link to SWS to download the Installation Wizard zip file.

   Recommended practices for file transfer and burning of CD/DVD media;
   1. If a checksum, md5sum or sha file is delivered with OpenScape software it is a good practice to compare the calculated value of the downloaded data against the applicable file to ensure the integrity of the download. **If necessary, third party software can be used to calculate these values.**
   2. When burning a file to a CD/DVD media use a lower burning speed (i.e.; 4x).
   3. Use the 'verify' option of the burning application to ensure data integrity after the DVD burning is complete.

   Unzip the downloaded file. Now there should be a parent directory named 'ncpe-OfflineWizard-<version_number>'. Change to the bin path located one level below 'ncpe-OfflineWizard-<version_number>'.

2. Start the OffLineWizard.

   a) Change directory to ncpe-OfflineWizard-<version_number>'\bin path.

      For Windows systems; open (double click) the file named ifgui.cmd.

      For Linux systems; open the file named ifgui.

   b) Select **Install** on the first screen, click **Next**, then select **Expert Mode** on the next screen.

      Note: For Linux users, if needed, export the DISPLAY of the output to your PC by entering "export DISPLAY=<IP address>:0", where the IP address of the destination of the DISPLAY is to be sent is used. This step is done as the root user.

Note: Some node.cfg files may report 'Invalid Data' related to IPV6 addressing. As a general rule; If IPV6 addressing is not needed, remove all IPV6 addresses. If IPV6 addressing is needed, all IPV6 address parameters must be populated.

IPV6 address parameters are located at:

- IP Configuration 1/5 in the Signaling tab
- IP Configuration 2/5 IPv6 Configuration
- IP Configuration 5/5 Node 1 and Node 2 IPv6 Routes tables

3. From the NCPE GUI:

   a) Under "**File**", open the file node_<node-name>.cfg (e.g., node_linux1.cfg) that was created in Section 8.3.1.2, “Download and Install the Migration Toolkit to Source Release and Generate Node.cfg File of the Target Release”, on page 457 and generate the node.cfg for the target release.

   b) Answer "**Yes**" to question "The file node_<node-name>.cfg is from "source release" (example given; V8). Do you want to convert it to "target release?" (example given is in V9)

   Answer '**OK**' to Messages indicating 'route operations' have been performed.

   c) Enter "**OK**" and the click "**OK**" to the Warning window to accept new parameters added to the node.cfg.

   d) Click the 'Expert Mode' button, under "Configuration and Hardware (1/1)" **make sure that the "Installation mode" is set to "normal".** As appropriate, specify all new parameters for the new configuration of the target system.

4. Follow the appropriate steps to complete your node.cfg (based on your migration procedure):

   a) **For the Low Cost to Standard Duplex Migration**: refer to Section 2.6, “Creating a Node.cfg File”, on page 50, and execute Section 2.6 through Section 2.6.9, step 7 on page 65. Following step 7, there will be a link back to step 6 in the "Low Cost to Standard Duplex Migration" section.

   b) **For the Low Cost Native Hardware to Virtual Integrated Simplex Migration**: Refer to Section 2.6, “Creating a Node.cfg File”, on page 50 for further details regarding the node.cfg creation. Following Section 2.6.9 on page 64, step 6 on page 64, there will be a link back to step 8 in the "Low Cost Native Hardware to Virtual Integrated Simplex Migration" section.

9.10 Restrictions for Migrations In Which The Network Configuration Is Changed

Attention: Any questions should be addressed to the next level of support.

This section list restrictions for migrations (with or without a hardware migration) in which the network configuration is changed. This text applies to these migrations;

- Section 9.1.2, “Simplex to Standard Duplex Migration”
- Section 9.1.3, “Standard Duplex to Standard Duplex Migration”
- Section 9.2, “Create the Node.cfg for the Target System”

1. Expansion of IP addresses or Ethernet circuits is not supported for migration. It is supported to preserve or even reduce the IP addresses or Ethernet circuits. This means that the number of network interfaces in node.cfg of the target system cannot be greater than the ones in the node.cfg of the source system. For example:

   - If 2 interfaces were configured in the source system node.cfg we can configure 2 or 1 interfaces in the node.cfg of the target system BUT NOT 3

2. Using pre-migration IP addresses, node names, domain names or search domain for new functions post-migration **IS NOT ALLOWED**. It is allowed to preserve the node names or an IP address as part of the migration. One example of this restriction is a co-located OSV deployment that migrates to a geo-separated deployment. The node_1_ip of the source system may not be used as the node_2_ip of the target system. The respective node names may be preserved.

   Source release co-located node.cfg:

   node_1_name: grt00n1
   node_1_ip: 10.0.2.10

   node_2_name: grt00n2
   node_2_ip: 10.0.2.30

   "**Wrong**" target release geo-separated node.cfg: the **node_1_ip** cannot be reused as the **node_2_ip**.

   node_1_name: grt00n1 ← **The node_1_name can be preserved.**
   node_1_ip: 10.0.3.10

   node_2_name: grt00n2 ← **The node_2_name can be preserved.**
   node_2_ip: 10.0.2.10 ← ***The re-use of the node_1_ip as the node_2_ip is not allowed.***

   "**Correct**" target release geo-separated node.cfg:

   node_1_name: grt00n1 ← **The node_1_name can be preserved.**
   node_1_ip: 10.0.2.10 ← **The node_1_ip can be preserved.**

node_2_name: grt00n2 ← **The node_2_ name can be preserved.**
node_2_ip: 10.0. 3.10 ← **The node_2_ip is not used in the source release node.cfg.**

3. **Do not change IPs of External servers in the target node.cfg**

   Do not change IPs of external servers in the target node.cfg (e.g.; SNMP servers, CMP / Assistant). The recommended method is to perform the migration and, after the successful migration, execute an EZIP to change the IPs of external applications servers.

   If it is necessary to change the external server IPs the EZIP feature can be employed to make the changes after the successful migration is complete. For more information regarding EZIP, Appendix 13, “Updating the Node.cfg File (Also Known as EZIP)”.

4. In case of co-located OSV deployment that migrates to a geo-separated deployment, you must change all IPs of both node1 and node2 of the target system to be different than those of the source system.

   This means that node1 target IPs should not be the same as either node1 or node2 source IPs and node2 target IPs again should not be the same as either node1 or node2 source IPs.

   Note: Changing the IPs by even one digit will suffice

   When you cannot change all IPs, change the following four node.cfg parameters in node1 and node2 of the target system to be different from the equivalent ones in the source system for the migration to be successful:

   – lsm_node_1_ip and lsm_node_2_ip
   – default_router and default_router_2
   – signaling_1_gateway and signaling_2_gateway
   – admin_1_gateway and admin_2_gateway

   and any other parameters that you can.

Note: Follow this link to return to step 1 on page 544 of Section 9.2, “Create the Node.cfg for the Target System”.

Note: Follow this link to return to step 1 on page 558 of Section 9.9, “Create the Node.cfg for the Target System (Source system = Low Cost)”.

9.11 Simplex System *response.cfg.primary* File Creation

This section ONLY applies to Simplex OSV upgrade or migration procedures. You should have arrived here from one of the following Simplex upgrade or migration task lists tables:

- Section 8.5, Table 19, step 7
- Section 8.7.2, Table 21, step 7
- Section 9.1.1, Table 22, step 8

Create the *response.cfg.primary* file for an Integrated Simplex system using one of the following methods:

- **Method 1:** This method builds the response file from file **responsefile.txt** that exists on the source system. For details, refer to Section 9.11.1

  This method is shorter and less complex than method 2.

- **Method 2:** This method builds the response file from scratch using a template. For details, refer to Section 9.11.2

9.11.1 Building Simplex Response File from Older Response File

The response file to be created for the target system is similar to the response file found on the source system at:

/enterprise/servicetools/install/conf/responsefile.txt

1. Copy the above *responsefile.txt* file to a local PC for editing.
2. Rename the copied file *responsefile.txt* on the local PC to *response.cfg.primary.*
3. In file *response.cfg.primary,* parameters SI_SYMPHONIA_ADMIN_PASSWORD and SI_DB_LOGON_PASSWORD are encrypted and must be edited and changed to clear text (i.e., unencrypted).

   - Replace the encrypted password string for both of the above passwords with the “normal” password string (i.e., unencrypted).

     Contact your next level of support if you don't know the unencrypted password string for the above two password parameters.

4. If you ran an earlier import8k or migrate8k with -noapps options and chose to preserve the applications data, then set **SI_FW_DB_MIGRATION=true** in response file *response.cfg.primary*.

Note: The options *-noapps* and *-noappsindb* are no longer supported.

---

5. Replace the IP addresses you find inside *response.cfg.primary* with the Admin IP address of the OSV node. This is the nafo0 IP address listed for node 1 in the target release node.cfg file that was created when the Migration Toolkit was installed.

   Note: To determine the nafo0 IP address of the node, refer to Section 9.11.3, “How to Determine Admin IP Address of Node 1 (nafo0 IP)”, on page 564.

   ---

6. Go to the bottom of Section 9.11.3, “How to Determine Admin IP Address of Node 1 (nafo0 IP)”, on page 564 for links back to your task list.

9.11.2 Building Simplex Response File from Template

If you choose to use a template, ensure that you know the following values that were used in the source system:

- The symphonia admin password (SI_SYMPHONIA_ADMIN_PASSWORD)
- The database logon password (SI_DB_LOGON_PASSWORD)
- The community name (SI_COMMUNITY_NAME)
- The Admin IP address of the node. This is the nafo0 IP address listed for node 1 in the target release node.cfg. The instructions for determining the Admin IP address are provided in the following procedure.

Contact your next level of support if you don't know the values of the parameters above that were used on the source system.

1. For a guide to help build the response file from a template, refer to Section Section 5.2.3.2, “Response File for Integrated Deployments”, on page 302.
2. In the response file */root/knut.responsefile.txt* that was created, edit the file as follows:
   - Replace the value of field SI_COMMUNITY_NAME with the value used in the source system.
   - Replace the value of field SI_SYMPHONIA_ADMIN_PASSWORD with the value used in the source system. However, the value that you will enter should be the **unencrypted** "normal" password string.

- Replace the value of field SI_DB_LOGON_PASSWORD with the value used in the source system. However, the value that you will enter should be the **unencrypted** "normal" password string.

3. Make sure to populate the correct IP addresses for IP related fields in the template. The IP address that should be used is the Admin IP address of the node. This is the nafo0 IP address listed for node 1 in the target release node.cfg that was created when the Migration Toolkit was installed.

   For determining the value of the Admin IP refer to Section 9.11.3, “How to Determine Admin IP Address of Node 1 (nafo0 IP)”, on page 564.

4. If you ran an earlier import8k or migrate8k with -noapps options and chose to preserve the application data, then set field **SI_FW_DB_MIGRATION=true** in the response file.

5. After having created the response file */root/knut.responsefile.txt*, copy it to a local PC. Rename the copied file on the local PC to *response.cfg.primary.*

6. Go to the bottom of Section 9.11.3, “How to Determine Admin IP Address of Node 1 (nafo0 IP)”, on page 564 for links back to your task list.

9.11.3 How to Determine Admin IP Address of Node 1 (nafo0 IP)

The admin IP address is the IP address assigned to node 1 of nafo0 in the target release node.cfg file that was created when the Migration Toolkit was installed.

In the following example, 1.2.3.6 is the nafo0 node 1 IP (this example is an excerpt of the nafo configuration from a Low Cost node.cfg file):

```
# id     nafo_grp   itf1  itf2  node_1  node_2   netmask          subnet
nafo0:  nafo_alias  eth0  eth0  1.2.3.6  0.0.0.0  255.255.255.240  1.2.3.0  .....
nafo1:  nafo_udp    eth0  eth0  1.2.3.4  0.0.0.0  255.255.255.240  1.2.3.0  .....
nafo2:  nafo_bms    eth0  eth0  1.2.3.7  0.0.0.0  255.255.255.240  1.2.3.0  .....
```

If you arrived here from Section 8.5, Table 19, return to step 7 on page 642.

If you arrived here from Section 8.7.2, Table 21, return to step 7 on page 554.

If you arrived here from Section 9.1.1, Table 22, return to step 8.

9.12 Customization of Nodes

9.12.1 Customizing Node 1

9.12.1.1 Log In to Node 1

Note that after the target release image installation the OpenScape Voice server userids and passwords are set to the target release configuration.

The OpenScape Voice V11 default users and passwords are:

Type	User	Password
Console	root	T@R63dis
Console	srx	2GwN!gb4
SFTP	cdr	MNY9$dta”
SSH	sysad	1clENtk=
SSH	superad	BF0bpt@x
SSH	hipatham	kH3!fd3a
SSH	hipathcol	jO3(fdqA
SSH	secad	$ECur8t.
SSH	dbad	d8$ECur.
SSH	webad	!WE8saf. **(for Simplex configurations only)**

Table 26 OpenScape Voice V11 default users and passwords

Users "sysad", "superad", "secad", "dbad" and "webad" have 90 day expiry limits set on their passwords. Unless restricted by the /etc/security/access.conf file, all users have access to the OSV via the console also.

Note: If your OpenScape Voice system was Upgraded or migrated to OpenScape Voice V11, then you have maintained the expiry data of the source release. This means the "sysad", "superad". "secad" and "dbad" userid passwords will never expire. For password management advice please refer to Section 17.2.2, “Password Management”, on page 617.

The following table provides the default passwords for Solid Users.

User	Password
dba	dba
rtp	RTP_USER
sym	sym **(for Simplex configurations only)**

Table 27 Default Passwords for Solid Users

1. Log in to Node 1 as user *sysad* using one of the following:
   – Remote shell (SSH)

– Remote access "KVM (Keyboard Video Mouse)" via IMM (Intel Management Module) or iRMC. The user-id/password for remote access to the IMM or iRMC is reset to the default values: userid=USERID, password=PASSW0RD (0 in PASSW0RD is zero, not the letter O).

– Console

Note that the default password of user *sysad* is '`1clENtk=`'.

2. After the first login, you have to change the password. The new password should have at least 8 characters and mixed cases (for example something like `!Q2w3e4r)`.

9.12.1.2 Customize Node 1

Prerequisites:

– One license file for the node 1 has been acquired

– Adequate administrative permissions

Follow the steps below:

1. Determine the appropriate license file for node 1 of the OSV system.

Note: The license file is used to activate the associated licenses and thus the products and their features.

2. Log in to node 1 as srx user in order to execute the following steps.
3. Transfer the node 1 license file to `path/opt/unisphere/srx3000/cla_inst/import/` of node 1.
4. Execute the following command: `/unisphere/srx3000/callp/bin/import_license.sh`

Note: For deployments were OSMO clients are configured, and the new license type *Dynamic ONS* is included at the V11 license file, activating a V11 license requires an image upgrade process. In such cases, *import_license.sh* is not supported.

The license management verifies the signature of the license file against each node's Locking ID.

5. Continue with the appropriate upgrade procedure:

• If you arrived at this section from the Installation checklist and this is a simplex system return to Section 2.2.4, "OpenScape Voice Installation Checklist", 23 on page 35.

- If you arrived here from Table 23 return to step 14.
- If you arrived at this section from the Installation checklist and this is a duplex system, proceed to Section 9.12.2.1, “Log In to Node 2”, on page 568 and then to Section 9.12.2.2, “Customize Node 2”, on page 570.
- If you arrived here from Table 24, return to step 18 of Table 24.
- If you arrived here from Table 25, return to step 18 of Table 25.

9.12.2 Customizing Node 2

9.12.2.1 Log In to Node 2

Note that after the target release image installation the OpenScape Voice server userids and passwords are set to the target release configuration.

The OpenScape Voice V11 default users and passwords are:

Type	User	Password
Console	root	T@R63dis
Console	srx	2GwN!gb4
SFTP	cdr	MNY9$dta”
SSH	sysad	1clENtk=
SSH	superad	BF0bpt@x
SSH	hipatham	kH3!fd3a
SSH	hipathcol	jO3(fdqA
SSH	secad	$ECur8t.
SSH	dbad	d8$ECur.
SSH	webad	!WE8saf. **(for Simplex configurations only)**

Table 28 OpenScape Voice V11 default users and passwords

Users "sysad", "superad", "secad", "dbad" and "webad" have 90 day expiry limits set on their passwords. Unless restricted by the /etc/security/access.conf file, all users have access to the OSV via the console also.

Note: If your OpenScape Voice system was Upgraded or migrated to OpenScape Voice V11, then you have maintained the expiry data of the source release. This means that the "sysad", "superad". "secad" and "dbad" userid passwords will never expire. For password management advice, please refer to Section 17.2.2, “Password Management”, on page 617.

The following table provides the default passwords for Solid Users.

User	Password
dba	dba
rtp	RTP_USER
sym	sym **(for Simplex configurations only)**

Table 29 Default Passwords for Solid Users

1. Log in to Node 2 as user `sysad` using one of the following:
   – Remote shell (SSH)

– Remote access "KVM (Keyboard Video Mouse)" via IMM (Intel Management Module) or iRMC. The user-id/password for remote access to the IMM or iRMC is reset to the default values: userid=USERID, password=PASSW0RD (0 in PASSW0RD is zero, not the letter O).

– Console

The default password for user *sysad* is '`1clENtk=`'.

2. After the first login, you have to change the password. The new password should have at least 8 characters and mixed cases (for example something like `!Q2w3e4r`).

9.12.2.2 Customize Node 2

Prerequisites:

– One license file for the node 2 has been acquired

– Adequate administrative permissions

Follow the steps below:

1. Determine the appropriate license file for node 2 of the OSV system.

Note: The license file is used to activate the associated licenses and thus the products and their features.

---

2. Log in to node 2 as srx user in order to execute the following steps.
3. Transfer the node 2 license file to path `/opt/unisphere/srx3000/cla_inst/import/` of node 2.
4. Execute the following command: `/unisphere/srx3000/callp/bin/import_license.sh`

Note: For deployments were OSMO clients are configured, and the new license type *Dynamic ONS* is included at the V11 license file, activating a V11 license requires an image upgrade process. In such cases, *import_license.sh* is not supported.

The license management verifies the signature of the license file against each node's Locking ID.

5. Continue with the appropriate upgrade procedure:

• If you arrived at this section from the Installation checklist (via Section 9.12.1.2) return to the Section 2.2.4, "OpenScape Voice Installation Checklist", step 23 on page 35.

- If you arrived here from Table 24, return to step 21.
- If you arrived here from Table 25, return to step 20.

10 Basic Traffic Tool

The Basic Traffic Tool (BTT) is a performance monitoring tool that helps analyze performance data for OpenScape Voice. The application has two software components: server and client.

- The server collects data into a csv file every 15 minutes. It runs under a cron job.
- The client, a Windows based JAVA application generates graphical and numerical data displays using the data in the csv file. An authorized user opens an SFTP shell and manually transfers the csv file to the PC where the BTT client is installed.

10.1 Installation (Server)

The BTT Server is installed automatically during the installation of the OpenScape Voice software and should be available immediately.

The file where the data is collected (/var/tmp/data.csv) is also created automatically (approximately 15 minutes after installation of the OpenScape Voice software). After initial creation the file is updated every 15 minutes.

10.2 Installing (Client)

Install the client as follows:

1. From SWS, copy **btt<nnnn>.zip** (where <nnnn> is the version for BTT, for example: Version 1.07 is *btt0107.zip*) to a directory on your PC.
2. Extract the contents of package **btt<nnnn>.zip** into a directory on the PC.

10.3 Using the Tool

Use the BTT as follows:

1. Open an SFTP shell and connect to the OpenScape Voice system.
2. Copy the file /var/tmp/data.csv to a folder on the PC where the BTT Client is installed.
3. Start the traffic tool by executing the batch file **pmStats.bat**.
4. You are prompted to enter the location of the data file (for example, C:/data.csv).

5. Enter a start date and an end date. The default end date is the current day and time; the default start date is five days prior to that.

   If data exists for the selected period, it will immediately be displayed.

   If the input start or end date is invalid, valid data within the input range is displayed if it is available.

10.3.1 Graphical and Numerical Data Screens

Graphical and numerical data is visible when the user clicks on one of the six tabs. Table 30 shows the four screens that provide graphical data. Table 31 shows the two screens that display numerical data.

Screen	Information Provided
Call attempts in selected period	Displays the call attempts within the user-selected time period.
Call attempts today	Displays the call attempts for the current day (if available).
Traffic load in selected period	Displays the traffic load for the selected period.
Traffic load today	Displays the traffic load for the current day (if available).

Table 30 Graphical Data Presented by the Basic Traffic Tool

Screen	Information Provided
Numerical data in selected period	Displays data for the user-selected period
Numerical data today	Displays data for the current day (if available).

Table 31 Numerical Data Presented by the Basic Traffic Tool

Numerical data is displayed for the following fields:

- Number of calls
- Number of incoming calls
- Number of outgoing calls
- Unsuccessful call attempts
- Busy hour call attempts (BHCA)

10.3.2 Menu Structure

Table 32 describes the various menu options.

Menu	Description
File	• A **new report** may be generated from the File menu without closing the application. When a new report is generated, the existing graphs and text areas are removed and new data is displayed. The user is prompted to enter the data file location. • The **print this tab sheet** permits output from any of the six screens to be printed.
Edit	**Copy numerical data** allows data from the text areas to be copied to another file, but data cannot be pasted into the text areas because they can not be edited. Graphical data cannot be saved to a file nor can it be copied or pasted.
Help	The **version number** of the application is available.

Table 32 Basic Traffic Tool Menu Structure

10.4 Feature Considerations

The Basic Traffic Tool is not a node failover-safe tool. It is installed on the primary node of the cluster and will not failover to the secondary node upon primary node failover.

11 Example Install_Time.log

The *install_time.log* (located in the */log* directory) holds installation execution times. Studying the contents of this log file can provide another simple verification of the installation. The execution times recorded in this file should be consistent for all installations of Node1 (master node). Node2 will have some variations due to timing dependencies. An example of the *install_time.log* follows.

```
start S96configure:     Wed Dec 11 14:00:37 EST 2002
stop  S96configure:     Wed Dec 11 18:39:43 EST 2002
start S97provision:     Wed Dec 11 18:39:43 EST 2002
stop  S97provision:     Wed Dec 11 18:41:22 EST 2002
start S98buildplus:     Wed Dec 11 18:41:22 EST 2002
stop  S98buildplus:     Wed Dec 11 18:54:01 EST 2002
```

12 Changing NTP Server or DNS Configurations

Changing the NTP server or DNS configuration is done by using the Update option of the EZIP tool as described in Appendix 13. The changes to NTP and DNS parameters will not cause a system outage.

When opening the EZIP GUI in the Update option, the parameter fields that are related to NTP and DNS have a green background color. Parameter fields with green background color indicate that the modification to these fields will neither cause a reboot of the nodes nor a system outage.

The EZIP tool updates all the files and packet filter rules that relate to the NTP and DNS parameters and IP addresses.

13 Updating the Node.cfg File (Also Known as EZIP)

The EZIP procedure can be performed on a simplex or a duplex system. On a simplex system, the node has to be at RTP state 4. In a duplex system, both nodes have to be at RTP state 4. The procedure should be executed during a low-traffic period.

The EZIP procedure may cause an outage depending on the background color of the parameter field(s) being modified. There are two categories as follows:

1. No outage - Green background

   Modifying parameter fields with a green background color would not cause an outage. Examples of this category:

   - Modifying NTP servers IP addresses
   - Modifying DNS servers IP addresses and configuration parameters
   - Modifying Default router IP address
   - Modifying Stand Alone Service Enabled parameter
   - Modifying Survival Authority IP address
   - Modifying Super User IP address (the offboard CMP IP Address used by a duplex OSV)
   - Modifying RSA/IMM/iRMC IP address
   - Adding, modifying or deleting static routes
   - Adding, modifying or deleting SNMP server IP address and port
   - Adding, modifying or deleting license server IP address and port

---

Note: EZIP changes of the parameters in Category 1 may also be triggered from the CMP. Refer to Section 13.2.1, “EZIP Method Using the CMP”, on page 583 for details.

---

2. Outage with reboot - White background

   Modifying parameter fields with a white background color would cause an outage and the nodes reboot. Most of the parameters fall into this category.

Note: When changing parameters from more than one category, the handling of the highest category takes precedence. For example, when changing a parameter from category 1 (with green background) and a parameter from category 2 (white background), the action of category 2 prevails meaning the system will have an outage and the node(s) reboot.

If EZIP is used to change the number of OSV IP subnets or to change/merge/unmerge IP addresses, the craft must verify any packet filter rules generated by the customer. These packet filtering rules must be reviewed to ensure they are appropriate for the new configuration. OpenScape Voice default packet filtering rules generated as a result of an EZIP update do not require review.

Caution: Changing the node.cfg can have unintended consequences and should be performed with care. Before beginning, ensure that an up-to-date file system backup is available and be prepared to do a file system restore in case of any problems.

The Installation Framework Update (EZIP) maintains the Source Based Routes configuration.

Also, save the /etc/hosts file of each node to a safe location. After you complete the update verify that any user-added entries to the /etc/hosts file were not removed during the update (or restore). If any user-added entries were removed, edit the /etc/hosts file and add the missing entries as the last lines in the file (edit the file in both nodes for redundant systems). An example hosts file edit is shown below.

A Data Collection procedure for EZIP issues has been added as the last section of this appendix. If a problem occurs during the EZIP execution your next level of support must be contacted first, the integrity of the OSV system verified and then data collection, if necessary, can be performed.

13.1 Verify the System Health before EZIP Configuration Change

It is a good practice to verify the system Health before an EZIP configuration change. Use the CMP to access the Node Health function (RapidStat) as described below.

1. From the CMP, navigate to **Maintenance > Inventory > Nodes and Applications> Nodes**
2. In the Nodes window frame, click on the node name of the system in which the EZIP will be executed. For a duplex system, click the name of one of the two nodes. The Dashboard for the node will be presented.
3. In the Actions section of the Dashboard, click the OSV Rapidstat Start button. The Node(s) Health window is presented. The OSV node(s) are checked for various items and the window is populated with data. For a Duplex OSV system, the checks are made on one node and then performed on the other node similar to running RapidStat from the node.

   Please be patient as the checks take a few minutes.

After the Node Health check completes, it is expected that no warnings or error messages should be present. **Do NOT proceed until it is resolved that the warnings or errors will not affect the EZIP function. Any questions regarding warnings or error messages should be addressed to your next level of support.**

13.2 EZIP Methods

13.2.1 EZIP Method Using the CMP

This method can be used for changing OSV parameters from category 1 (EZIP without outage). For changing other OSV parameters from category 2, the traditional NCPE Tool in Update mode is used. For details, refer to Section 13.2.2, “EZIP Method Using the NCPE Tool in Update Mode”, on page 584.

To perform EZIP without outage from the CMP for changing OSV parameters in category 1, do the following:

- Login onto CMP
- Click **Configuration** tab
- Click **OpenScape Voice**
- Select your switch
- Click **Administration** > **General Settings** > **EZIP**
- Edit, add or delete the desired parameter(s) of Category 1. Click **Save** to start EZIP.

Please ensure that the values entered for node.cfg are only IPs (where applicable) and under no circumstances FQDNs, as FQDNs are not officially supported by OpenScape Voice IDS service.

Forbidden from being FQDNs CMP fields
EZIP Settings - General - "NTP Server 1"
EZIP Settings - General - "NTP Server 2"
EZIP Settings - General - "Superuser IP"
EZIP Settings - General - "Name Server" - "IP 1"
EZIP Settings - General - "Name Server" - "IP 2"
EZIP Settings - General - "Name Server" - "IP 3"
EZIP Settings - Servers - "SNMP" - "Add/Edit" - "Destination IP"
EZIP Settings - Servers - "Miscellaneous hosts" - "Add" - "Host IP"

CMP fields that must be forbidden from being FQDNs

See also in Chapter 2, “Creating a Node.cfg File” and Appendix 13.2.2, “EZIP Method Using the NCPE Tool in Update Mode” for startCli and NCPE fields respectively, that must be forbidden from being FQDNs.

13.2.2 EZIP Method Using the NCPE Tool in Update Mode

13.2.2.1 Preparation

A PC that has the NCPE software installed and a network connection (one of the SNMP servers listed in "Section 4: IP Security" of the node.cfg file) can be used for the Installation Framework (IFgui) update.

Always verify that the IP address of the PC hosting the IFgui is contained in the node(s) */etc/hosts* file before each IFgui update. If the */etc/hosts* file does not contain the IP address of the machine hosting the IFgui, edit the hosts file by adding the IFgui host PC IP address as the last line of the hosts file. The hosts file should be edited on each node. As an example, IP address 10.235.200.29 was added to the hosts file:

```
10.235.54.10      rtp_com0_eth6
10.235.54.30      rtp_com1_eth6
########################################
# Please add new hosts under this line #
########################################
10.235.200.230    nmcsnmptrap
10.235.200.29     host_pc
```

This update will allow the console terminal window on the IFgui host PC to log activity as the IFgui update (or restore) proceeds. The console terminal window should not be closed during the IFgui update or restore as it can not be re-established. The console terminal window will close when the Installation Framework is closed (steps 8 through 10 on page 587).

Note: For integrated systems only: Before you start the update, open a console terminal and as user *root* stop the onboard assistant with the command:

```
# /etc/init.d/symphoniad stop
```

13.2.2.2 Update the node.cfg file for the OpenScape Voice system

---

Attention: The following updates will the impact the ALI licensing of a VM;

If your Virtual Machine is deployed with the Advanced Locking Identification (ALI), changing any of the following node.cfg parameters will necessitate the generation of a new license for the node;

- Gateway Address
- Host Name
- Host IP address

Changing the Primary DNS IP will necessitate the generation of a new license for each node of a cluster (because the Primary DNS IP is the same for each node).

Refer to Section 20.2, “Virtual OSV Server”, on page 707 for an overview of the ALI. There is a link back to this page at the end of Appendix 20.

These rules apply to each node! Apply the license file as soon as possible after the IFgui update completes!

Update the node.cfg file for the OpenScape Voice system as follows:

> **Note:** Performing this procedure will generally cause an outage and should only be done during a low-traffic period. The exception is when changing parameters that have a green background color (e.g., NTP, DNS, etc). Changes to such parameters will not cause an outage.

1. In the directory where the Installation Wizard/NCPE software is stored, double-click **ifgui.cmd** for a Windows system or **ifgui** for a Linux system.

   The Installation Framework options screen is displayed.

2. In the Installation Framework options screen, select **Update** and click **Next**.

   The Installation Framework - Update Mode screen appears and displays Section 1: System Menu

3. In Section 1: System Menu window, enter the requested data:

Username:	Type the name of a predefined RtpAdminCli user (for example: *sysad*, *sysop1* and so on). Do not use *root* or *srx*. The users *root* and *srx* are not typically allowed remote access to the OpenScape Voice server.
Password:	Type the password for the user entered in the Username field.
root Pass:	Type the password for the *root* user.

Node 1 IP:	Insert the IP address of Node1.
Port	Port 22 is mandatory for the OSV nodes, but for the OSEE nodes it depends on the current port access configurations

Click **Next**.

Section 2: System Configuration window is displayed.

4. In Section 2: System Configuration window, click **Edit System Configuration.** Click **OK** to any messages. The NCPE opens in Expert Mode and displays the current configuration of the OpenScape Voice system.
5. Make your changes to the current configuration. Some parameter fields are disabled and cannot be changed.

Note: For parameter descriptions, please refer to Section 2.6, “Creating a Node.cfg File”, on page 50. Remember that some parameter fields are disabled and cannot be changed. The following parameters are NOT described in Section 2.6, “Creating a Node.cfg File”;

Redundancy:
Enter the Location Node 1 (CLLI) value
Enter the Location Node 2 (CLLI) value

The CLLI value is a free-form character string that can be used to document the location of each OSV node. This string is not used by the OpenScape Voice software. Example CLLI strings;

Munich (for node 1)
Athens (for node 2)
BocaRatonFlOSV1
Boca_Raton_Fl_OSV1
OrosOlymposOSV2
Oros_Olympos_OSV2

Misc. Hosts: Miscellaneous host IP addresses that may require access to the OpenScape Voice (i.e.; the IP address of the machine that will access the Voice server to perform the IFgui update (EZIP) function).

---

6. After you are done, save your changes and exit the NCPE tool.
   Section 2: System Configuration window is displayed.
7. In Section 2: System Configuration window, click **Apply New Configuration**. Click **Yes** to confirm that you want to proceed. A log console is opened that shows the process of the update.

   After the update is complete, a message is shown certifying that all of the changes were made.

8. Click **Back** to return to Section 1: System Menu screen.
9. In Section 1: System Menu screen, click **Finish** and then click **Yes**. The Installation Framework options screen is displayed.
10. In the Installation Framework options screen, click **Finish.**
11. It is a good practice to verify the system Health after an EZIP configuration change. To access the Node Health function (RapidStat), refer to Section 13.1, “Verify the System Health before EZIP Configuration Change”.
12. For integrated systems only: Open a console terminal and as user *root* enter the following commands:

    ```
    # /etc/init.d/symphoniad stop
    # /etc/init.d/openfire stop
    # /enterprise/servicetools/install/bin/changeSFWip.sh -CPFv -c
    change
    # /etc/init.d/symphoniad start
    # /etc/init.d/openfire start
    ```

    Login to the CMP, navigate to **OpenScape Voice** tab-> **General->List of Switches** -> **Switches**; select the checkbox for the updated Voice Server system. Select the Refresh button. The Voice server cluster information will be updated on the List of Switches page.
13. For an external applications server (standard duplex):
    - For changes to the OpenScape Voice server administration subnet IP address scheme that would change the node 1 and node 2 administration IP addresses;
      a) Navigate to **OpenScape Voice** tab-> **General->List of Switches** -> **Switches**, select the checkbox for the updated Voice Server system.
      b) Select the **`Edit`** button.
      A window titled **Edit Switch:<ClusterName>** is presented.
      c) Select the **Change IP address** button.
      A window titled **<ClusterName>-Connection Settings** is presented.
      d) Update the IP address of the node 1.
      e) Select the **Test Connection** button.
      f) After a successful connection test, select the **Save** button.
      The window titled **Edit Switch:<ClusterName>** is presented. The IP address values of node 1 and node 2 will be updated.
      g) Select the **Save** button.
      The List of Switches will be presented with the updated IP addresses of node 1 and node 2.
    - For changes to the OpenScape Voice server cluster or node names;

a) Navigate to **OpenScape Voice** tab -> **General** -> **List of Switches** -> **Switches**, select the checkbox for the updated Voice Server system.

b) Select the **Refresh** button. The Voice server cluster information will be updated on the List of Switches page.

- IF a duplex cluster reconfigures the OpenScape Voice server administration subnet IP address scheme such that the node 1 and node 2 administration IP addresses change **AND** that duplex cluster employs a **Standalone Survival Authority**;

  The assistant file on the Standalone Survival Authority must be configured with the updated node 1 and node 2 administration IP addresses. Refer to Section 6.5.3, “Installing the Standalone Survival Authority”, steps 2 and 3 for instructions on updating the configuration file. Any questions can be addressed to your next level of support.

  Please ensure that the values entered for node.cfg are only IPs (where applicable) and under no circumstances FQDNs, as FQDNs are not officially supported by OpenScape Voice IDS service.

Forbidden from being FQDNs NCPE fields
IP Configuration 1/4 - IPV4 - Sip - Node1
IP Configuration 1/4 - IPv4 - Sip - Node2
IP Configuration 1/4 - IPv4 - Sipmtls - Node1
IP Configuration 1/4 - IPv4 - Sipmtls - Node2
IP Configuration 1/4 - IPv4 - Sig - Node1
IP Configuration 1/4 - IPv4 - Sig - Node1
IP Configuration 1/4 - IPv4 - Billing - Node1
IP Configuration 1/4 - IPv4 - Billing - Node2
IP Configuration 1/4 - IPv4 - Xch - Node1
IP Configuration 1/4 - IPv4 - Xch - Node2
IP Configuration 1/4 - IPv4 - Mgmt - Node1
IP Configuration 1/4 - IPv4 - Mgmt - Node2
IP Configuration 1/4 - IPv4 - CSTA - Node1
IP Configuration 1/4 - IPv4 - CSTA - Node2
IP Configuration 1/4 - IPv4 - Lsm - Node1
IP Configuration 1/4 - IPv4 - Lsm - Node2
IP Configuration 1/4 - IPv4 - MGCP - Node1
IP Configuration 1/4 - IPv4 - MGCP - Node2
IP Configuration 1/4 - IPv6 - Sig - Node1
IP Configuration 1/4 - IPv6 - Sig - Node2

Table 33 NCPE fields that must be forbidden from being FQDNs

Forbidden from being FQDNs NCPE fields
IP Configuration 1/4 - IPv6 - Sip - Node1
IP Configuration 1/4 - IPv6 - Sip - Node2
IP Configuration 1/4 - IPv6 - Sipmtls - Node1
IP Configuration 1/4 - IPv6 - Sipmtls - Node2
IP Configuration 1/4 - IPv6 - MGMT - Node1
IP Configuration 1/4 - IPv6 - MGMT - Node2
IP Configuration 1/4 - IPv6 - Billing - Node1
IP Configuration 1/4 - IPv6 - Billing - Node2
IP Configuration 1/4 - IPv6 - CSTA - Node1
IP Configuration 1/4 - IPv6 - CSTA - Node2
IP Configuration 1/4 - IPv6 - Lsm - Node1
IP Configuration 1/4 - IPv6 - Lsm - Node2
IP Configuration 1/4 - IPv6 - MGCP - Node1
IP Configuration 1/4 - IPv6 - MGCP - Node2
IP Configuration 1/4 "SIS IP"
IP Configuration 2/4 "Super User"
IP Configuration 2/4 - Name Server IP 1
IP Configuration 2/4 - Name Server IP 2
IP Configuration 2/4 - Name Server IP 3
IP Configuration 2/4 - NTP Configuration - Server 1
IP Configuration 2/4 - NTP Configuration - Server 2
IP Security 1/3 - SNMP Servers - Address (Entry 1)
IP Security 1/3 - SNMP Servers - Address (Entry 2)
IP Security 1/3 - SNMP Servers - Address (Entry 3)
IP Security 1/3 - SNMP Servers - Address (Entry 4)
IP Security 2/3 - Misc hosts - Address (Entry 1)
IP Security 2/3 - Misc hosts - Address (Entry 2)
IP Security 2/3 - Misc hosts - Address (Entry 3)
IP Security 2/3 - Misc hosts - Address (Entry 4)
IP Security 2/3 - Misc hosts - Address (Entry 5)
IP Security 2/3 - Misc hosts - Address (Entry 6)
IP Security 2/3 - Misc hosts - Address (Entry 7)
IP Security 2/3 - Misc hosts - Address (Entry 8)
IP Security 2/3 - Misc hosts - Address (Entry 9)
IP Security 2/3 - Misc hosts - Address (Entry 10)
IP Security 2/3 - Misc hosts - Address (Entry 11)
IP Security 2/3 - Misc hosts - Address (Entry 12)

Table 33 NCPE fields that must be forbidden from being FQDNs

Forbidden from being FQDNs NCPE fields
IP Security 2/3 - Misc hosts - Address (Entry 13)
IP Security 2/3 - Misc hosts - Address (Entry 14)
IP Security 2/3 - Misc hosts - Address (Entry 15)
IP Security 2/3 - Misc hosts - Address (Entry 16)
IP Security 2/3 - Misc hosts - Address (Entry 17)
IP Security 2/3 - Misc hosts - Address (Entry 18)
IP Security 2/3 - Misc hosts - Address (Entry 19)
IP Security 2/3 - Misc hosts - Address (Entry 20)

Table 33 NCPE fields that must be forbidden from being FQDNs

See also in Chapter 2, “Creating a Node.cfg File” and Appendix 13.2.1, “EZIP Method Using the CMP” for startCli and CMP fields respectively, that must be forbidden from being FQDNs.

13.3 Verify the System Health after EZIP Configuration Change

It is a good practice to verify the System Health after an EZIP configuration change. Use the CMP to access the Node Health function (RapidStat). The steps are the same as in Section 13.1, “Verify the System Health before EZIP Configuration Change”.

13.4 Data Collection for EZIP issues

Overview

The section describes an OpenScape Voice command line interface that collects log files and data to aid in debugging problems related to the EZIP.

OSV Tools menu option 82 (System information - collects SMU and EZIP log files and data) will be used to collect the data. This option will collect data from both nodes of a duplex system and place the collected data of both nodes in a tar ball (on the node from which the data collection was initiated). The data collection contains a RapidStat result therefore it is not necessary to include a RapidStat log (unless asked to do so).

If the tool can not contact the other node a message advising as much will be presented on the terminal. In that case the tool should be invoked on the partner node also. The data will have to be collected from each node in this case.

"**[*] Done!**" is reported when the data collection completes. Notice that the data collection script indicates where the collected data is stored in the line preceding the "**[*] Done!**" indication.

After the data collection is complete enter 99 to exit the OSV Tools menu:

It is a good practice to copy the collected data to an offboard server for safe keeping. The collected data and the following information should be provided to your next level of support;

- Customer document title (and number) that was used to perform the IFgui Update (EZIP).
- "The point at which the problem occurred (with reference to the customer doc if possible).
- The OSV patchset level.
- The NCPE version used to perform the IFgui Update.

13.4.1 Accessing the 'tools' Menu and Example Session Collecting the EZIP log files and data

---

Note: The user will be prompted for the root user password after selecting menu option 82.

Logon to the OpenScape voice node as user srx (or su - srx). Type "tools" and a display similar to the following is presented;

```
srx@srxl41a:[/unisphere/srx3000/srx] #358

$ tools


################################################################################

#                      Welcome to the Hipath 8K Tools

These tools are dangerous! They can affect call processing

Do not run if you are not familiar with the side effects
################################################################################

Main Menu :

1. UCE context util - displays UCE contexts (ctxutil)

2. RDAL shared memory - displays and changes CAC bandwidth and call counts
(rdalTool)

3. SIP-SM dump - displays and accesses SIP SM shared memory (sipsmdump)

4. FQDN resolver - displays and manages the FQDN black list (fqdnresTool)

5. CSTA SM dump non-interactive - displays CSTA SM shared memory (cstasmdump)

6. CSTA SM dump interactive - displays CSTA SM shared memory (cstasmdump)

7. MLHG print - displays MLHG shared memory (mlhgprint)

8. NDAL memory display - numbering modification and CAC policies shared memory
(ndalMemDisplay)
```

```
9. OMM print - displays OMM shared memory (ommprint)

30. CDR decode - decodes CDR into readable text format (cdrdecode)

31. XLA verify - displays translation information for calling/called numbers
(xlaverify)

32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)

33. XDM SM Display - displays the content of the XDM Shared Memory (XdmShmDis-
play.exe)

50. RTP parameter delta - compares default vs. current RTP parameters

51. Security Model - displays the network packets rules

52. Network model - displays all network connections

53. Failover model - displays the network configuration for survivability

80. System information - collects low-level system information to diagnose plat-
form issues

81. System information - collects SPT and RU log files, traces and data

82. System information - collects SMU and EZIP log files and data

83. System information - collects DB log files and data

84. System information - collects Survival Authority log files and data

99. Exit

selection: 82

Password: (enter root user password here)

SMU Log collection

[*] Testing connectivity with other node

[*] This node (bocast4a) was installed using image installation. Continuing!

[*] Local node (bocast4a) - Primary partition installed version/patch:
V6.00.01.ALL.05/UNSPps0012E05

[*] Local node (bocast4a) - Secondary partition installed version/patch:
V6.00.01.ALL.05/UNSPps0012E04

[*] The partner node (bocast4b) was installed using image installation. Continu-
ing!

[*] Partner node (bocast4b) - Primary partition installed version/patch:
V6.00.01.ALL.05/UNSPps0012E05

[*] Partner node (bocast4b) - Secondary partition installed version/patch:
V6.00.01.ALL.05/UNSPps0012E04

[*] Collecting /log from primary partition (bocast4a)...

[*] Collecting /var/log/messages and /var/log/boot.msg from primary partition
(bocast4a)...

[*] Collecting /root/.bash_history from primary partition (bocast4a)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from primary partition
(bocast4a)...

[*] Collecting /export/home/units/smu from primary partition (bocast4a)...

[*] Collecting /opt/unisphere/srx3000/ifw from primary partition (bocast4a)...
```

```
[*] Collecting /etc from primary partition (bocast4a)...

[*] Collecting /log from secondary partition (bocast4a)...

[*] Collecting /var/log/messages and /var/log/boot.msg from secondary partition
(bocast4a)...

[*] Collecting /root/.bash_history from secondary partition (bocast4a)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from secondary partition
(bocast4a)...

[*] Collecting /export/home/units/smu from secondary partition (bocast4a)...

[*] Collecting /opt/unisphere/srx3000/ifw from secondary partition (bocast4a)...

[*] Collecting /etc from secondary partition (bocast4a)...

[*] Collecting RTP dump (bocast4a)...

[*] Collecting RapidStat output...

[*] Collecting iptables rules (bocast4a)...

[*] Collecting network interface configuration - ifconfig (bocast4a)...

[*] Collecting network routing configuration - ip route (bocast4a)...

[*] Collecting network routing configuration - route (Node 1)...

[*] Collecting filesystem configuration - df (Node 1)...

[*] Collecting node.cfg (bocast4a)...

[*] Collecting /log from primary partition (bocast4b)...

[*] Collecting /var/log/messages and /var/log/boot.msg from primary partition
(bocast4b)...

[*] Collecting /root/.bash_history from primary partition (bocast4b)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from primary partition
(bocast4b)...

[*] Collecting /export/home/units/smu from primary partition (bocast4b)...

[*] Collecting /opt/unisphere/srx3000/ifw from primary partition (bocast4b)...

[*] Collecting /etc from primary partition (bocast4b)...

[*] Collecting /log from secondary partition (bocast4b)...

[*] Collecting /var/log/messages and /var/log/boot.msg from secondary partition
(bocast4b)...

[*] Collecting /root/.bash_history from secondary partition (bocast4b)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from secondary partition
(bocast4b)...

[*] Collecting /export/home/units/smu from secondary partition (bocast4b)...

[*] Collecting /opt/unisphere/srx3000/ifw from secondary partition (bocast4b)...

[*] Collecting /etc from secondary partition (bocast4b)...

[*] Collecting RTP dump (bocast4b)...

[*] Collecting iptables rules (bocast4b)...

[*] Collecting network interface configuration - ifconfig (bocast4b)...
```

```
[*] Collecting network routing configuration - ip route (bocast4b)...

[*] Collecting network routing configuration - route (Node 1)...

[*] Collecting filesystem configuration - df (Node 1)...

[*] Collecting node.cfg (bocast4b)...

[*] Archiving collected files...

[*] The collected logs can be found in /tmp/
BOCAST4_20110901074143_log_collection.tgz

[*] Done!



################################################################################

Welcome to the Hipath 8K Tools

These tools are dangerous! They can affect call processing

Do not run if you are not familiar with the side effects

################################################################################


Main Menu :


1. UCE context util - displays UCE contexts (ctxutil)

2 . RDAL shared memory - displays and changes CAC bandwidth and call counts
(rdalTool)

3. SIP-SM dump - displays and accesses SIP SM shared memory (sipsmdump)

4. FQDN resolver - displays and manages the FQDN black list (fqdnresTool)

5. CSTA SM dump non-interactive - displays CSTA SM shared memory (cstasmdump)

6. CSTA SM dump interactive - displays CSTA SM shared memory (cstasmdump)

7 MLHG print - displays MLHG shared memory (mlhgprint)

    8. NDAL memory display - numbering modification and CAC policies shared mem-
ory (ndalMemDisplay)

9. OMM print - displays OMM shared memory (ommprint)


30. CDR decode - decodes CDR into readable text format (cdrdecode)

31. XLA verify - displays translation information for calling/called numbers
(xlaverify)

32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)

33. XDM SM Display - displays the content of the XDM Shared Memory (XdmShmDis-
play.exe)


50. RTP parameter delta - compares default vs. current RTP parameters

51. Security Model - displays the network packets rules
```

```
52. Network model - displays all network connections

53. Failover model - displays the network configuration for survivability


80. System information - collects low-level system information to diagnose plat-
form issues

81. System information - collects SPT and RU log files, traces and data

82. System information - collects SMU and EZIP log files and data

83. System information - collects DB log files and data

84. System information - collects Survival Authority log files and data


99. Exit

selection:
```

Note: Enter 99 to exit the OSV Tools menu.

---

14 Media Server Hardware Requirements and Prefix Access Code Installation

14.1 Hardware Recommendations for the OpenScape Media Server at OpenScape Voice

For OpenScape Media Server Standalone hardware recommendations refer to *OpenScape Media Server Vx Administrator Documentation* (where *x is the software release version*).

Note: For media server announcement and treatments, refer to *OpenScape Voice Vx Administration, Administrator Documentation* (where *x is the software release version*), the section titled *Media Services*.

The governing document for the media server hardware requirements is *OpenScape Media Server Vx Administrator Documentation* (where *x is the software release version*). The info in Section 14.1 is presented for information purposes only.

For Prefix Access Code (PAC) information, refer to Section 14.2, “How to Add/Delete Default PACs for Vertical Services”, on page 598.

The hardware requirements on the OpenScape Media Server at OpenScape Voice depend on the desired performance requirements and the operating mode in which you use the OpenScape Media Server.

Depending on the operating mode used and the desired performance requirements, there are hardware recommendations for the OpenScape Media Server at OpenScape Voice for the following applications:

- Internal OpenScape Media Server
- External OpenScape Media Server - basic system
- External OpenScape Media Server - default system
- External OpenScape Media Server - high performance system

14.2 How to Add/Delete Default PACs for Vertical Services

A configuration script (pac.sh) for the provisioning of the default Services Prefix Access Codes (PACs) is delivered with new/fresh OpenScape Voice installations.

14.2.1 Add Default PACs for Vertical Services Using the pac.sh Script

For Integrated Simplex or Standard duplex (Co-located or Geo separated deployments) run the following commands from node 1 (as the srx user);

```
su - srx
cd /unisphere/srx3000/srx/bin
./pac.sh
```

Note: There is a ‘period’ proceeding the forward slash (/) in the third command example.

You will be asked for the action you want to perform; create (c) PACs, delete (d) PACs, and the Numbering Plan (NP) name in which you wish to delete the PACs. In this case **create (c) PACs** is the correct choice.

The pac.sh script accepts a Private Numbering Plan (PNP) Name as an optional input.

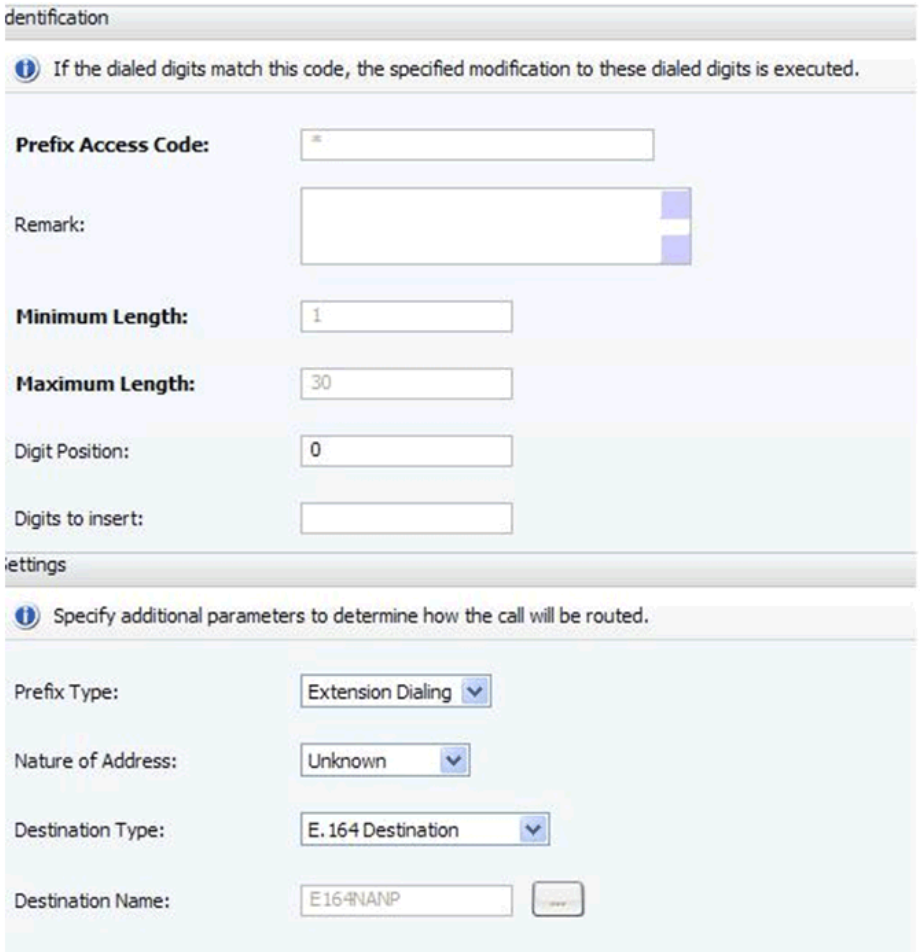
If the PNP Name **IS NOT PROVIDED, the script adds the default PACs to the E164 NP**.

If the PNP Name **IS PROVIDED, the script adds the default PACs to the specified PNP**.

Note: If the basic Business Group has already been provisioned, the PNP name can be found through the **OpenScape Voice Assistant > Business Group > Private Numbering Plans**.

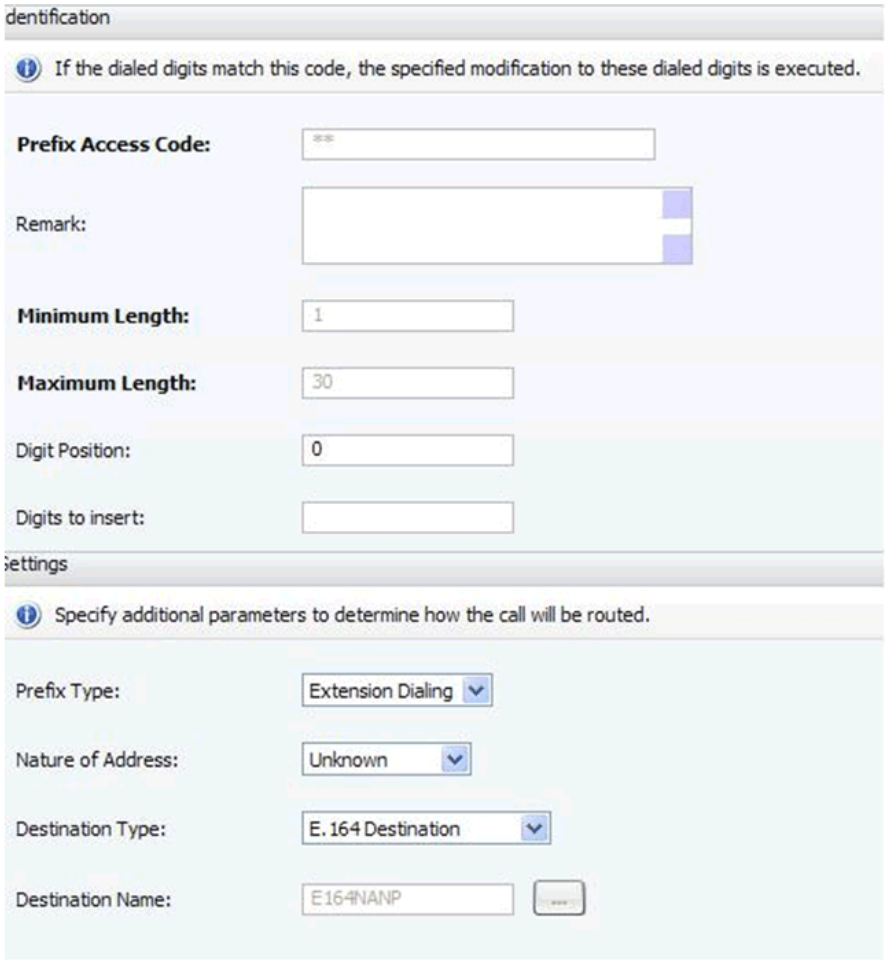
If you choose to create the PACs for the default E164 NP, you will need to create the needed *,**, # PACs and reference them to the E164 NP (in each working BG).
Examples are provided in the following snapshots (the user interface may change in later versions of the OpenScape Voice (OSV) Assistant);

PAC * create;


dentification
If the dialed digits match this code, the specified modification to these dialed digits is executed.
Prefix Access Code:
*
Remark:
Minimum Length:
1
Maximum Length:
30
Digit Position:
0
Digits to insert:
ettings
Specify additional parameters to determine how the call will be routed.
Prefix Type:
Extension Dialing
Nature of Address:
Unknown
Destination Type:
E.164 Destination
Destination Name:
E164NANP

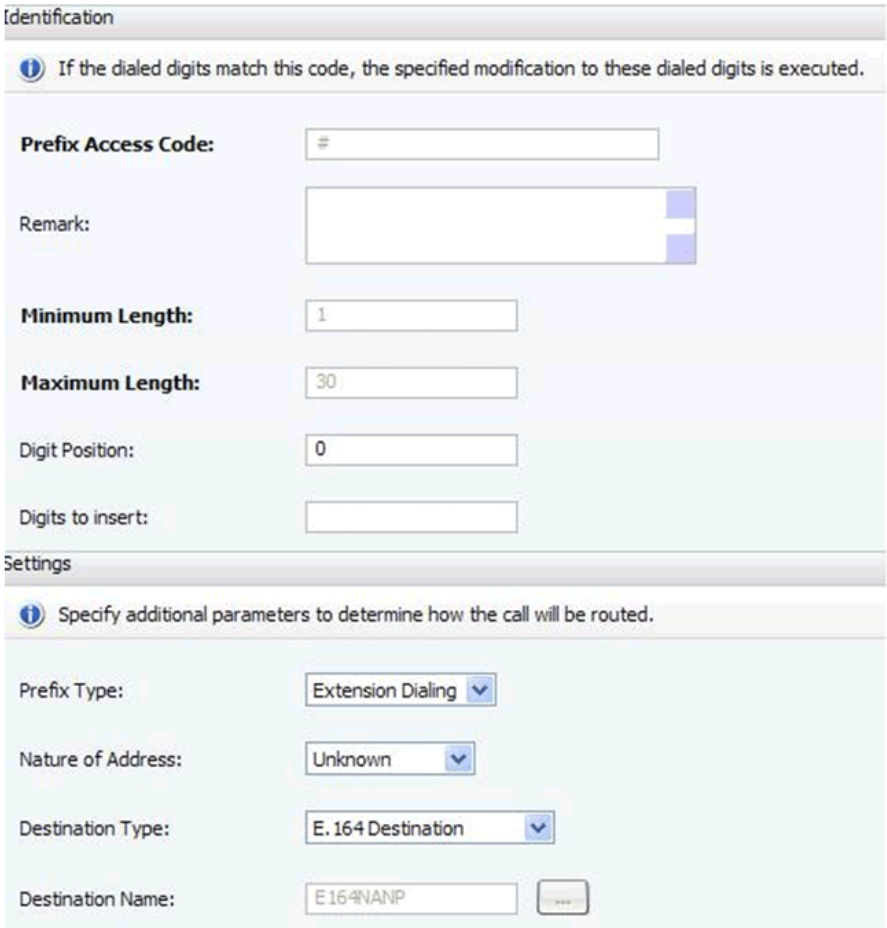
...

PAC ** create;


dentification
If the dialed digits match this code, the specified modification to these dialed digits is executed.
Prefix Access Code:
**
Remark:
Minimum Length:
1
Maximum Length:
30
Digit Position:
0
Digits to insert:
ettings
Specify additional parameters to determine how the call will be routed.
Prefix Type:
Extension Dialing
Nature of Address:
Unknown
Destination Type:
E.164 Destination
Destination Name:
E164NANP
...

...

PAC # create;


Identification
If the dialed digits match this code, the specified modification to these dialed digits is executed.
Prefix Access Code:
#
Remark:
Minimum Length:
1
Maximum Length:
30
Digit Position:
0
Digits to insert:
Settings
Specify additional parameters to determine how the call will be routed.
Prefix Type:
Extension Dialing
Nature of Address:
Unknown
Destination Type:
E.164 Destination
Destination Name:
E164NANP
...

14.2.2 Delete the Default PACs (Prefix Access Codes) for Vertical Services Using the pac.sh Script

For Integrated Simplex or Standard duplex (Co-located or Geo separated deployments), run the following commands from node 1 (as the srx user);

```
su - srx
cd /unisphere/srx3000/srx/bin
./pac.sh
```

Note: There is a 'period' proceeding the forward slash (/) in the third command example.

You will be asked for the action you want to perform; create (c) PACs, delete (d) PACs, and the Numbering Plan (NP) name in which you wish to delete the PACs. In this case, delete (d) PACs is the correct choice.

The pac.sh script accepts a Private Numbering Plan (PNP) Name as an optional input.

If the PNP Name **IS NOT PROVIDED, the script removes the default PACs from the E164 NP**.

If the PNP Name **IS PROVIDED, the script removes the default PACs from the specified PNP**.

Note: If the basic Business Group has already been provisioned, the PNP name can be found through the OpenScape Voice Assistant > Business Group > Private Numbering Plans.

If you chose to create the PACs *, ** and # (referencing them to the E164 NP) in each working BG; these PACs should be deleted using the OpenScape Voice (OSV) Assistant.

15 Example data collection session with the OSV Tools

The data collection is performed from the '**OSV Tools**' menu (delivered with the source release software). Data is collected from both partitions of each node. The resulting data collection is stored in a zipped tar file (on the server which the user initiated the data collection).

For consistency execute the command from node 1 of a duplex system (the script will collect data from both nodes of the duplex system).

User input is in bold font.

This example data collection log is from a V5.00.01.ALL.11/UNSPps0017E14 system;

The '**OSV Tools'** menu is invoked as user srx.

```
srx@bocast4a:[/unisphere/srx3000/srx] #83
$ tools


#################################################################
Welcome to the OSV Tools
These tools are dangerous! They can affect call processing
Do not run if you are not familiar with the side effects
#################################################################


Main Menu :


    1. UCE context util - displays UCE contexts (ctxutil)
    2. RDAL shared memory - displays and changes CAC bandwidth
and call counts (rdalTool)
    3. SIP-SM dump - displays and accesses SIP SM shared memory
(sipsmdump)
    4. FQDN resolver - displays and manages the FQDN black list
(fqdnresTool)
    5. CSTA SM dump non-interactive - displays CSTA SM shared
memory (cstasmdump)
    6. CSTA SM dump interactive - displays CSTA SM shared memory
(cstasmdump)
    7. MLHG print - displays MLHG shared memory (mlhgprint)
    8. NDAL memory display - numbering modification and CAC
policies shared memory (ndalMemDisplay)
    9. OMM print - displays OMM shared memory (ommprint)


   30. CDR decode - decodes CDR into readable text format
(cdrdecode)
```

```
   31. XLA verify - displays translation information for
calling/called numbers (xlaverify)

   32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)

   33. XDM SM Display - displays the content of the XDM Shared
Memory (XdmShmDisplay.exe)


   50. RTP parameter delta - compares default vs. current RTP
parameters

   51. Security Model - displays the network packets rules

   52. Network model - displays all network connections

   53. Failover model - displays the network configuration for
survivability


   80. System information - collects low-level system
information to diagnose platform issues

   81. System information - collects SPT and RU log files,
traces and data

   82. System information - collects SMU and EZIP log files and
data

   83. System information - collects DB log files and data


   99. Exit


selection: 82

Password: <root_user_password>

SMU Log collection

[*] Testing connectivity with other node

[*] This node (bocast4a) was installed using image installation.
Continuing!

[*] Local node (bocast4a) - Primary partition installed version/
patch: V5.00.01.ALL.11/UNSPps0017E14

[*] Local node (bocast4a) - Secondary partition installed
version/patch: V5.00.01.ALL.11/UNSPps0017E14

[*] The partner node (bocast4b) was installed using image
installation. Continuing!

[*] Partner node (bocast4b) - Primary partition installed
version/patch: V5.00.01.ALL.11/UNSPps0017E14

[*] Partner node (bocast4b) - Secondary partition installed
version/patch: V5.00.01.ALL.11/UNSPps0017E14

[*] Collecting /log from primary partition (bocast4a)...

[*] Collecting /var/log/messages and /var/log/boot.msg from
primary partition (bocast4a)...

[*] Collecting /root/.bash_history from primary partition
(bocast4a)...
```

```
[*] Collecting /unisphere/srx3000/srx/.kshrc_history from
primary partition (bocast4a)...

[*] Collecting /export/home/units/smu from primary partition
(bocast4a)...

[*] Collecting /opt/unisphere/srx3000/ifw from primary partition
(bocast4a)...

[*] Collecting /etc from primary partition (bocast4a)...

[*] Collecting /log from secondary partition (bocast4a)...

[*] Collecting /var/log/messages and /var/log/boot.msg from
secondary partition (bocast4a)...

[*] Collecting /root/.bash_history from secondary partition
(bocast4a)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from
secondary partition (bocast4a)...

[*] Collecting /export/home/units/smu from secondary partition
(bocast4a)...

[*] Collecting /opt/unisphere/srx3000/ifw from secondary
partition (bocast4a)...

[*] Collecting /etc from secondary partition (bocast4a)...

[*] Collecting RTP dump (bocast4a)...

[*] Collecting RapidStat output...

[*] Collecting iptables rules (bocast4a)...

[*] Collecting network interface configuration - ifconfig
(bocast4a)...

[*] Collecting network routing configuration - ip route
(bocast4a)...

[*] Collecting network routing configuration - route (Node 1)...

[*] Collecting filesystem configuration - df (Node 1)...

[*] Collecting node.cfg (bocast4a)...

[*] Collecting /log from primary partition (bocast4b)...

[*] Collecting /var/log/messages and /var/log/boot.msg from
primary partition (bocast4b)...

[*] Collecting /root/.bash_history from primary partition
(bocast4b)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from
primary partition (bocast4b)...

[*] Collecting /export/home/units/smu from primary partition
(bocast4b)...

[*] Collecting /opt/unisphere/srx3000/ifw from primary partition
(bocast4b)...

[*] Collecting /etc from primary partition (bocast4b)...

[*] Collecting /log from secondary partition (bocast4b)...

[*] Collecting /var/log/messages and /var/log/boot.msg from
secondary partition (bocast4b)...
```

```
[*] Collecting /root/.bash_history from secondary partition
(bocast4b)...

[*] Collecting /unisphere/srx3000/srx/.kshrc_history from
secondary partition (bocast4b)...

[*] Collecting /export/home/units/smu from secondary partition
(bocast4b)...

[*] Collecting /opt/unisphere/srx3000/ifw from secondary
partition (bocast4b)...

[*] Collecting /etc from secondary partition (bocast4b)...

[*] Collecting RTP dump (bocast4b)...

[*] Collecting iptables rules (bocast4b)...

[*] Collecting network interface configuration - ifconfig
(bocast4b)...

[*] Collecting network routing configuration - ip route
(bocast4b)...

[*] Collecting network routing configuration - route (Node 1)...

[*] Collecting filesystem configuration - df (Node 1)...

[*] Collecting node.cfg (bocast4b)...

[*] Archiving collected files...

[*] The collected logs can be found in /tmp/
BOCAST4_20110612152343_log_collection.tgz

[*] Done!


####################################################################

Welcome to the OSV Tools

These tools are dangerous! They can affect call processing

Do not run if you are not familiar with the side effects

####################################################################


Main Menu :


    1. UCE context util - displays UCE contexts (ctxutil)

    2. RDAL shared memory - displays and changes CAC bandwidth
and call counts (rdalTool)

    3. SIP-SM dump - displays and accesses SIP SM shared memory
(sipsmdump)

    4. FQDN resolver - displays and manages the FQDN black list
(fqdnresTool)

    5. CSTA SM dump non-interactive - displays CSTA SM shared
memory (cstasmdump)

    6. CSTA SM dump interactive - displays CSTA SM shared memory
(cstasmdump)

    7. MLHG print - displays MLHG shared memory (mlhgprint)
```

```
    8. NDAL memory display - numbering modification and CAC
policies shared memory (ndalMemDisplay)

    9. OMM print - displays OMM shared memory (ommprint)


   30. CDR decode - decodes CDR into readable text format
(cdrdecode)

   31. XLA verify - displays translation information for
calling/called numbers (xlaverify)

   32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)

   33. XDM SM Display - displays the content of the XDM Shared
Memory (XdmShmDisplay.exe)


   50. RTP parameter delta - compares default vs. current RTP
parameters

   51. Security Model - displays the network packets rules

   52. Network model - displays all network connections

   53. Failover model - displays the network configuration for
survivability


   80. System information - collects low-level system
information to diagnose platform issues

   81. System information - collects SPT and RU log files,
traces and data

   82. System information - collects SMU and EZIP log files and
data

   83. System information - collects DB log files and data


   99. Exit


selection: 99

srx@bocast4a:[/unisphere/srx3000/srx] #84

$
```

16 Flexible Ethernet circuit and IP Address Configuration Examples

Starting in V6, the Flexible Ethernet circuit and IP Address Configuration feature is introduced. This feature allows for a flexible configuration of Ethernet circuits and IP addresses.

16.1 Static IP notes

In this appendix, a Static IP refers to the 'Node X IP' listed NCPE Expert mode on IP Configuration (1/5). An 'X' designation refers to the Node number (1 or 2);

- Static IPs

  Node X IP … Found on each tab of IP Configuration (1/5)

16.2 Virtual IP notes

Virtual IP refers to the LSM and/or signaling manager IP addresses (e.g.; Sip Node X IP, SIP Node X MTLS IP). These Virtual IP address parameters are found in the NCPE Expert mode on IP Configuration (1/6). An 'X' designation refers to the Node number (1 or 2);

- Virtual IPs

  LSM Node X IP … iP Configuration (1/6) Management tab)

  SIP Node X IP … iP Configuration (1/6) Signaling tab)

  SIP-MTLS Node X IP … IP Configuration (1/6) 1/6 Signaling tab

  CSTA Node X IP … IP Configuration (1/6) Signaling tab

  Node X MGCP/NCS IP … IP Configuration (1/6) Signaling tab

  Node X IPV6 MGCP/NCS/SIP … IP Configuration (2/6) IPV6 Configuration

  Node X IPV6 SIP-MTLS … IP Configuration (2/6) IPV6 Configuration

---

Note: “Virtual” IPs are not really virtual in a network separated installation as they can't move to the partner. A network separated configuration would have "Node Separation = separate" set in the node.cfg file.

16.3 Node.cfg file changes on page IP Configuration 1/6

a) **Share Cluster with Mgmt** button was added. Select the associated box If the Cluster (X-channel) (CIuster Interconnect Group- CIGroup) is to share the same subnet (and Ethernet ports) as the Management Network. When this box is selected the CIGroup parameters will be grayed out and the CIGroup is placed in the Management Network subnet address scheme.

   IF the Cluster (X-Channel) is shared with the Mgmt subnet THEN the Cluster (X-Channel) is assigned the same IP addresses as the Mgmt Node IPs

b) **Subnet Sharing** parameter. This parameter will dictate the number of Ethernet ports used and the IP addressing schema for the subnets. Examples are included in this section

   - **Mgmt-Billing-Signaling-Separated:** Default configuration. All 8 Ethernet port pairs are used. Each subnet is assigned to ports as defined in Chapter 3 of this document (in the "Connecting the Cables" section of each platform).
   - **Mgmt-Billing-Shared:** The Mgmt and Billing subnets are merged - the Signaling and Cluster ports are separate. The Billing ports are not used.
   - **Mgmt-Billing-Signaling-Shared:** Mgmt, Billing and Signaling subnets are merged - Cluster ports are separate. Billing and Signaling ports are not used.

16.4 Co-located Cluster Signaling Subnet

In a co-located cluster Signaling subnet (node.cfg parameter Node Separation = none); a virtual IP cannot be the same as a static IP (Node X IP). The virtual IPs may all share the same IP.

- In this Appendix, 'X' refers to the Node number (1 or 2).
- Static IP refers to the 'Node X IP' listed in each table.
- Virtual IP refers to the LSM and/or signaling manager IP addresses (e.g.; Sip Node X IP, SIP Node X MTLS IP).

Static IPs	Virtual IPs ... Paramter location in NCPE expert mode
Node X IP	LSM Node X IP ... iP Configuration (1/6) Management tab)
	SIP Node X IP ... iPConfiguration (1/6) Signaling tab)
	SIP-MTLS Node X IP ... IPConfiguration (1/6) 1/6 Signaling tab
	CSTA Node X IP ... IP Configuration (1/6) Signaling tab
	Node X MGCP/NCS IP ... IP Configuration (1/6) ... Not shown here.
	Node X IPV6 MGCP/NCS/SIP .. IP Configuration (2/6)..Not shown here

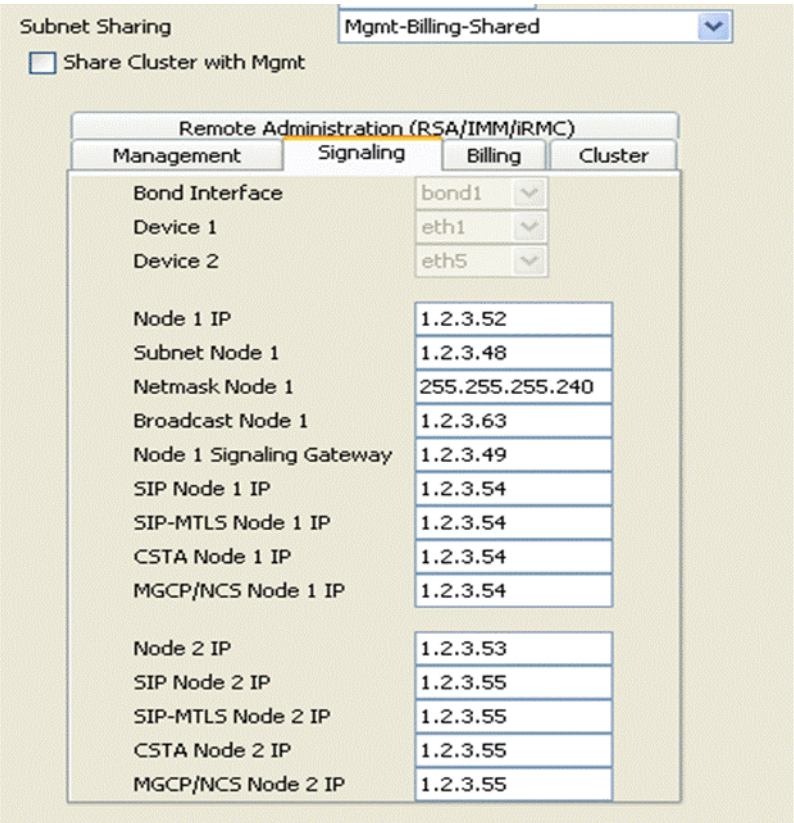
In this example (NCPE v6.0-17 is the reference for these displays);

- Node Separation = none (Not shown)
- Subnet Sharing = Mgmt-Billing-Shared
- The Cluster group (X-channel) is NOT shared with the Mgmt.
- With this installation configuration only the Mgmt, Signaling, and Cluster Ethernet ports will be used.
- In this example the virtual IPs share the same IP address. Note that the LSM Node X IP can also share this same IP address.

IF the Cluster (X-Channel) is shared with the Mgmt subnet THEN the Cluster (X-Channel) is assigned the same IP address as the Mgmt subnet Node IP.

Note: Follow this link to return to:Section 2.5.3, “Sharing of IP addresses”, on page 46.

Note: Follow this link to return to: Section 7.1.2, “Flexible Ethernet circuit and IP Address Configuration”, on page 421.



16.5 Separated Cluster Signaling Subnet

In a network separated cluster Signaling subnet (node.cfg parameter Node Separation = separated), **a virtual IP *can* be the same as a static IP.**

Note: 'Virtual' IPs are not really virtual in a network separated installation as they can't move to the partner node.

- In this Appendix, 'X' refers to the Node number (1 or 2).
- Static IP refers to the 'Node X IP' listed in each table.
- Virtual IP refers to the LSM and/or signaling manager IP addresses (e.g.; Sip Node X IP, SIP Node X MTLS IP).

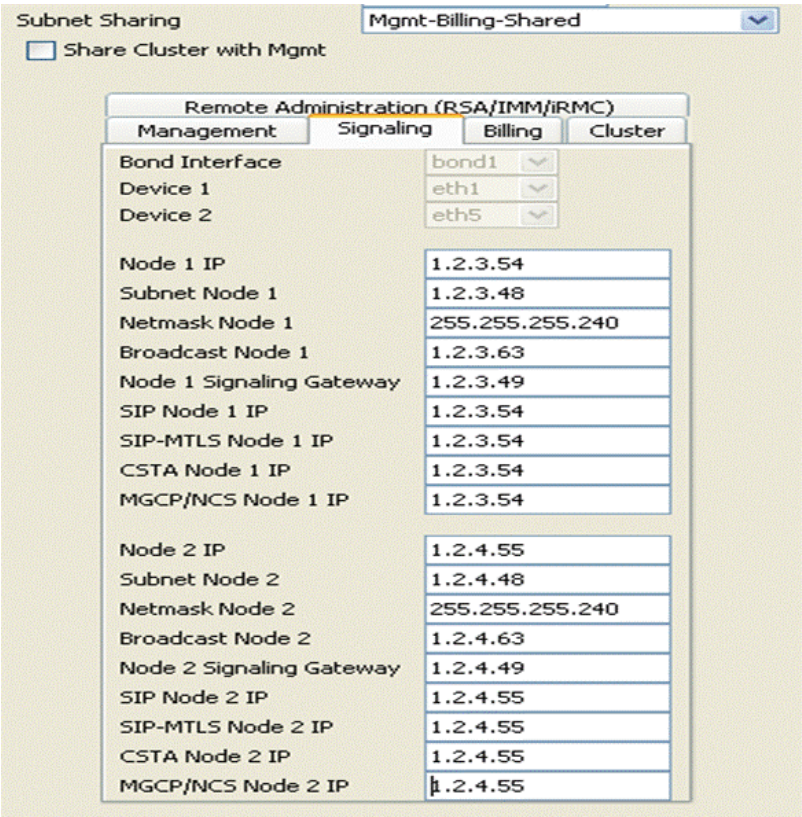
Static IPs	Virtual IPs ... Paramter location in NCPE expert mode
Node X IP	LSM Node X IP ... iP Configuration (1/6) Management tab)
	SIP Node X IP ... iPConfiguration (1/6) Signaling tab)
	SIP-MTLS Node X IP ... IPConfiguration (1/6) 1/6 Signaling tab
	CSTA Node X IP ... IP Configuration (1/6) Signaling tab
	Node X MGCP/NCS IP ... IP Configuration (1/6) ... Not shown here.
	Node X IPV6 MGCP/NCS/SIP .. IP Configuration (2/6)..Not shown here

In this example (NCPE v6.0-17 is the reference for this display);

- Node Separation = separate (Not shown)
- Subnet Sharing = Mgmt-Billing-Shared
- The Cluster group (X-channel) is NOT shared with the Mgmt.
- With this installation configuration only the Mgmt, Signaling, and Cluster Ethernet ports will be used. In this example, the virtual IPs (signaling managers) share the same IP address as the Static IP (Node X IP). Note that the LSM Node X IP can also share this same IP address.

IF the Cluster (X-Channel) is shared with the Mgmt subnet, THEN the Cluster (X-Channel) is assigned the same IP address as the Mgmt subnet Node IP.

Return to Section 2.5.3, “Sharing of IP addresses”, on page 46.


Subnet Sharing
Mgmt-Billing-Shared
Share Cluster with Mgmt
Remote Administration (RSA/IMM/iRMC)
Management
Signaling
Billing
Cluster
Bond Interface
bond1
Device 1
eth1
Device 2
eth5
Node 1 IP
1.2.3.54
Subnet Node 1
1.2.3.48
Netmask Node 1
255.255.255.240
Broadcast Node 1
1.2.3.63
Node 1 Signaling Gateway
1.2.3.49
SIP Node 1 IP
1.2.3.54
SIP-MTLS Node 1 IP
1.2.3.54
CSTA Node 1 IP
1.2.3.54
MGCP/NCS Node 1 IP
1.2.3.54
Node 2 IP
1.2.4.55
Subnet Node 2
1.2.4.48
Netmask Node 2
255.255.255.240
Broadcast Node 2
1.2.4.63
Node 2 Signaling Gateway
1.2.4.49
SIP Node 2 IP
1.2.4.55
SIP-MTLS Node 2 IP
1.2.4.55
CSTA Node 2 IP
1.2.4.55
MGCP/NCS Node 2 IP
1.2.4.55

17 Security

Note: When hardening the system, please refer to the OSV V11 Security Checklist Planning Guide. The Security Checklist Planning Guide contains the offical signoff forms.

This appendix includes information on settings of:

- Hardware
- BIOS
- Operating System
- OpenScape Voice Assistant
- Extending Software
- Secure Endpoint Communication
- 3rd-party software
- Traffic Separation

Deviations of the security settings on customer request are to be documented via the OSV V11 Security Checklist Planning Guide.

17.1 Hardware and BIOS Settings

Security settings for hardware and BIOS are described here.

17.1.1 Hardware Settings

Hardware Settings	
Settings	There are no necessary security hardware settings known now for any of the OpenScape Voice supported hardware platforms.
Description	Precondition: OpenScape Voice has been installed / updated according to Installation Manual. Enter the manufacturer name and model number on which OpenScape Voice is installed.

17.1.2 BIOS Settings

BIOS	
Settings	Change the administrator password to access the BIOS according to the instructions in your server's documentation guides.
Description	Access to the BIOS allows changing the boot order of the server. Once changed an intruder may use tools that are bootable from CD-ROM or USB device that allow a user to change the administrator password or install files. To prevent this from happening, the BIOS needs to be password protected.

Note: BIOS passwords should be set in accordance with company security policies.

17.2 Operating System

The OpenScape Voice V11 operates on a SLES 15 operating system.

17.2.1 Close Unused IP Ports

The Linux Firewall on OpenScape Voice is activated and only needed ports are open and in use. A comprehensive port list can be found in the Interface Management Data Base. Only needed ports are open and in use.

17.2.2 Password Management

Note: OSV security policies do not tolerate users with passwords that do not expire. By default, all passwords will expire in 90 days except for some administrator accounts (srx, cdr, solid) that have a one year expiry. Users with passwords that have no expiration date will trigger daily alarms to warn about a possible security risk.

17.2.2.1 Change Predefined Passwords for Administrator Accounts

---

Attention: The 'solid' user account does not carry a password and does not require a change of password because only the root user is permitted to login to the Solid account. Log in as the 'solid' user from user accounts other than the root account is not allowed and will receive an "incorrect password" response.

During the installation, all administrator accounts are created with default passwords which are generally known. These passwords must be changed upon deployment.

OS Lockdown	
Settings	Change default passwords for the following accounts: • "root" default account for the Linux Operating System • "srx" default account used by the OSV application related processes • "sysad" default account for System Administrators • "superad" default account for System Administrators with special rights • "hipatham" default account for OpenScape Accounting Manager • "hipathcol default account for OpenScape Collector • "cdr" default account used by the Call Detail Recording process on OSV • "secad" default account for System Security Administrators • "dbad" default for Database Administrators • "webad" default for Web Server Administrator (for Simplex configurations only) For an OpenScape Voice cluster, these passwords must be changed on each node individually. Users "sysad", "superad", "secad", "dbad" and "webad" have 90 day expiry limits set on their passwords. Refer to Section 4.2.3, “Installation Procedure” for additional information regarding passwords.
Description	Login to the system as root and enter the following command: `root# passwd user` Passwords should be 8-36 characters long in accordance with the customer's password policy.

OS Lockdown	
Affects on other products	The "srx" account is used by the OpenScape Voice Assistant to log in to OpenScape Voice and therefore, the new password needs to be entered on the Common Management Platform (CMP) as well. To do this, login to the Common Management Platform (CMP) and navigate to: **Configuration > OpenScape Voice > Select Switch > Switches > Select Switch and Edit > Mark "Enable Password(s)", modify password(s) for "srx" and Save.** For other products like, e.g., billing services using the "cdr" account, logging in via SSH/SFTP using any of the accounts mentioned in Settings would need to be changed as well.

17.2.2.2 Change Predefined Passwords for Application Accounts

OS Lockdown	
Settings	Change default passwords for solid users: "dba" "rtp" "sym" **(for Simplex configuration Applications only)** These passwords can be changed via the OpenScape Voice Assistant as follows: Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch > Administration > General Settings > Database** Refer to Section 4.2.3, “Installation Procedure” for additional information regarding passwords.
Description	Use the assistant to change the password of the solid database accounts.

17.2.3 Change Default Password Policies for New Accounts

Attention:

In order to prevent a potential collision between customer defined user accounts and OSV system accounts it is necessary to observe the following account restrictions;

- The account names and IDs listed below are reserved for OSV system accounts
- The group names and IDs listed below are reserved for OSV system accounts

In the event a customer defined account conflicts with an OSV system account ID (or group ID) listed below then the following action should be taken:

- Remove (and/or redefine) the conflicting customer defined account.
- Remove (and/or redefine) the conflicting customer defined group.

The following tables summarize the reserved system accounts and groups for the OpenScape Voice Server.

Reserved OSV System Account IDs.

Account Name	Account ID
haldaemon	501
sym	502
cdr	1001
srx	1522
solid	5000
superad	10000
sysad	10001
secad	10010
dbad	10011
reserved	10012
webad	10013

Table 34 Reserved OSV System Account IDs

Group Name	Group ID
rtpgrp	911

Group Name	Group ID
reserved	912
sym	913
dba	3020
cdrusers	3021
seclog	10001
reserved	10002

Table 35 Reserved OSV Group IDs

The customer's password policy has to be installed in case the customer creates new administrator accounts that are allowed to log in via SSH or SFTP.

OS Lockdown	
Settings	Ensure the customer's password policy has been applied to the system, preferably by using the /etc/pam.d mechanism. If the customer has no password policy, make sure that new user accounts have a minimum password length of 8 or 15 for a JITC system, a password history of no less than 5 and the character requirements defined.

OS Lockdown	

Description	To set the password history and minimum password length modify the "password:" line in the **/etc/security/pam_pwcheck.conf** configuration file as follows:
	`password: minlen=8 maxlen=16 remember=5 use_cracklib use_authtok use_first_pass`
	For password history it is necessary to create the **opasswd** file for storing old password hashes:
	`touch /etc/security/opasswd`
	`chown root:root /etc/security/opasswd`
	`chmod 600 /etc/security/opasswd`
	For minimum password length also modify /etc/login.defs as follows:
	`PASS_MIN_LEN 8`
	The default password age should be set to 60 days.
	After 60 days, the user will be prompted to change his password. There is a 30 day grace period to do so before the account is locked.
	To set the password age:
	`passwd -x 60 -w 14 -n 1 -i 30 <userid>`
	The default password character requirements are two Upper case letters, two Lower case, one Numeric character (two for a JITC system) and at least one special character (two for a JITC system). Also a limitation of three repeats for the same character class exists. For a JITC system there must be at least 15 characters.
	To set the password minimum character requirements, minimum difference, and password retries modify the "password requisite" line in the:
	/etc/security/common-password-pc configuration file:
	`password requisite pam_cracklib.so retry=3 difok=4 maxclassrepeat=3 minlen=8 dcredit=-1 ucredit=-2 lcredit=-2 ocredit=-1`

17.2.4 Change Denial of Service Thresholds

During the installation, a large amount of data must be transferred to and from the server from software servers and between nodes of the cluster, etc. In order not to impede this process, the threshold for detection of a denial of service attack has been intentionally set at 20,000 messages per second. After installation, this value should be reduced.

A default white list is automatically generated at startup, based on the following node.cfg entries; Each partner on the admin, signaling and billing interfaces, and snmp_servers.

OS Lockdown	
Settings	Change the default packet rate that will trigger a denial of service lockout.
Description	You can provision the Denial of Service thresholds from the CLI. The following are the defaults and provisionable ranges: • Block Period: 1 to 2048 seconds, with a default value of 60 seconds • Rate Threshold: 1 to 256,000 packets per second, with a default of 200,000 packets per second Typically, no single network IP-Address (for example, single phone or server) will deliver heavy amounts of packet traffic; however, message concentrators such as an SBC or proxy can create heavier amounts of packet traffic and need to be taken into account when setting the rate threshold value and the “white list” of trusted hosts, which is the list of IP addresses that are exempt from the rate threshold limit. After installation, and bring up is complete and verified, for normal operation of the OpenScape Voice system, it is recommended that the rate threshold value be set to 200 packets per second (CLI:6,1,1,6,3) for a clustered deployment and 2000 packets per second for an integrated simplex deployment. Use Option 2 to display the Rate Thresholds and option 1to modify the Rate Thresholds. For more information, see *OpenScape Voice Security Checklist*, chapter **Change Denial of Service (DoS) Thresholds.**

17.2.5 Allow IPsec Fragmentation

If remote branch offices are connected to the data center by way of VPN or IPsec tunnel, the routers doing that may require an MTU lower than the default of 1500. This is most noticeable when SIP keysets are deployed at the remote branch offices, as they exchange large amounts of data in a message that normal endpoints would not transmit. Many customer routers that establish this tunnel use ICMP (type 3) packets to determine what the maximum packet size is that can be reliably transmitted. The firewall in the OpenScape Voice must be opened to respond to these kinds of ICMP packet challenges. If these (type 3) ICMP packets are being dropped, these settings will allow safely opening the firewall to permit the traffic.

Secure Endpoint Communications	
Settings	Change default ICMP types to allow IPsec fragmentation between SIP endpoints (by way of VPN tunnel on remote router).

Description	To enable ICMP message type 3 on OpenScape Voice:
	• Modify the ICMPDefaultTypes parameter string to include message type 3 (CLI: 1,1,3)
	`Configuration Parameters (methods):`
	`browseParameterNames ...........1`
	`getParameter.................2`
	`modifyParameter .............3`
	`Selection (default: 2): 3`
	
	`modifyParameter:`
	`name : hiQ/Security/Filt/ ICMPDefaultTypes`
	
	`modifying variable parameters:`
	`current value: 0, 8`
	`value <max length: 2047>: 0,3,8`
	`input value was: "0,3,8"`
	`Do you want to execute this action? (default: yes) :`
	
	• `executing method modifyParameter...`
	`Ok.`

Secure Endpoint Communications	

Description continued.	• Restart the Security Manager on each node (CLI: 98)
	`CLI> procStopProcess "SecMgr1"`
	...wait a few seconds for it to shut down.
	`CLI> procStartConfiguredProcess "SecMgr1"`
	Menu commands are:
	`5…1…8 (to stop) and then 6 (to start)`
	• Create ICMP packet filter rule(s) for remote host, subnet, or all hosts (CLI: 6,8,4,1):
	`Packet Filter Rule Name <Max Length 63 (max length: 63)> (def: ) : SUBNET789_SIP1_FRAGMENT_ALLOWED`
	`Description <Max Length 63 (max length: 63)> (def: ):`
	`Allow ipsec fragmentation with remote SIP subnet`
	`Remote FQDN <Max Length 63 (max length: 63)> (def: ):`
	`Remote IP Address <Max Length 15 (max length: 15)> (def:): <remote subnet for SIP endpoints>`
	`Remote NetMask <Max Length 15 (max length: 15)> (def: 255.255.255.255) : 255.255.255.0`
	`<remote subnet mask for SIP endpoints>`
	`Transport Protocol <1=icmp, 2=udp, 3=tcp, 4=all, 5=esp, 6=ah, 7=sctp> (default: 4): 1`
	`Direction <1=incoming, 2=outgoing, 3=bothways (default: 1): 1`
	`Action <1 = Allow, 2 = Drop> (default: 1): 1`
	`Do you want to execute this action <y/n> (default: yes):`
	`Operation successful`

17.2.6 Turn on IPsec (Internet Protocol Security) Between Servers

After the installation of all servers and connected devices and a functional test has been completed, ensure that you have defined IPsec policies and activated IPsec communication to the OpenScape Voice Assistant, etc. This applies to all servers that are somehow accessed using an un-secure protocol (such as SNMP, MGCP, CSTA).

Secure Communications	
Subcomponent	Inter-server secure communication
Settings	Verify that IPsec is used to encrypt all non-secure communication between the OpenScape Voice and its associated servers.
Description	Add Secure Endpoints for all associated servers that appoint IPsec natively through their OS. Refer to Appendix 19, “IPSec Configuration”. Refer to the guidelines from those associated servers as to how to configure IPsec on their side. Typically, this is done at an OS level. The OS supplier usually provides guidelines as to how to configure IPsec for their products. Use IPsec for the following servers: • Media Servers (to protect the MGCP protocol which only supports UDP). This includes an OpenScape Branch deploying an on-board media server. • Transfer of logging files • Common Management Platform server • Pulling of billing files from OpenScape Voice by a billing server.
Affect on other products	The IPsec credentials must be entered on the peer server as well.

NOTICE: OpenScape Voice uses "racoon" to establish IPsec connections. Racoon uses the IKE (ISAKMP/Oakley) key management protocol to establish secure connections with older hosts.

Note: Click this link to return to step 43 on page 36 in Section 2.2.4, “OpenScape Voice Installation Checklist”.

17.2.7 TLS (Transport Layer Security) Certificates

17.2.7.1 Change the Default TLS Certificates

OpenScape Voice comes with a default self-signed TLS Server Certificate. Even when not integrated in a PKI infrastructure, the default TLS certificate of OSV should be replaced with a new TLS certificate.

TLS Certificates	
Settings	Create new root and server certificates for the OpenScape Voice solution.
Description	Follow the instructions in *OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS)*, chapter **OpenScape Voice**.
Affect on other products	Creating your own root certificate means that the root CA certificate must be installed in the trusted Root CA store of all products that need to establish a TLS connection to OpenScape Voice. This includes, but is not limited to,: • Phones • Proxies • Gateways • Voice Mail Servers • etc.

17.2.7.2 Activate Verification for Mutual TLS

TLS connections can have post-connection validation performed upon them where the certificate that the peer offers is checked for validity. The checks performed at the current time are that if there is a subject alternative name within the certificate and that if that name contains either DNS names, or IP addresses that these DNS names, (after DNS resolution to IP address) and/or IP addresses are checked against the IP address of the peer presenting the certificate. If the DNS/IP address does not match the IP address of the peer the connection is closed automatically. If there is no subject alternative name within the certificate, the common name within the subject name is assumed to be a DNS name or IP address. This is then similarly checked against the IP address of the peer

presenting the certificate. If the DNS name after resolution to IP address does not match the IP Address of the peer, the connection is also closed automatically.

NOTICE: By default, post-connection verification is switched off. As a prerequisite to switching the verification on, the certificates must have been exchanged.

Post-connection Verification Parameter	
Settings	Verify that post-connection verification is switched on.
Description	Via CLI (CLI: 1,1) Use Option 2 to verify the value for RTP parameter: **Srx/ttud/verification** is set to **RtpTrue**. Use Option 3 to set the value for RTP parameter: **Srx/ttud/verification** to **RtpTrue,** if it is currently set to **RtpFalse** --- **Note:** The procedure might interrupt call processing and should be executed in a timely manner (or low traffic periods). For a live system the best practice would be to execute the procedure in a maintenance window. --- Stop and start the ttud process on each node. Expert Cli examples follow: CLI> **procStopProcess "ttudProc1"** ...wait a few seconds for it to shut down. CLI> **procStartConfiguredProcess " ttudProc1"** In a duplex configuration, be sure to restart the process in node2. Expert Cli examples follow; CLI> **procStopProcess "ttudProc2"** ...wait a few seconds for it to shut down. CLI> **procStartConfiguredProcess "ttudProc2"** From the Cli Menu, make the following selections: 5…1…8 (to stop the process) 5…1…6 (to start the process)
Affects on other products	The server certificate issued to MTLS (Mutual Transport Layer Security) capable endpoints must abide to above rules. Before turning on this RTP parameter, ensure that all server certificates issued to MTLS endpoints either have the DNS name or the IP address in the subject alternative name extension or the common name of the subject field.

17.3 Securing Interfaces

OpenScape Voice offers 3 interfaces: administration, billing and signalling.

17.3.1 Securing the Administration Interface

17.3.1.1 SNMP Community Name

SNMP V2c uses the notion of communities to establish trust between managers and agents. Community names are essentially passwords. A community name allows a level of access to Management Information Base (MIB) data. Access levels are read-only (RO) for data retrieval and read-write (RW) for data modification. Thus an SNMP Manager requires at least two community names or passwords.

The OpenScape Voice sets by default the RO community name to "SENread" and the RW community name to "SENsnmp". It is very important to change these default values at the time of installation as they could be well known to the general public.

NOTICE: V2c of the SNMP protocol sends the community names in clear text. To prevent sniffing the community name, the interface between the SNMP agent and the SNMP server needs to be secured via IPsec.

Securing Administration Interface	
Protocol	SNMP
Settings	Change default values for RO and RW community names.
Description	The OpenScape Voice provides the capability to modify the SNMP RO and RW community names via the CLI (CLI: 6,1,9). Use Option 1 to display the current SNMP configuration and Option 2 to modify the SNMP configuration.
Affects on other products	Any server (with exception of the Survival Authority) using SNMP to retrieve information from OpenScape Voice or to set information in OpenScape Voice has to also change the read and write community names.

Note: Click this link to refer to Section 4.4.7, “SNMP Community Names on OpenScape Voice”, on page 292. Follow the instructions in Section 4.4.7.1, “Changing the Community String for the Emanate Master Agent”, on page

293 and Section 4.4.7.1, “Navigate to menu 6 > 1 > 9 > 2 to display the SNMP configuration for verification purposes.”, on page 294. A link back to here is provided in Section 4.4.7.1.

In addition to sending SNMPv2 traps for example to the CMP, the OSV can be configured with (additional) trap destinations for SNMPv3 traps.

This trap destination is configured via NCPE/EZIP and OSV Assistant. Passwords can only be set by Assistant for an already installed active OSV and they are not stored in node.cfg. Once configured the trap destination configuration is maintained over SW upgrades.

Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, it looks much different due to new textual conventions, concepts, and terminology. SNMPv3 primarily added security, replaces the community name with authentication and privacy (encryption) capabilities to SNMP trap messages sent by OSV. Authentication consists of a security name and a password. The password is hashed using either MD5 or SHA, default is SHA, and then used to create a digest of the message content to protect the integrity of the message. Privacy for the payload is also possible, making use of a password which is also hashed and then used to encrypt the PDU section of a message using either AES or DES, default is DES.

The user can define 'No Authentication or Privacy' (which is no better than v2c and is not recommended), 'Authentication Only', or 'Authentication and Privacy'. Privacy by itself is not permitted by the standards. Default is Authentication and Privacy.

To uniquely identify an agent (in our case an OSV), the SNMP v3 protocol defines an "engineID" that uniquely identifies an agent. The engineID must be consistent through time and should not change or conflict with another agent's engineID. The OSV trap engineID shall be built from the cluster name (engineID as 80:00:00:00:04:<cluster name in hex, up to 27 char>) and displayed read-only at the NCPE/EZIP/Assistant GUI.

Note: It is assumed that this feature is only for alarm traps generated by OSV. So OSV does not support SNMPv3 get and set, only SNMPv2.The OSV to Survival Authority/CMP trap is SNMPv2 only. OSV can already receive SNMPv3 traps (reporting link status to OSV LSM IP, e.g. from OpenBranch). Here SNMPv3 settings are done via RTP parameters.

You can configure the parameters stated in the table below:

Add/Edit SNMP EZIP Server parameter	Description
Destination IP	IP of destination server. This is a mandatory parameter
Port	Trap destination port. Default value: 162 This is a mandatory parameter.
Version	SNMP Privacy Protocol. Options: • v2c • v3 NOTE: The Auth/Security Level, Auth Protocol, Auth Password, Privacy Type and Privacy Password fields are intended for SNMPv3 configurations only and are not used for SNMPv2c configurations.
Security Name	User name If Version is set to: • v2c, Security Name = public • v3, Security Name = SnmpV3User This is a mandatory parameter.
Auth/Security Level	Authentication/Security Level. If Version is set to v3 the following options are available: • NoAuthNoPriv (unauthenticated and unencrypted) • authNoPriv (authenticated but unencrypted) • authPriv (authenticated and encrypted)
Auth Protocol	Authentication protocol. If Version is set to v3 and Auth/Security Level is set to authPriv or authNoPriv the following options are available: • MD5 • SHA
Privacy Type	Encryption standard. If Version is set to v3 and Auth/Security Level is set to authPriv the following options are available: • AES (Advanced Encryption Standard) • DES (Data Encryption Standard)
Trap Engine ID	Identifier for the given SNMP.

17.3.1.2 Securing SOAP Signaling

The OpenScape Voice allows configuration changes to be made via the SOAP interface. SOAP Applications should use one of 2 mechanisms to secure this interface:

- Secure the connection between the SOAP client and the SOAP server via IPsec. This allows connecting to the TCP SOAP server ports.
- Secure the connection between the SOAP client and the SOAP server by connecting to the TLS SOAP server ports.

NOTICE: The OpenScape Voice firewall must be opened to allow SOAP clients other than the Assistant to connect.

17.3.1.3 Securing SOAP Signaling via IPsec

SOAP Clients that do **not** support TLS can connect to OpenScape Voice via TCP with a secure IPsec connection.

The unsecure SOAP Server ports are 8767-8770.

The ports can be checked using the CLI or the Display of Rtp parameters using the Assistant:

- Srx/Subp/Port for the first available port
- Srx/Subp/NumberOfInstances for the number of available ports

When changing any of the above Rtp parameters the soapserver process on each node needs to be stopped and started. Expert Cli examples follow;

CLI> **procStopProcess "soapServer01"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer01"**

In a duplex configuration, be sure to restart the process in node2. Expert Cli examples follow;

CLI> **procStopProcess "soapServer02"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer02"**

From the Cli Menu, make the following selections:

5…1…8 (to stop the process)

5…1…6 (to start the process)

Securing SOAP Signaling	
Subcomponent	SOAP Server
Settings	Secure TCP SOAP Clients (such as the Common Management Platform) with IPsec. **Note:** The communication between the OpenScape Voice Server and the Common Management Platform can also be secured using TLS.
Description	See Section 17.2.6, “Turn on IPsec (Internet Protocol Security) Between Servers”, on page 629

17.3.1.4 Securing SOAP Signaling via TLS

SOAP Clients that support TLS can connect to OpenScape Voice via TLS instead of TCP with IPsec connection.

The secure SOAP server ports are 8757 - 8760.

The number can be changed using CLI (**to up to 4 ports**) or via the Assistant:

- Srx/Subp/NumberOfInstancesWithTLS

Default server port is 8757, **defined with**

- Srx/Subp/StartingPortWithTLS

When changing any of the above Rtp parameters, the soapserver process on each node needs to be restarted (CLI: 98)

CLI> **procStopProcess "soapServer01"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer01"**

In a duplex configuration also:

CLI> **procStopProcess "soapServer02"**

...wait a few seconds for it to shut down.

CLI> **procStartConfiguredProcess "soapServer02"**

The menu commands are:

5…1…8 (to stop the process)

5…1…6 (to start the process))

Securing SOAP Signaling	
Settings	Secure SOAP Clients that support establishing TLS connections with TLS.
Description	The starting port for SOAP TLS can be verified via the CLI (CLI: 1,1). Use Option 2 to verify the value for RTP Parameter: `Srx/Subp/StartingPortForTLS`

17.3.1.5 Adding Authorization to SOAP

Securing SOAP Signaling	
Subcomponent	SOAP Server
Settings	The SOAP server must be set up to authorize SOAP clients for limited access to the SOAP server.
Description	Enabling the SOAP Authorization check is done via the CLI or the Assistant. Via the CLI (CLI: 1,1): Use Option 2 to verify that the value for RTP Parameter **Srx/Subp/Authorization** is set to **RtpTrue**. Use Option 3 to set the value for RTP Parameter **Srx/Subp/Authorization** to **RtpTrue** if it is currently set to **RtpFalse**. Via the Assistant: **Configuration > OpenScape Voice > Select Switch > Administration > General Settings > RTP** Check the parameter value for Parameter Srx/Subp/Authorization and modify it to RtpTrue if it is currently set to RtpFalse. Authorization can then be added for each SOAP client via the OpenScape Voice Assistant. SOAP clients are identified via their IP address. To authorize SOAP clients for limited access to OpenScape Voice, login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select Switch > Administration> General Settings > SOAP/XML Client > Add >** Enter all required information and **Save**.

17.3.1.6 Firewalling the SOAP Clients

By default, OpenScape Voice blocks all admin traffic via the firewall. To allow a SOAP client to connect, the firewall must be opened for the SOAP client.

Securing SOAP Signaling	
Subcomponent	SOAP Clients
Settings	Open firewall for authorized SOAP clients.
Description	<Enter firewall rule here to allow the traffic>

17.3.2 Securing the IMM or iRMC Access

The Intel IMM / iRMC cards are used by hardware platforms for remote access.

Securing Remote Administration Interface	
Subcomponent	Access cards
Settings	• Restrict IPMI to Internal Networks • Encrypt Traffic • Utilize Strong Passwords • Require Authentication

17.3.2.1 Restrict IPMI to Internal Networks

Restrict IPMI traffic to trusted internal networks. Traffic from IPMI (usually UDP port 623) should be restricted to a management VLAN segment with strong network controls. Scan for IPMI usage outside of the trusted network and monitor the trusted network for abnormal activity.

17.3.2.2 Change the Default Passwords for the IMM/iRMC Card

By default, the IMM/iRMC card is shipped with well known and well documented default passwords.

Securing Remote Administration Interface	
Subcomponent	IMM/iRMC card
Settings	Change the default passwords.
Description	Refer to Section 4.4.3, “Changing the User ID and Password for the IMM/iRMC/BMC Account”.

Change the User ID and Password to the user name and password configured for the IMM/iRMC on the specified node. This must be complete for each node of the cluster.

CAUTION

Failure to complete this update for each cluster configuration will result in Communication Failure alarms and could cause a failure event resulting in one of the nodes in the cluster being shutdown.

Note: Click this link to jump to Section 4.4.3, “Changing the User ID and Password for the IMM/iRMC/BMC Account”.
(A doc link to return to this section is provided.)

17.3.3 Securing the Signaling Interface

17.3.3.1 Activate TLS Signaling for SIP Subscribers

By default, SIP subscribers are generated using SIP signaling in clear-text via TCP or UDP. Signaling should be encrypted using TLS provided the SIP subscriber supports it.

Securing SIP Signaling	
Subcomponent	SIP Subscribers
Settings	Turn on TLS for SIP Signaling to the Subscribers. This setting can be controlled on a per subscriber basis.
Description	Set SIP Subscribers to TLS using the OpenScape Voice Assistant. **For subscribers in branch offices:** 1. Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch > Business Group > Select Business Group > Select Branch Office > Members > Subscribers > Select Subscriber, click Edit > Connection tab > Set Transport Protocol to TLS >** 2. Click **Save** **For subscribers in the main office:** 1. Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch > Business Group >Select Business Group > Members > Subscribers >Select Subscriber, click Edit > Connection tab > Set Transport Protocol to TLS >** 2. Click: **Save**

17.3.4 Activate TLS Keep-Alive for OpenStage Phones

Activate TLS Keep-Alive for OpenStage Phones	
Subcomponent	SIP Signaling Management
Settings	Enable TLS Keep-Alive for OpenStage Phones
Description	Set TLS Keep-Alive for OpenStage Phones using the OpenScape Voice Assistant. Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch > Signaling Management > Digest authentication>** **Select "Enable TLS Keep-Alive for Openstage phones"** in section **"Transport Layer Security",** click **Save**

17.3.4.1 Activate MTLS Signaling for SIP Endpoints

By default, SIP endpoints are generated using SIP signaling in clear-text via TCP or UDP. Signaling should be encrypted using mutual TLS provided the SIP endpoint supports it.

Securing SIP Signaling	
Subcomponent	SIP Endpoints
Settings	Turn on MTLS for SIP Signaling to the Endpoints. This setting can be controlled on a per Endpoint basis.
Description	Set SIP Endpoints to MTLS using the OpenScape Voice Assistant. Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch** Endpoints can be created in business groups and globally. To set an endpoint in the business group to MTLS: **Business Group > Select Business Group > Select Branch Office > Members > Endpoints > Select Endpoint, click Edit > SIP tab > Set Transport Protocol to MTLS > Save** To set a global endpoint to MTLS: **Global Translation and Routing > Endpoint Management > Endpoints > Select Endpoint, click Edit > SIP tab > Set Transport Protocol to MTLS > Save**

17.3.4.2 Activate Digest Authentication to the SIP Subscribers and SIP Endpoints

By default, Digest Authentication is not activated after installation. This allows a hacker to register a phone using the phone number of any subscriber, and thus fake their identity. By assigning a unique login, password, and realm to each subscriber, a hacker will be discouraged from hijacking a user's identity.

Note: Remote SBC End Points having the same SBC core signaling address with different sip port can be included as a trusted realm in the OpenScape Voice server Digest Authentication settings only with the same Digest authentication credentials (Username, password, realm etc). That is why OSV supports a unique Signaling IP entry in the Digest Authentication trusted realm list.

Securing SIP Signaling	
Subcomponent	SIP Subscribers and SIP Endpoints
Settings	Turn on Digest Authentication for SIP signaling to SIP Subscribers and SIP Endpoints. This setting is system-wide for SIP Subscribers and endpoint specific for SIP Endpoints.
Description	Digest Authentication can be provisioned from the CLI and from the OpenScape Voice Assistant. To activate digest authentication globally in the system, login to the Common Management Platform and navigate to: **OpenScape Voice > Select Switch > Administration > Signaling Management > Digest Authentication > Check Enable Authentication > Save** Assign user name, individual password, and realm to each SIP subscriber using the customer's password policy. Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch > Business Group > Select Business Group > Select Branch Office > Members > Subscribers > Select Subscriber, click Edit > Security tab > Set Realm, User Name and Password > Save** SIP Endpoints that are not secured via MTLS must be provisioned for digest authentication. Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch**

Securing SIP Signaling	
Description continued	Endpoints can be created in business groups and globally. To set digest authentication for an endpoint in the business group: **Business Group > Select Business Group > Select Branch Office > Members > Endpoints > Select Endpoint, click Edit > SIP tab / Security / Add … or Edit > Set Local and Remote Realm, User Name and Password. Local is used for challenges received from the peer endpoint and Remote is used for creating challenges towards the peer endpoint. > Save** To set digest authentication for a global endpoint: **Global Translation and Routing > Endpoint Management > Endpoints > Select Endpoint, click Edit > SIP tab / Security / Add … or Edit > Set Local and Remote Realm, User Name and Password. Local is used for challenges received from the peer endpoint and Remote is used for creating challenges towards the peer endpoint. > Save**
Affect on other products	This change must occur in the OpenScape Voice and the Subscriber or SIP endpoint at the same time, so coordination of these activities is necessary.

17.3.4.3 Activate Authentication of SIP Subscribers and SIP Endpoints behind Trusted Endpoints

OpenScape Voice allows SIP subscribers and SIP endpoints to be considered trusted as soon as they are communicating with OpenScape Voice through a trusted SIP proxy. This is not a recommended setting.

Authenticating SIP Subscribers and SIP Endpoints behind SIP Proxies	
Subcomponent	Authentication
Settings	Enforce authentication of SIP Subscribers and SIP Endpoints behind SIP Proxies.
Description	Authentication of SIP Subscribers and SIP Endpoints behind SIP Proxies is done via the CLI (CLI: 1,1). Use Option 2 to verify that the value for RTP parameter Srx/Sip/AuthTraverseViaHdrs is set to value RtpFalse. Use Option 3 to set the value for RTP parameter **Srx/Sip/AuthTraverseViaHdrs** to value **RtpFalse**, if it is currently set to **RtpTrue**.

17.3.4.4 Securing Media Servers

Media Servers communicate via the MGCP protocol which only supports the UDP transport type.

Securing MGCP Signaling	
Subcomponent	Media Servers
Settings	Secure Media Servers with IPsec.
Description	See Section 19.3, “Configuring IPSec for MGCP Connections”, on page 682.

17.3.4.5 Securing CSTA Applications

CSTA Applications only support the TCP transport type.

Securing CSTA Signaling	
Subcomponent	CSTA Applications
Settings	Secure CSTA Applications with IPsec.
Description	See Section 19.2, “Configuring IPSec for CSTA Connections”, on page 673.

17.3.5 Securing the Billing Interface

Billing files can be pushed or pulled, securely by OpenScape Voice to a billing server or from a billing client. The transfer of these files must be done using SFTP.

Securing Billing	
Subcomponent	Billing
Settings	Turn on SFTP for pushing billing files to a billing server. When a billing client pulls billing files from OpenScape Voice, it must be configured to set up an SFTP session using the "cdr" account’s credentials..
Description	Login to the Common Management Platform and navigate to: **Configuration > OpenScape Voice > Select switch > Administration > General Settings > CDR > General tab > Set the CDR Delivery Method to SPush > Enter username and password for Primary and possibly backup billing server > Save**

17.4 Used IP Ports

The IP ports used by the phones are described here. It can generally be noted that according to the SIP protocol, the phones send a REGISTER message with 'Contact' information about their IP address and port number. The OpenScape Voice sends SIP messages to the IP address / port number provided by the phones. Usually, these ports are 5060 (for UDP or TCP) or 5061 (for TLS), but can sometimes be configurable on the phones.

18 OpenScape Voice Signaling Stream Security

18.1 TLS Overview

Note: Certificate Management is fully documented in the following manual:

OpenScape Solution Set V10 Certificate Management and Transport Layer Security (TLS) Administration Guide

Note: TLS v1.2 is the default version supported in OpenScape Voice V11.

The TLS protocol allows applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS runs on OSI layers beneath application protocols such as HTTP, SOAP, and SIP, and above a reliable transport protocol-for example, TCP. It does not run over UDP.

Usually, only the server is authenticated using TLS - for example, its identity is ensured. The client is often authenticated using a method other than TLS. The end user (whether an individual phone, gateway, or application such as a Web browser) can be sure with whom it is communicating using TLS with unilateral server authentication.

In OpenScape Voice, phones use TLS to authenticate the OpenScape Voice server; the OpenScape Voice server authenticates the phones to using digest authentication.

As shown in Figure 12, the client always establishes the TLS session. After it is negotiated successfully, the OpenScape Voice server challenges it for a digest login, realm, and password. The connection is established by the phone on power-up; the TLS connection remains open after successful negotiation to avoid call setup times being delayed later.

The client sends *keep-alive* packets to the server to ensure that the server is still there. If a client is configured with the FQDN of a DNS-SRV record and it does not receive a response on the keep-alive packets, it will reconnect to the next server in its list of DNS-SRV servers for redundancy and failover purposes.

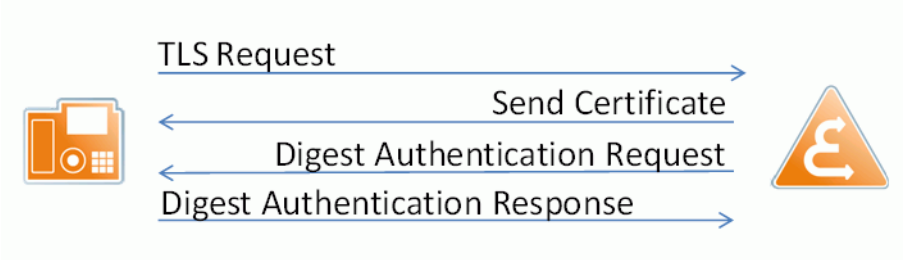


Figure 18 Authentication Between TLS Client and OpenScape Voice Server

On server-to-server interfaces, such as a SIP-Q connection between two OpenScape Voice servers, or between an OpenScape Voice server and a SIP gateway to the PSTN, a TLS connection with mutual authentication is used to bilaterally authenticate the connection in both directions. This means each machine can act as either a client or a server for the connection setup.

Figure 13 shows authentication between two OpenScape Voice servers. The TLS connection may be established from either side. Once established, a connection is usually reused. However, via configuration re-use of a TLS connection established by the peer may be turned off in favor of setting up a TLS connection towards the peer as well, ending up with a TLS connection in each direction.

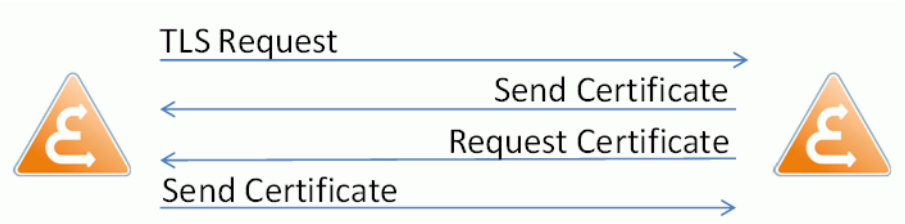


Figure 19 Mutual Authentication Between Two OpenScape Voice Servers

18.1.1 Endpoint Signaling

OpenScape Voice supports SIP signaling to endpoint devices and MGCP signaling to media servers.

OpenScape Voice supports digest authentication for all SIP endpoint devices in accordance with Internet Engineering Task Force (IETF) Request for Comment (RFC) 3261, *Session Initiation Protocol (SIP)*, June 2002. In addition, for SIP endpoint devices that use TCP instead of UDP, OpenScape Voice also supports secure SIP using TLS to protect the SIP signaling connection.

18.1.1.1 TLS Protection of Endpoint Device SIP Signaling

Using OpenScape Voice's back-to-back user agent architecture, TLS can be individually enabled or disabled on the SIP signaling connection between the OpenScape Voice SIP signaling manager and each SIP endpoint device.

Because TLS is applied on a hop-by-hop basis, end-to-end signaling security is only provided when all hops of the signaling connection use TLS or an equivalent security mechanism, such as IPsec for MGCP signaling connections.

End-to-end signaling security can be ensured in a customer's OpenScape Voice network by configuring security on all of the signaling interfaces. Also, when the SIPS uniform resource identifier (URI) is used by the originating endpoint device to specify the called party, the OpenScape Voice system blocks the call when signaling security is not available on every hop from the originating endpoint device to the last hop serving the terminating endpoint device within the same administrative domain. Signaling security cannot be guaranteed for calls that leave the administrative domain of the customer's OpenScape Voice network.

A server-side certificate is used on OpenScape Voice to permit the SIP endpoint device to authenticate OpenScape Voice when the endpoint device establishes its TLS connection to the OpenScape Voice SIP signaling manager or when the SIP endpoint device requests a client certificate after OpenScape Voice opens a TLS connection to a SIP endpoint device that supports mutual TLS authentication. OpenScape Voice authentication of a SIP endpoint device that does not support mutual authentication is provided by applying SIP digest authentication after the SIP endpoint device registers with OpenScape Voice.

Warning: OpenScape Voice complies with the TLS security mechanism as defined in *IETF RFC 3261 for SIP,* including *Section 26.3.2.1*, which requires the SIP server to reuse the TLS connection that is established by the SIP endpoint device.

Therefore, use of TLS for SIP signaling requires a persistent (full-time) signaling connection be established between OpenScape Voice and the SIP endpoint device.

IETF RFC 3261 does not require SIP endpoint devices to support TLS server functionality; for those SIP endpoint devices that do not support TLS server functionality such as SIP phones, the TLS connection must always be established from the SIP endpoint device to OpenScape Voice. It is not possible for OpenScape Voice to reestablish the TLS connection toward the SIP endpoint device if it fails. Therefore, the responsibility to keep the TLS connection open and to re-establish the connection if it fails rests solely with the SIP endpoint device. If the TLS connection fails, OpenScape Voice cannot deliver SIP messages to the SIP endpoint device, for example, it cannot deliver an incoming call to the SIP endpoint device.

It is the responsibility of the TLS client (the SIP endpoint device) to detect and recover the TLS connection whenever it fails. Therefore, the SIP endpoint device must monitor the TLS connection to detect a loss of signaling communication with the OpenScape Voice server.

OpenScape Voice supports a rapid recovery mechanism for TLS connections. This mechanism is only supported for SIP endpoints that also support initiating this mechanism.

The rapid recovery mechanism is based on a frequent connectivity check (*keep-alive message)* the SIP endpoint device sends to OpenScape Voice. The interval of the connectivity check is provisioned in the SIP endpoint device. The connectivity check is successful if the SIP endpoint device receives back the identical message that was sent within five seconds.

The OpenScape Voice server responds to the *keep-alive message* whenever it is received. If the SIP endpoint fails to receive the response within five seconds, it repeats the keep-alive message. If a response is still not received after the number of attempts indicated by the specific phone device, the SIP endpoint device considers the TLS connection to be failed and establishes a new TLS connection.

To allow the SIP endpoint devices that support rapid recovery of TLS connections to determine when it is connected to an OpenScape Voice version that also supports this mechanism, OpenScape Voice includes a server version in its response to the SIP REGISTER message. The following conditions must be present:

- The SIP signaling manager must be provisioned to include the server version in its response to the SIP REGISTER messages. Refer to the *OpenScape Voice Configuration Manual: Volume 2, Configuration and Administration Using CMP and Assistant Plug-Ins*.
- The SIP REGISTER message from a SIP endpoint device must be received on a TLS connection. The OpenScape Voice server does not provide the server version when the SIP REGISTER message is received on UDP or TCP without TLS.

18.1.1.2 TLS Protection of SIP and SIP-Q Server Signaling

TLS can be used to protect SIP and SIP-Q signaling interfaces between network servers. Examples of where TLS may be used include the following:

- OpenScape Voice-to-OpenScape Voice interfaces
- OpenScape Voice-to-RG 8700 interfaces (when supported by the RG 8700)
- SIP-Q to HiPath 3000 and HiPath 4000

Mutual authentication within TLS (MTLS) is supported for SIP and SIP-Q server connections. When MTLS is used, both OpenScape Voice and the remote SIP or SIP-Q server can do the following:

- Act as either a TLS client or a TLS server; either side can set up or re-establish a TLS session.
- Authenticate each other using certificates. This is different from the use of TLS with SIP subscriber devices (refer to Section 18.1.1.1, “TLS Protection of Endpoint Device SIP Signaling”, on page 653) which, in accordance with IETF RFC 3261, uses digest authentication for authentication of the client to OpenScape Voice.

18.1.2 Sample Connection Call Flows

Figure 20 on page 656 provides an example of a simple connection one-way TLS example, including a full handshake:

1. A client sends a **ClientHello** message specifying the highest TLS protocol version it supports, a random number, a list of suggested cipher suites and compression methods.
2. The server responds with a **ServerHello** message, containing the chosen protocol version, a random number, cipher suite, and compression method from the choices offered by the client. The server may also send a session id as part of the message to perform a resumed handshake.
3. The server sends its **Certificate** message.
4. The server sends a **ServerHelloDone** message, indicating it is done with handshake negotiation.
5. The client responds with a **ClientKeyExchange** message, which may contain a PreMasterSecret, public key, or nothing. (Again, this depends on the selected cipher.)
6. The client and server use the random numbers and PreMasterSecret to compute a common secret, known as the *master secret*. All other key data for this connection is derived from this master secret and the client- and server-generated random values, which is passed through a carefully designed pseudo-random function.
7. The client sends a **ChangeCipherSpec** record, essentially telling the server, "Everything I tell you from now on will be encrypted."
8. The client sends an encrypted **Finished** message, containing a hash and MAC over the previous handshake messages.
9. The server attempts to decrypt the client's Finished message, and verify the hash and MAC. If the decryption or verification fails, the handshake is considered to have failed and the connection is torn down.

10. The server sends a **ChangeCipherSpec** and its encrypted **Finished** message, and the client performs the same decryption and verification.

At this point, the TLS connection is established and the application protocol is enabled. Application messages exchanged between client and server will be encrypted.

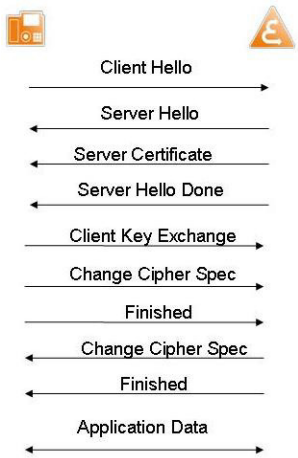


Figure 20 Sample TLS Connection Call Flow

Figure 21 on page 657 provides an example of a client being authenticated using TLS with mutual authentication (MTLS):

1. A client sends a **ClientHello** message specifying the highest TLS protocol version it supports, a random number, a list of suggested cipher suites and compression methods.
2. The server responds with a **ServerHello** message, containing the chosen protocol version, a random number, cipher suite, and compression method from the choices offered by the client. The server may also send a session id as part of the message to perform a resumed handshake.
3. The server sends its **ServerCertificate** message.
4. The server requests a certificate from the client, so that the connection can be mutually authenticated, using a **CertificateRequest** message.
5. The server sends a **ServerHelloDone** message, indicating it is done with handshake negotiation.
6. The client responds with a **Certificate** message, which contains the client's certificate.
7. The client sends a **ClientKeyExchange** message, which may contain a PreMasterSecret, public key, or nothing. (Again, this depends on the selected cipher.) This PreMasterSecret is encrypted using the public key of the server certificate.

8. The client sends a **CertificateVerify** message, which is a signature over the previous handshake messages using the client's certificate's private key. This signature can be verified by using the client's certificate's public key. This lets the server know that the client has access to the private key of the certificate and thus owns the certificate.
9. The client and server use the random numbers and PreMasterSecret to compute the master secret. All other key data for this connection is derived from this master secret (and the client- and server-generated random values), which is passed through a carefully designed pseudo-random function.
10. The client sends a **ChangeCipherSpec** record, essentially telling the server, "Everything I tell you from now on will be encrypted."
11. Finally, the client sends an encrypted **Finished** message, containing a hash and MAC over the previous handshake messages.
12. The server attempts to decrypt the client's **Finished** message, and verify the hash and MAC. If the decryption or verification fails, the handshake is considered to have failed and the connection should be torn down.
13. Finally, the server sends a **ChangeCipherSpec** and its encrypted **Finished** message, and the client performs the same decryption and verification.

At this point, the MTLS connection is established and the application protocol is enabled. Application messages exchanged between client and server will be encrypted.

Figure 21 Sample Mutual TLS Connection Call Flow

18.1.3 OpenScape Voice Platform Signaling Managers

This section describes the concept of primary and backup signaling managers as it exists on the OpenScape Voice platform. These concepts are useful in understanding the practical DNS examples presented elsewhere in this chapter.

As shown in Figure 22 below:

- When establishing a unilaterally (server) authenticated TLS connection-for example, a SIP phone-the connection is made to one of the IP addresses of the SIP signaling manager (SIPSM). Each node has its own SIP signaling manager. In addition, each signaling manager has a secondary instance on the other node, in case one node was to go down. In a co-located scenario, this avoids the need for all non-TLS SIP endpoint devices to re-register on the partner node after node failover due to an outage of the node with which they are currently registered. The secondary signaling manager on each node shares all the registration credentials that the primary signaling manager recorded as the phones registered. TLS SIP endpoint devices always need to re-register on the partner node after an outage of the node with which they are currently registered.
- When establishing a TLS connection with mutual authentication for server-to-server interworking, for example, SIP Trunks, a different set of IP addresses is used. These IP addresses exclusively handle mutual TLS connections and cannot handle unilateral TLS connections, such as those from SIP phones. Similarly, the IP addresses associated with unilateral TLS cannot handle mutual TLS connection attempts.

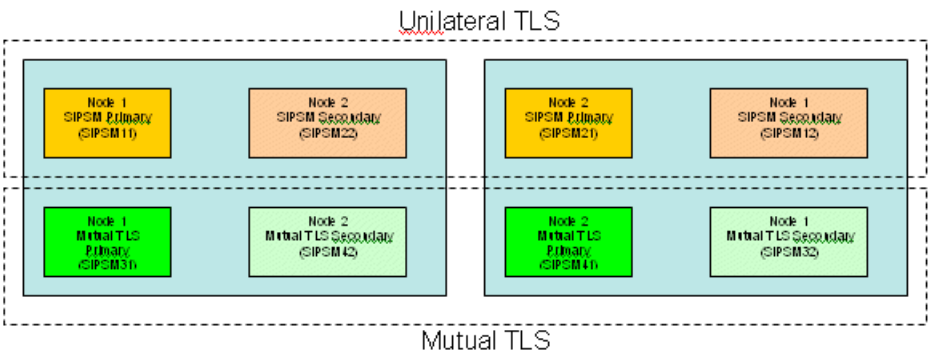


Figure 22 Signaling Managers Used in Unilateral and Mutual TLS Connections

18.1.4 DNS Survivability Overview

An SRV record or Service record is a category of data in the Internet Domain Name System specifying information on available services. It is defined in RFC 2782, *A DNS RR for Specifying the Location of Services (DNS SRV)*. Newer Internet protocols such as SIP often require SRV support from clients.

The remainder of this section describes the problem DNS-SRV solves.

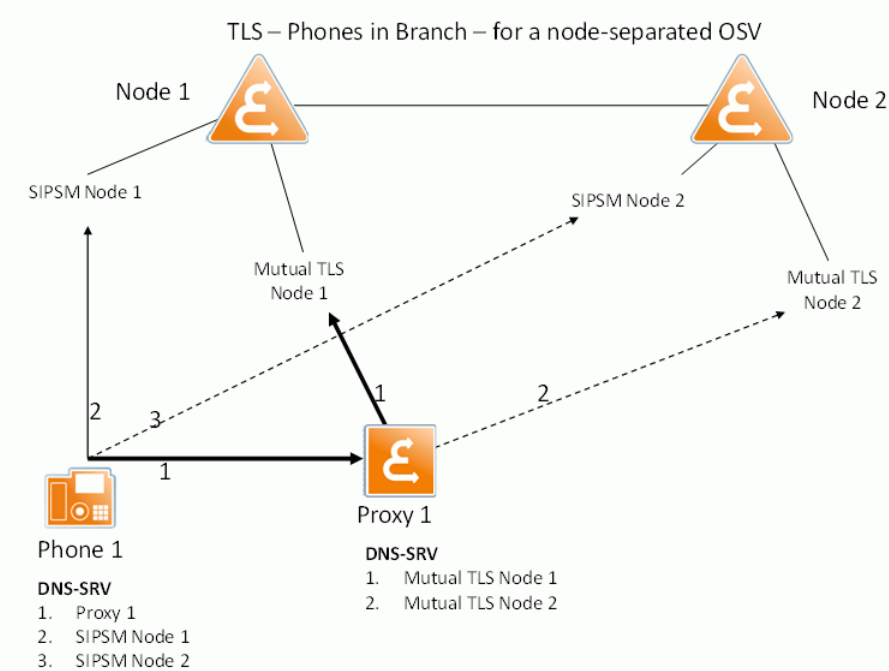


Figure 23 TLS- Phones in Branch - for a Node-Separated OSV

Assuming an endpoint device in a branch office can obtain service from the local branch office proxy or from the OpenScape Voice server directly (Figure 17), an automated flexible method is required that enables the endpoint device to determine this configuration as part of the boot-up process. The concept of DNS-SRV provides this ability.

If the configuration were to be statically configured within the phone, the phone could not be moved from location to location without a Move, Add or Change (MAC) being done manually. This does not fit with the idea of being available on any device, anywhere, any time with the same one number service.

An SRV record has the form:

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

- **Service**: the symbolic name of the desired service, for example, SIP or SIPS.
- **Proto**: the protocol of the desired service; this is usually either TCP or UDP.

- **Name**: the domain name for which this record is valid.
- **TTL**: standard DNS time-to-live.
- **Class**: standard DNS class (this is always IN).
- **Priority**: the priority of the target host, with lower values having higher priority.
- **Weight**: A relative weight for records with the same priority.
- **Port**: the TLS, TCP or UDP port on which the service is to be found.
- **Target**: the canonical host name of the machine providing the service.

An example SRV record might look like this:

```
_sip._udp.example.com. 86400 IN SRV 0 5 5060 sipserver.example.com.
```

This SRV record points to a server named sipserver.example.com listening on UDP port 5060 for SIP protocol connections. The priority given here is 0, and the weight is 5.

As with PTR records, SRV records must point to the canonical name of the host. Aliases or CNAMEs cannot be used as valid targets.

Note: When you want to configure SIP UAs, configure the DNS SRV name you entered on the sip server and sip registrar address on the phone. For more information on SIP DNS SRV parameters, see Section "How to Configure parameters for SIP FQDN (Fully Qualified Domain Name) Support" in *OpenScape Voice, Administrator Documentation.*

18.1.5 High Availability with SRV

The Priority field is similar to an MX record's priority value. Clients always use the SRV record with the lowest-numbered priority value first, and only fall back to other records if the connection with this record's host fails. Thus a service may have a designated fallback server, used only if the primary server fails. Only another SRV record, with a priority field value higher than the primary server's record, is needed.

If a service has multiple SRV records with the same priority value, clients use the Weight field to determine which host to use. The weight value is relevant only in relation to other weight values for the service, and only among records with the same priority value. OpenScape Voice does not use weights to perform load balancing.

If we consider our original problem, a solution would appear as follows:

```
_sips._tcp.example.com. 86400 IN SRV 10 10 5070 proxy1.example.com.
```

```
_sips._tcp.example.com. 86400 IN SRV 20 10 5070 osv1.example.com.
_sips._tcp.example.com. 86400 IN SRV 30 10 5070 osv2.example.com.
```

Because proxy1 has the highest priority (lowest number), phones firstly register with it. If the proxy is unavailable, the record with the next highest priority value is chosen, which is osv1.example.com. This is the primary SIPSM of node 1 of the OpenScape Voice server in the data center. If it is down for maintenance, the phone connects with osv2, which is the secondary SIPSM of node 2 of the cluster.

Note: The load balancing provided by SRV records is inherently limited, since the information is essentially static; current load of servers is not taken into account. For that reason, its use is not recommended.

After the branch office proxy comes back online, the phones detect this (as they recheck its availability periodically) and automatically switch back to using the proxy. This is an advantage over configuring classic A-Records.

18.1.5.1 Simple Example Including DNS Server

In the following example, assume that no branch offices are present; the phones connect directly to the OpenScape Voice server. In this example, a customer may require the capability to use DNS-SRV to connect both UDP, TCP, and TLS devices. Depending on which protocol they support, they must be connected to different IP addresses or ports.

```
;;;; NAPTR records for sip services
; order pref flags service regexp replacement
IN NAPTR 50 50 "s" "SIPS+D2T" "" _sips._tcp.example.com.
IN NAPTR 90 50 "s" "SIP+D2T" "" _sip._tcp.example.com.
IN NAPTR 100 50 "s" "SIP+D2U" "" _sip._udp.example.com.
;;;; SRV records for each sip service
;; Priority Weight Port Target
_sips._tcp.bocb.siemens.com SRV 10 1 5061 osv1.example.com.
SRV 20 1 5061 osv2.example.com.
_sip._tcp.bocb.siemens.com SRV 10 1 5060 osv1.example.com.
SRV 20 1 5060 osv2.example.com.
_sip._udp.bocb.siemens.com SRV 10 1 5060 osv1.example.com.
SRV 20 1 5060 osv2.example.com.
;;;; A records for the contacts mentioned in SRV records
osv1 IN A 1.2.3.4 ;; sip-sm OSV node1
osv2 IN A 1.2.3.5 ;; sip-sm OSV node2
```

```
;;;; PTR records for reverse lookup of the contacts mentioned in SRV records

4.3.2.1.in-addr.arpa. 3570 IN PTR osv1.example.com.

5.3.2.1.in-addr.arpa. 3570 IN PTR osv2.example.com.
```

After it is installed, the following commands can be used to test the record:

- To return the DNS names of the nodes and the port number offering UDP service:

  ```
  host -t srv _sip._udp.example.com
  ```

- To return the DNS names of the nodes and the port number offering TCP service:

  ```
  host -t srv _sip._tcp.example.com
  ```

- To return the DNS names of the nodes and the port number offering TCP service:

  ```
  host -t srv _sips._tcp.example.com
  ```

18.1.6 Interaction of DNS-SRV and TLS

By default, the contents of the TLS certificates are not checked after the TLS handshake is complete. However, the certificates' contents will be checked if the RTP system parameter **Srx/ttud/verification** is set to **RtpTrue**. The information contained in a certificate (Figure 24 and Figure 25) can be viewed by opening any of the certificates that come preinstalled on any web browser.

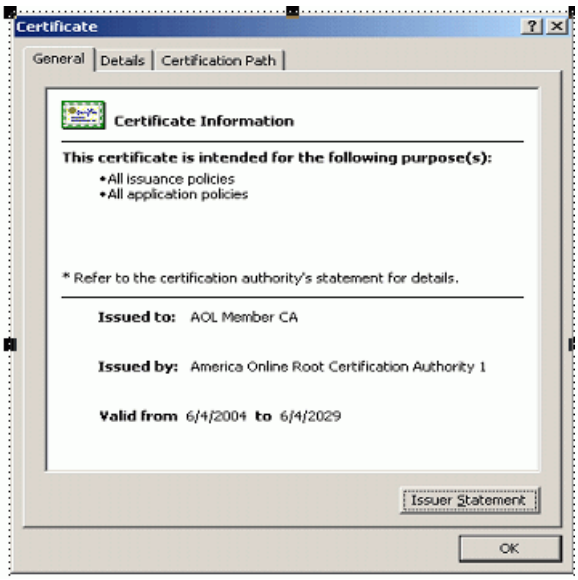


Figure 24 TLS Certificate Example-General Properties

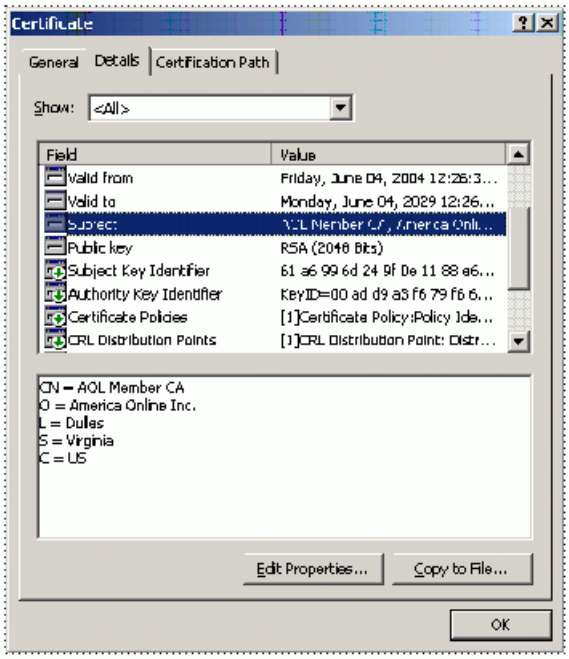


Figure 25 TLS Certificate Example - Details

The following are particularly important fields that are checked:

- **Valid From and Valid To**: Checking these fields verifies that the certificate is currently valid and not out of date.
- **SubjectAlternativeName (SAN) or CommonName (CN)**: Contains the name or the IP address of the certificate owner.

By comparing the IP address that sent the certificate as part of establishing a TLS connection with the IP address (possibly resolved using DNS) of the SubjectAlternativeName or Subject CommonName field, it can be verified that the certificate issued for that server really came from that server. If it does not match, the TLS connection is rejected and torn down.

In the previous example shown in Figure 23 on page 659 with a branch office proxy and a duplex OpenScape Voice cluster, it is necessary to ensure that the contents of the server certificate are correct or the certificates will be rejected after the post-connection check takes place. However, the CommonName field can only contain one DNS name or IP address, which does not match with the concept of DNS-SRV. Therefore, certificates use a concept of SubjectAlternativeName, which can be used instead of a single CommonName to identify the accepted source of service.

The SubjectAlternativeName fields of a certificate can be as long a list as is required for the solution at hand, and can contain DNS names, IP addresses, or a combination of both. It should also contain the FQDN of the server system it

belongs to. If a SubjectAlternativeName is found in a received certificate, the Subject CommonName field is ignored and no longer evaluated as part of the post-connection check mechanism.

The following sections, which provide examples of DNS-SRV and TLS certificate content, illustrate what is required in which scenario.

18.1.6.1 Example 1

In this example (Figure 20):

- No proxy is present.
- Phones are directly connected to OpenScape Voice, with both nodes in the same subnet.

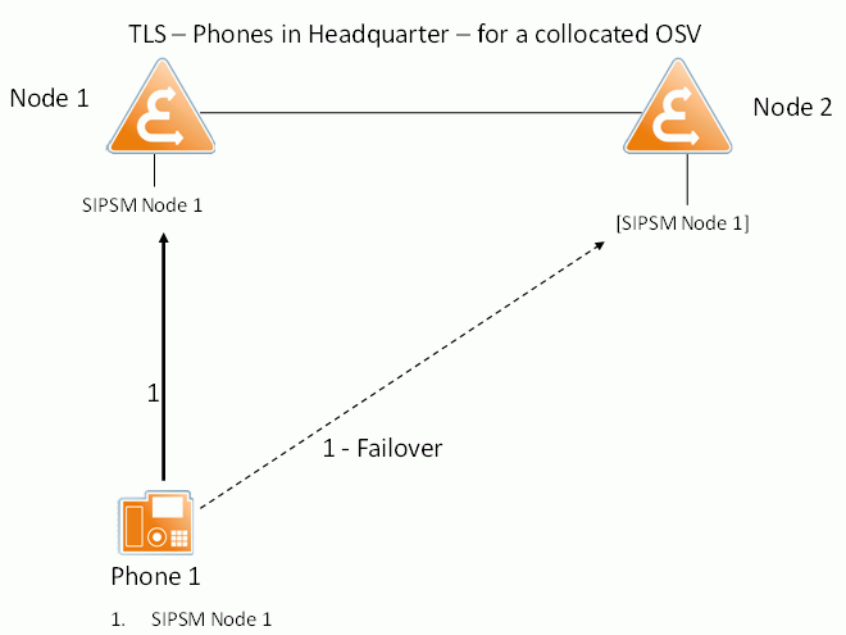


Figure 26 TLS - Phones in Headquarter for a Collocated System

In this case, the phones do not need to use DNS-SRV because they always connect to the SIPSM Node 1 address. In case of failover of a collocated OSV cluster, the IP address of the failed node appears on the surviving node. Therefore the certificate can be made to have just one CommonName, which would have the name osv1.example.com. If the primary node goes down, this IP address is taken over by the secondary node's backup signaling manager. Thus the CN field would still resolve to the IP address that communication is being established with.

18.1.6.2 Example 2

In this example (Figure 27):

- A local proxy is present.
- Phones are connected to a collocated OpenScape Voice cluster using the proxy. The same is valid for a geo-separated cluster that uses the same subnets for each data center.
- If the proxy fails, the phones register to Node 1 for service.

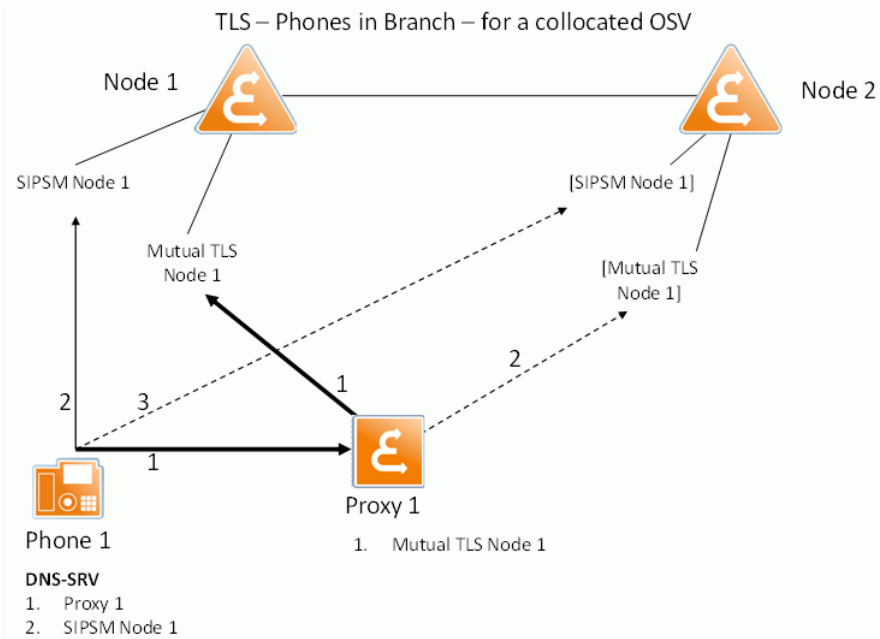


Figure 27 TLS-Phones in Branch for a Collocated System

In this case, the phone normally registers via the local proxy for service. If the proxy goes down, the phones register directly with SIPSM of Node 1 for service. Therefore one CommonName for the Subject field is not adequate; instead, the SubjectAlternativeName fields are used in combination with the correct DNS-SRV record:

```
_sips._tcp.proxy1.example.com. 86400 IN SRV 10 10 5070 proxy1.example.com.
_sips._tcp.proxy1.example.com. 86400 IN SRV 20 10 5070 osv1.example.com.
```

The corresponding certificate sent by proxy1 would contain:

```
X509v3 Subject Alternative Name:

DNS:proxy1.example.com
```

The DNS SRV records for a different branch office would look similar to the records of branch1 but its proxy name would be slightly different:

```
_sips._tcp.proxy2.example.com. 86400 IN SRV 10 10 5070 proxy2.example.com.
_sips._tcp.proxy2.example.com. 86400 IN SRV 20 10 5070 osv1.example.com.
```

The corresponding certificate sent by node1 would contain:

```
X509v3 Subject Alternative Name:

DNS:osv1.example.com
```

18.1.6.3 Example 3

In this example (Figure 28):

- No proxy is present.
- Phones are registered to a two-node redundant OpenScape Voice system with each node being in a different subnet.

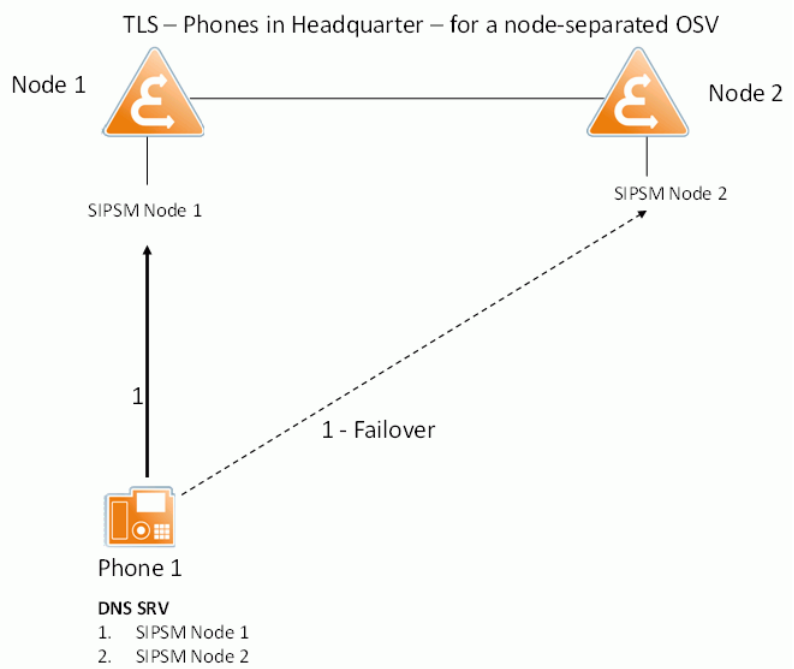


Figure 28 TLS - Phones in Headquarter for a Node Separated System

In this case, the phones register with the primary signaling manager on node 1 for service. If that node goes down, the phones switch to the primary signaling manager on node 2.

```
_sips._tcp.example.com. 86400 IN SRV 10 10 5070 osv1.example.com.
_sips._tcp.example.com. 86400 IN SRV 20 10 5070 osv2.example.com.
```

The corresponding certificate sent by node2 would contain:

```
X509v3 Subject Alternative Name:
DNS:osv1.example.com, DNS:osv2.example.com
```

18.1.6.4 Example 4

In this example (Figure 29):

- A local proxy is present.
- Phones are connected to OpenScape Voice using the proxy, with both nodes in different subnets.
- If the proxy fails, the phones register to the primary node for service.
- If the primary node is down, the phones register with the backup signaling manager on node 2.

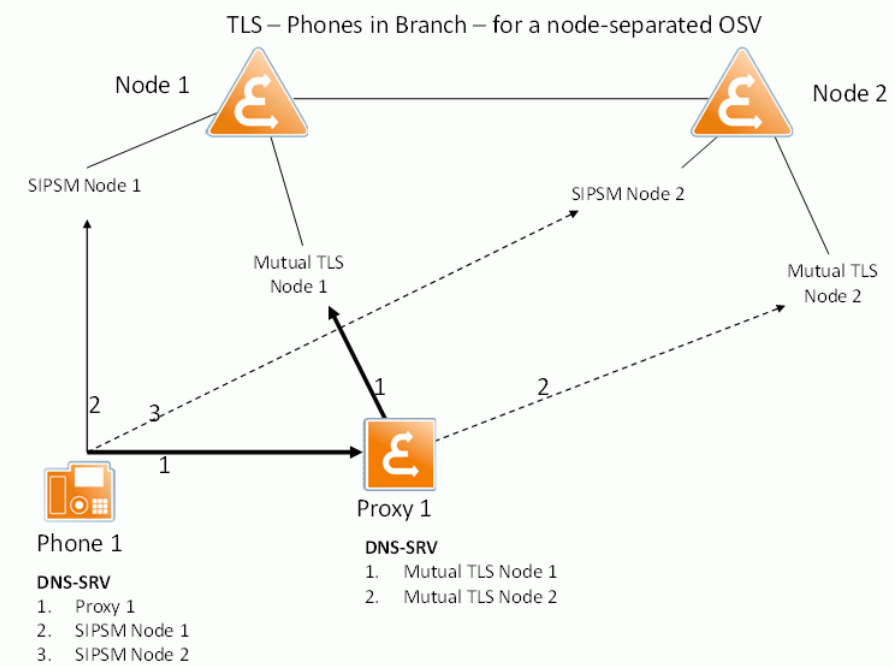


Figure 29 TLS-Phones in Branch for a Node-Separated System

In this case, the phones normally register to the local proxy for service. If the proxy goes down, the phones register directly with SIPSM node 1 for service. If that node is unavailable as well, the phones register to SIPSM node 2. Therefore one CommonName will not be adequate; instead, the SubjectAlternativeName fields are used in combination with the correct DNSSRV record:

```
_sips._tcp.example.com. 86400 IN SRV 10 10 5070 proxy1.example.com.
_sips._tcp.example.com. 86400 IN SRV 20 10 5070 osv1.example.com.
_sips._tcp.example.com. 86400 IN SRV 30 10 5070 osv2.example.com
```

The corresponding certificate sent by proxy1 would contain:

```
X509v3 Subject Alternative Name:
DNS:proxy1.example.com
```

The DNS SRV records for a different branch office would look similar to the records of branch1 but its proxy name would be slightly different:

```
_sips._tcp.example.com. 86400 IN SRV 10 10 5070 proxy2.example.com.
_sips._tcp.example.com. 86400 IN SRV 20 10 5070 osv1.example.com.
_sips._tcp.example.com. 86400 IN SRV 30 10 5070 osv2.example.com.
```

The corresponding certificate sent by node1 would contain:

```
X509v3 Subject Alternative Name:
DNS:osv1.example.com, DNS:osv2.example.com
```

18.1.7 Practical Deployment Recommendations

OpenScape Voice can be the target of a server authenticated TLS connection and the target or originator of a mutually authenticated TLS connection. Though it is possible to generate different server and/or client TLS certificates for any of these 3 types of TLS connections, it is recommended to use the same device certificate for all signaling TLS connections. It is recommended to create a different administration TLS certificate in case the administration and signaling networks are separated.

In Figure 30, the connections in bold red are mutual TLS connections and all others are unilateral TLS connections. The certificate on both nodes of a dual-node (collocated) cluster contains the IP addresses of the SIP signaling managers of both nodes of the cluster. For a geo-separated cluster, a device certificate should be issued for each node of the cluster with each device certificate only listing the IP addresses of the own node in the SubjectAlternativeName extension field.

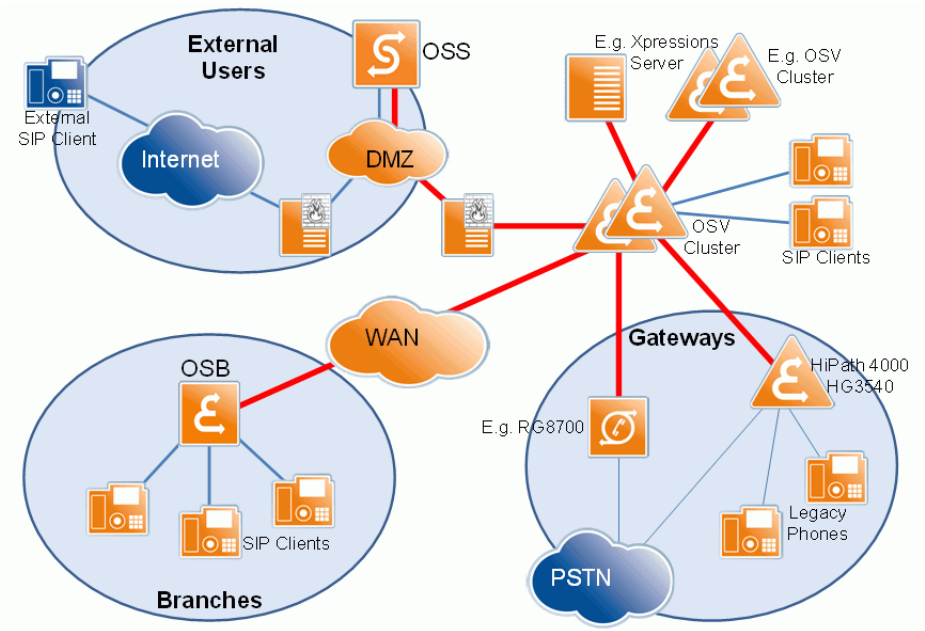


Figure 30 Deployment Recommendations

18.2 Client (Endpoint) Authentication

SIP digest authentication is enabled or disabled on OpenScape Voice using provisioning of SIP signaling manager options. It is recommended that SIP digest authentication be enabled during system installation. Refer also to Section 18.3, “Media Server Signaling”.

Weak or short SIP passwords can be easily cracked by currently available hacker tools. OpenScape Voice supports SIP passwords of up to 20 characters. It is recommended that SIP passwords be of at least 8 characters and contain a mix of uppercase, lowercase, numeric characters, and special characters. Dictionary words or purely numeric SIP passwords should be avoided.

18.3 Media Server Signaling

OpenScape Voice supports IPsec with IKE and pre-shared keys for MGCP signaling interfaces.

19 IPSec Configuration

This chapter provides information about the following topics:

- Using IPSec
- Configuring IPSec for CSTA Connections
- Configuring IPSec for MGCP Connections

19.1 Using IPSec

During operation, OpenScape UC Application and OpenScape Voice exchange sensitive data using the MGCP and CSTA protocols. Always make sure to protect such data from unauthorized access.

The most simple way to achieve this is operating all involved systems in a common, protected sub-network. This is in particular possible for Integrated Simplex.

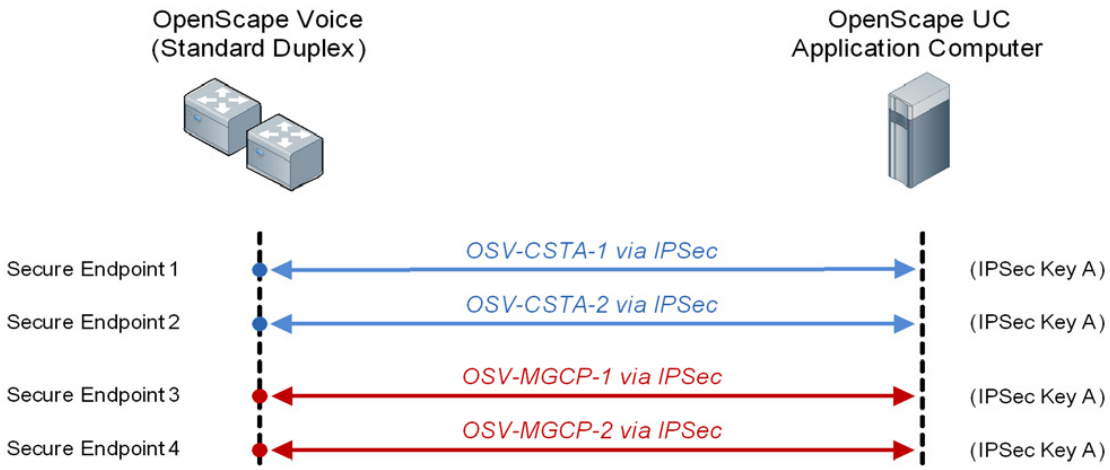
If you operate the various system components in different or even unprotected sub-networks, communication between these components must be encrypted. We recommend IPSec for this purpose. This protocol establishes connection tunnels between the involved systems. Data transmitted through such a connection tunnel is encrypted by IPSec and consequently protected from unauthorized access.

To use IPSec tunnels in OpenScape Voice, a so-called secure end point is configured there for each tunnel. A target system and an IPSec key is assigned to such an end point.

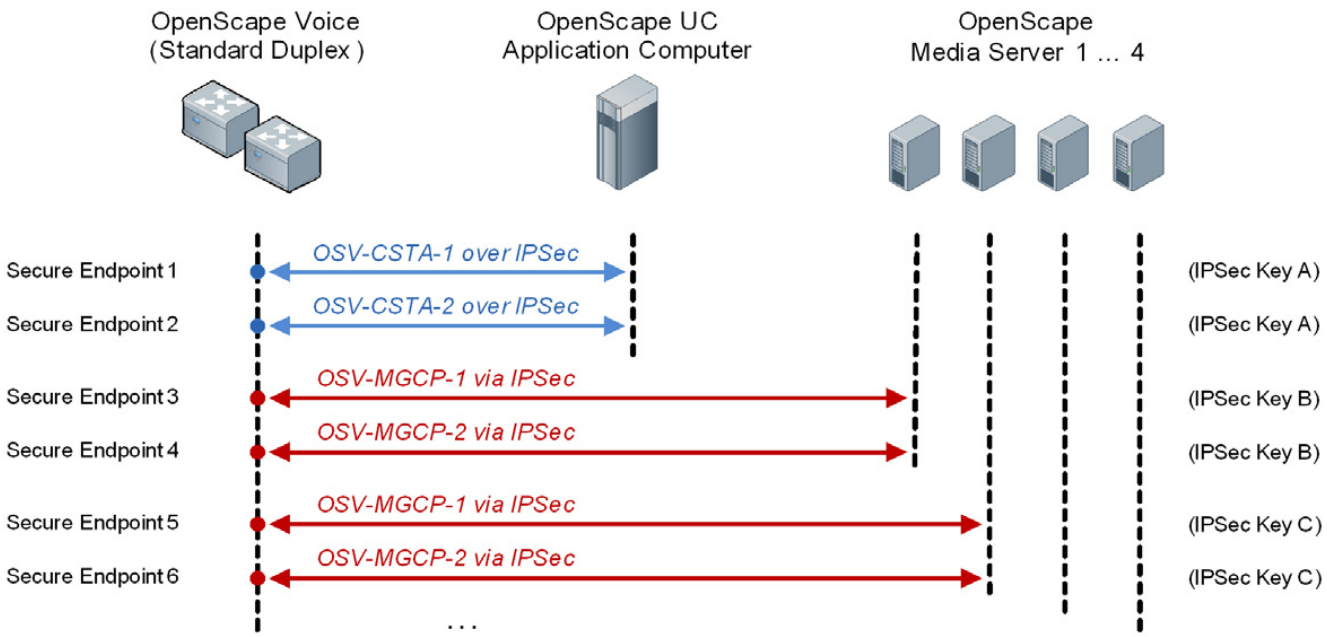
NOTE: If OpenScape Voice is to use several IPSec tunnels to a common target system, the same key must be configured in OpenScape Voice for the associated secure end points.

The computer systems of OpenScape UC Application are configured for IPSec with the help of a configuration file.

Using IPSec for OpenScape UC Application – Standard Duplex (small)



Using IPSec for OpenScape UC Application – Standard Duplex (large)



19.2 Configuring IPSec for CSTA Connections

You need to execute the following configuration steps for encrypting the CSTA connections between OpenScape UC Application and OpenScape Voice using IPSec.

- Configuring OpenScape Voice for IPSec-based CSTA Connections
- Configuring OpenScape UC Application for IPSec-based CSTA Connections

NOTE: From V8 and later versions, CSTA connections can be made over TLS to the OSV.

19.2.1 Configuring OpenScape Voice for IPSec-based CSTA Connections

Encrypting the CSTA communication between OpenScape Voice and OpenScape UC Application by IPSec requires configuring IPSec in OpenScape Voice.

NOTE: You need to execute the configuration steps for OpenScape Voice (Standard Duplex) on one of the two system nodes only. All settings are automatically transmitted from the configured system node to the second system node.

Start the configuration

How to configure IPSec for OpenScape Voice:

1. Start the RTP Command Line Interface (startCLI) on one of the OpenScape Voice (Standard Duplex) nodes and log in there as **sysad**.
2. Select:

   Main Menu >
   Application-level Management >
   Network Element Security Management >
   Secure End Point Device Security Management

3. Create a secure end point for the IP address of the first CSTA interface of OpenScape Voice.

   Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the CSTA Endpoint>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP Addr. of the UC application computer>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): <csta_ip_alias_1>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 1
Key Length in Bytes (default: 16):
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

NOTE: If you do not specify an IP address but the associated fully qualified host name under `Local Host`, you need not modify the IPSec configuration in the event that the IP address of the relevant interface changes at a later date.
The fully qualified host names for CSTA are defined for OpenScape Voice in `/etc/hosts`. They read by default **csta_ip_alias_1** and **csta_ip_alias_2**.

4. Determine the key used for the tunnel of the first CSTA interface. To do so, display the settings of the just created end point as shown in the following example.

   Example:

```
Selection (default: 3): 4
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <name of the created CSTA end point>
Do you want to execute this action? <y/n> (default: yes): y
Total Number of SecEndPts Retrieved : 1
Name: Ext_Asst
Description:
FQDN:
Remote IP Address: <Ext_Asst_IP_Address>
Remote NetMask: 255.255.255.255
Remote Port : 0
Local Host: bond_node_alias
Local Port: 0
IPsec Profile: IPSEC_ESP_SHA_AES
IKE Profile: IKE_SHA2_AES
Key Gen Method: Automatic
Key Type: Hex
Key Length: 16

Key: 7aa88aecd7f40699884b75795fbf9354
```

5. Note down the **Key:** output.

6. Create a secure end point for the second CSTA interface of OpenScape Voice. Because the relevant IPSec tunnel will later lead to the same application computer as for the first end point, you need to use the same key – the one you just noted down. Proceed as shown in the following example:

   Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the CSTA Endpoint>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP Addr. of the UC application computer>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): <csta_ip_alias_2>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 2
Key Length in Bytes (default: 16): <key of the first CSTA Endpoint>
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

You have now configured IPSec for the CSTA connection in OpenScape Voice.

19.2.2 Configuring OpenScape UC Application for IPSec-based CSTA Connections

Encrypting the CSTA communication between OpenScape Voice and OpenScape UC Application by IPSec requires configuring IPSec on the application computer of OpenScape UC Application.

The RPM `strongSwan` must be installed and configured on the relevant computer system for this purpose. This RPM is already contained in the SLES repository of every UC Application system.

Start the configuration

How to configure IPSec for the application computer:

1. Place the SLES DVD in the application computer drive.
2. If you have not integrated the SLES DVD as additional installation source yet, do this now via the `zypper ar` command.
3. Execute the following command to install the RPM `strongSwan`:

   ```
   zypper in strongSwan
   ```

4. Open the following configuration file in a text editor:

   ```
   /etc/ipsec.conf
   ```

5. In the `Add connections here` section, define an IPsec connection for each CSTA end point you have configured in OpenScape Voice.

   In doing so, use the following format:

```
conn <unique connection name>
        keyexchange=ikev1
        left=<IP addr. of the CSTA interface of OpenScape Voice>
        right=<IP addr. of the UC application computer>
        leftprotoport=%any/%any
        rightprotoport=%any/%any
        leftfirewall=no
        auto=start
        authby=secret
        keylife=24m
        ikelifetime=1h
        dpddelay=5
        dpdtimeout=3
        dpdaction=restart
        type=transport
        ike=3des-sha-modp1024
        esp=3des-sha-modp2048
```

6. Save the changes in the configuration file.

7. Open the following configuration file in a text editor:

   `/etc/ipsec.secrets`

8. At the end of the configuration file, define the key to be used for encrypting the CSTA data. This is the key you noted down during the IPsec configuration of OpenScape Voice.

   In doing so, use the following format:

```
<IP addr. of the UC Application computer> <IP addr. of the CSTA interface of OpenScape Voice> : PSK 0x<key>
```

   Example:

```
10.235.85.20 10.235.98.58 : PSK 0xc3daff51c40778fe2a92f31ecb93e653
10.235.85.20 10.235.98.59 : PSK 0xc3daff51c40778fe2a92f31ecb93e653
```

NOTE: Both CSTA interfaces of OpenScape Voice (`10.235.98.58/59`) end on the same application computer (`10.235.85.20`). This is why the connections use the same key.

IMPORTANT: There must be a space between the IP-Address and the colon (":")

NOTE: Leave the configuration file otherwise unchanged.

---

9. Save the changes in the configuration file.
10. Open file `/etc/strongswan.conf`
11. Modify the file to include the following:

```
# strongswan.conf - strongSwan configuration file
charon
{
   # number of worker threads in charon
   threads = 16
   # plugins to load in charon
   # load = aes des sha1 md5 sha2 hmac gmp random pubkey
xcbc x509 stroke

  plugins {
     sql
     {
        # loglevel to log into sql database
        loglevel = -1
        # URI to the database
        # database = sqlite:///path/to/file.db
        # database = mysql://user:password@localhost/
database
     }

     duplicheck
     {
        # Enable duplicheck plugin (if loaded).
        # enable = yes
        enable = no

        # Whether to load the plugin. Can also be an
integer to increase the
        # priority of this plugin.
        load = no

        # Socket provided by the duplicheck plugin.
        # socket = unix${piddir}charon.dck
     }
  }
# filelog
# {
#    /log/ipsec.log
#    {
#       # add a timestamp prefix
#       time_format = %y%m%d-%H%M%S
#       # prepend connection name, simplifies grepping
#       ike_name = yes
#       # overwrite existing files
```

```
#       append = yes
#       # increase default loglevel for all daemon
#subsystems
#       default = 1
#       # flush each line to disk
#       flush_line = yes
#    }
# }

  stderr
  {
     # more detailed loglevel for a specific subsystem,
overriding the
     # default loglevel.
     ike = -1
     knl = -1
     enc = -1
     net = -1
  }
  # ...
  syslog {
    # prefix for each log message
    identifier = charon
    # use default settings to log to the LOG_DAEMON
facility
    daemon {
      default = -1
      ike = -1
      enc = -1
      net = -1
    }
    # very minimalistic IKE auditing logs to LOG_AUTHPRIV
    auth {
      default = -1
      ike = -1
    }
  }
}
pluto
{
  # plugins to load in pluto
  # load = aes des sha1 md5 sha2 hmac gmp random pubkey
}
libstrongswan
{
  #  set to no, the DH exponent size is optimized
  #  dh_exponent_ansi_x9_42 = no
}
```

12. For customers updating from SLES11SP2, racoon logging in `/var/log/messages` has to be disabled by commenting the log entry in `/etc/racoon/racoon.conf`.

```
========================================
/etc/racoon/racoon.conf
#log debug2;
```

13. To start the IPsec service, execute the following command as `root` in a shell:

```
ipsec start
```

> ***NOTE:*** Every time you modify the IPSEC rules a new `ipsec restart` is necessary.
> With `ipsec status` or `ipsec statusall` you can check the active IPSEC Connections.

14. To have the IPsec service started automatically when the application computer reboots, execute the following command as `root` in a shell:

```
chkconfig ipsec on
```

> ***NOTE:*** In SLES 12 installations, IPSec can be enabled and started via the following commands:
> `systemctl enable strongswan.service`
> `systemctl start strongswan.service`
> `systemctl status strongswan.service`

15. To check whether the IPsec service works correctly, execute the following command in a shell:

```
tcpdump –i any | grep ESP
```

If OpenScape Voice and OpenScape UC Application communicate via CSTA, the shell should put out messages in the following format:

```
17:09:23.063745 IP 10.1.250.20 > adsa11n1: ESP(spi=0xfb1c7d52,seq=0x16)
17:09:23.064081 IP adsa11n1 > 10.1.250.20: ESP(spi=0x39281790,seq=0x16)
17:09:23.064086 IP adsa11n1 > 10.1.250.20: ESP(spi=0x39281790,seq=0x16)
```

IPsec is now operable for CSTA connections between OpenScape Voice and OpenScape UC Application.

19.3 Configuring IPSec for MGCP Connections

NOTE: You need to execute the configuration steps of this chapter only if you use the OpenScape Media Server of OpenScape UC Application also as Media Server Stand-alone) for OpenScape Voice.

The steps you execute to configure IPSec for MGCP connections depend on whether you use OpenScape UC Application as Standard Duplex (small) or Standard Duplex (large).

- Configuration for Standard Duplex (small)
- Configuration for Standard Duplex (large)

19.3.1 Configuration for Standard Duplex (small)

NOTE: You need to execute the configuration steps of this chapter only if you use Standard Duplex (small).

You need to execute the following configuration steps for encrypting the MGCP connections between OpenScape UC Application (Standard Duplex (small)) and OpenScape Voice using IPSec.

- Configuring OpenScape Voice for IPSec-based MGCP Connections (Standard Duplex (small))
- Configuring OpenScape UC Application for IPSec-based MGCP Connections (Standard Duplex (small))

19.3.1.1 Configuring OpenScape Voice for IPSec-based MGCP Connections (Standard Duplex (small))

Encrypting the MGCP communication between OpenScape Voice and the OpenScape Media Server by IPSec requires configuring IPSec in OpenScape Voice.

Start the configuration

How to configure IPSec for OpenScape Voice:

1. Start the RTP Command Line Interface (startCLI) on one of the OpenScape Voice (Standard Duplex) nodes and log in there as **sysad**.
2. Select:

   Main Menu >
   Application-level Management >
   Network Element Security Management >
   Secure End Point Device Security Management
3. Create a secure end point for the fully qualified host name of the first MGCP interface of OpenScape Voice.

   Because the relevant IPSec tunnel will later be set up to the application computer of OpenScape UC Application also, you need to use the same key as for the CSTA tunnels. Proceed as shown in the following example:

Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the MGCP Endpoint>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP addr. of the UC Application computer>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): ncs_ip_alias_1
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 2
Key Length in Bytes (default: 16): <key of the CSTA end points>
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

NOTE: If you do not specify an IP address but the associated fully qualified host name under `Local Host`, you need not modify the IPSec configuration in the event that the IP address of the relevant interface changes at a later date.
The fully qualified host names for MGCP are defined for OpenScape Voice in `/etc/hosts`. They read by default **ncs_ip_alias_1** and **ncs_ip_alias_2**.

---

4. Create a secure end point for the second MGCP interface of OpenScape Voice in the same way. But use the expression **ncs_ip_alias_2** instead of **ncs_ip_alias_1** under `Local Host`.

You have now configured IPSec for the MGCP connection in OpenScape Voice.

19.3.1.2 Configuring OpenScape UC Application for IPSec-based MGCP Connections (Standard Duplex (small))

Encrypting the MGCP communication between OpenScape Voice and OpenScape Media Server by IPSec requires configuring IPSec on the application computer of OpenScape UC Application.

The RPM `strongSwan` must be installed and configured on the relevant computer system for this purpose. This RPM is already contained in the SLES repository of the UC Application system.

Start the configuration

How to configure IPSec for the application computer:

1. Place the SLES DVD in the application computer drive.
2. If you have not integrated the SLES DVD as additional installation source yet, do this now via the `zypper ar` command.
3. Execute the following command to install the RPM `strongSwan`:

   `zypper in strongSwan`
4. Open the following configuration file in a text editor:

   `/etc/ipsec.conf`
5. Remove the following sections from the configuration file:
   - `default settings for connections`
   - `sample VPN connection`

IMPORTANT: **Do not** delete section `Disable Opportunistic Encryption`. The relevant computer system will otherwise lose its network connection as soon as IPSec starts.

---

6. In the `Add connections here` section, define an IPSec connection for each MGCP end point you have configured in OpenScape Voice.

   In doing so, use the following format:

```
conn <unique connection name>
        left=<IP addr. of the MGCP interface of OpenScape Voice>
        right=<IP addr. of the UC application computer>
        auto=start
        authby=secret
        pfs=no
        keylife=24m
        dpddelay=5
        dpdtimeout=3
        dpdaction=restart
        type=transport
```

7. Save the changes in the configuration file.
8. Open the following configuration file in a text editor:

   `/etc/ipsec.secrets`

9. At the end of the configuration file, define the key to be used for encrypting the MGCP data. This is the key you noted down during the IPSec configuration of OpenScape Voice.

   In doing so, use the following format:

```
<IP addr. of the application computer> <IP addr. of the MGCP interface of OpenScape Voice>: PSK 0x<key>
```

   Example:

```
10.235.85.22 10.235.98.60: PSK 0xc3daff51c40778fe2a92f31ecb93e653
10.235.85.22 10.235.98.61: PSK 0xc3daff51c40778fe2a92f31ecb93e653
```

NOTE: In the example, both MGCP connections of OpenScape Voice (`10.235.98.60/61`) end on the application computer (`10.235.85.22`). This is why the connections use the same key.

NOTE: Leave the configuration file otherwise unchanged.

---

10. Save the changes in the configuration file.
11. Open file `/etc/strongswan.conf`
12. Modify the file in order to include the following

```
# strongswan.conf - strongSwan configuration file
charon
{
   # number of worker threads in charon
   threads = 16
   # plugins to load in charon
   # load = aes des sha1 md5 sha2 hmac gmp random pubkey
xcbc x509 stroke

  plugins {
     sql
     {
        # loglevel to log into sql database
        loglevel = -1
        # URI to the database
        # database = sqlite:///path/to/file.db
        # database = mysql://user:password@localhost/
database
     }

     duplicheck
     {
        # Enable duplicheck plugin (if loaded).
        # enable = yes
        enable = no

        # Whether to load the plugin. Can also be an
integer to increase the
        # priority of this plugin.
        load = no

        # Socket provided by the duplicheck plugin.
        # socket = unix${piddir}charon.dck
     }
  }
# filelog
# {
#    /log/ipsec.log
#    {
#       # add a timestamp prefix
#       time_format = %y%m%d-%H%M%S
#       # prepend connection name, simplifies grepping
#       ike_name = yes
#       # overwrite existing files
```

```
#       append = yes
#       # increase default loglevel for all daemon
#subsystems
#       default = 1
#       # flush each line to disk
#       flush_line = yes
#    }
# }

  stderr
  {
     # more detailed loglevel for a specific subsystem,
overriding the
     # default loglevel.
     ike = -1
     knl = -1
     enc = -1
     net = -1
  }
  # ...
  syslog
    # prefix for each log message
    identifier = charon
    # use default settings to log to the LOG_DAEMON
facility
    daemon {
      default = -1
      ike = -1
      enc = -1
      net = -1
    }
    # very minimalistic IKE auditing logs to LOG_AUTHPRIV
    auth {
      default = -1
      ike = -1
    }
  }
}
pluto
{
  # plugins to load in pluto
  # load = aes des sha1 md5 sha2 hmac gmp random pubkey
}
libstrongswan
{
  #  set to no, the DH exponent size is optimized
  #  dh_exponent_ansi_x9_42 = no
}
```

13. For customers updating from SLES11SP2, racoon logging in `/var/log/messages` has to be disabled by commenting the log entry in `/etc/racoon/racoon.conf`.

```
========================================
/etc/racoon/racoon.conf
#log debug2;
```

14. To start the IPsec service, execute the following command as `root` in a shell:

```
ipsec start
```

> ***NOTE:*** Every time you modify the IPSEC rules a new `ipsec restart` is necessary.
> With `ipsec status` or `ipsec statusall` you can check the active IPSEC Connections.

15. To have the IPsec service start automatically when the application computer reboots, execute the following command as `root` in a shell:

```
chkconfig ipsec on
```

> ***NOTE:*** In SLES 12 installations IPSec can be enabled and started via the following commands:
> `systemctl enable strongswan.service`
> `systemctl start strongswan.service`
> `systemctl status strongswan.service`

16. To check whether the IPsec service works correctly, execute the following command in a shell:

```
tcpdump –i any | grep ESP
```

If OpenScape Voice and application computers communicate via MGCP, the shell should put out messages in the following format:

```
17:09:23.063745 IP 10.1.250.20 > adsa11n1: ESP(spi=0xfb1c7d52,seq=0x16)
17:09:23.064081 IP adsa11n1 > 10.1.250.20: ESP(spi=0x39281790,seq=0x16)
17:09:23.064086 IP adsa11n1 > 10.1.250.20: ESP(spi=0x39281790,seq=0x16)
```

IPsec is now operable for MGCP connections between OpenScape Voice and OpenScape UC Application.

19.3.2 Configuration for Standard Duplex (large)

NOTE: You need to execute the configuration steps of this chapter only if you use Standard Duplex (large).

You need to execute the following configuration steps for encrypting the MGCP connections between OpenScape UC Application (Standard Duplex (large)) and OpenScape Voice using IPSec.

- Configuring OpenScape Voice for IPSec-based MGCP Connections (Standard Duplex (large))
- Configuring OpenScape UC Application for IPSec-based MGCP Connections (Standard Duplex (large))

19.3.2.1 Configuring OpenScape Voice for IPSec-based MGCP Connections (Standard Duplex (large))

Encrypting the MGCP communication between OpenScape Voice and the relevant OpenScape Media Servers by IPSec requires configuring IPSec in OpenScape Voice.

Start the configuration

How to configure IPSec for OpenScape Voice:

1. Create a secure end point for the fully qualified host name **ncs_ip_alias_1**.

   Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the MGCP Endpoint>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP addr. of the Media Server MGCP interface>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): ncs_ip_alias_1
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 1
Key Length in Bytes (default: 16):
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

NOTE: If you do not specify an IP address but the associated fully qualified host name under `Local Host`, you need not modify the IPSec configuration in the event that the IP address of the relevant interface changes at a later date.
The fully qualified host names for MGCP are defined for OpenScape Voice in `/etc/hosts`. They read by default **ncs_ip_alias_1** and **ncs_ip_alias_2**.

---

2. Determine the key the secure end point uses for the tunnel of the first MGCP interface by having the settings of the just created end point displayed. Proceed as shown in the following example:

   Example:

```
Selection (default: 3): 4
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <name of the created MGCP end point>
Do you want to execute this action? <y/n> (default: yes): y
Total Number of SecEndPts Retrieved : 1
Name: Ext_Asst
Description:
FQDN:
Remote IP Address: <Ext_Asst_IP_Address>
Remote NetMask: 255.255.255.255
Remote Port : 0
Local Host: bond_node_alias
Local Port: 0
IPsec Profile: IPSEC_ESP_SHA_AES
IKE Profile: IKE_SHA2_AES
Key Gen Method: Automatic
Key Type: Hex
Key Length: 16

Key: 7aa88aecd7f40699884b75795fbf9354
```

3. Note down the **Key:** output.

4. Create a secure end point for the fully qualified host name of the second MGCP interface of OpenScape Voice. Because the relevant IPSec tunnel will later be set up to the same OpenScape Media Server as for the first end point, you need to use the same key – the one you just noted down. Proceed as shown in the following example:

   Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the MGCP Endpoint>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP addr. of the Media Server MGCP interface>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): ncs_ip_alias_2
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 2
Key Length in Bytes (default: 16): <key of the first MGCP end point>
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

5. If you use several OpenScape Media Servers as Media Server for OpenScape Voice, execute steps **1** to **4** for the MGCP interface of the relevant OpenScape Media Servers.

   In doing so, use an individual key for each OpenScape Media Server.

You have now configured IPSec for the MGCP connection in OpenScape Voice.

19.3.2.2 Configuring OpenScape UC Application for IPSec-based MGCP Connections (Standard Duplex (large))

Encrypting the MGCP communication between OpenScape Voice and the relevant OpenScape Media Servers by IPSec requires configuring IPSec on every involved OpenScape Media Server.

The RPM `openswan` must be installed and configured on the relevant computer systems for this purpose. This RPM is already contained in the SLES repository of every UC Application system.

Start the configuration

How to configure IPSec for an involved OpenScape Media Server:

1. Place the SLES DVD in the application computer drive.
2. If you have not integrated the SLES DVD as additional installation source yet, do this now via the `zypper ar` command.
3. Execute the following command to install the RPM `strongSwan`:

   ```
   zypper in strongSwan
   ```

4. Open the following configuration file in a text editor:

   ```
   /etc/ipsec.conf
   ```

5. Remove the following sections from the configuration file:
   - `default settings for connections`
   - `sample VPN connection`

IMPORTANT: **Do not** delete section `Disable Opportunistic Encryption`. The relevant computer system will otherwise lose its network connection as soon as IPSec starts.

---

6. In the `Add connections here` section, define an IPSec connection for each MGCP end point you have configured in OpenScape Voice for the relevant OpenScape Media Server.

   In doing so, use the following format:

```
conn <unique connection name>
        left=<IP addr. of the MGCP interface of OpenScape Voice>
        right=<IP addr. of the OpenScape Media server>
        auto=start
        authby=secret
        pfs=no
        keylife=24m
        dpddelay=5
        dpdtimeout=3
        dpdaction=restart
        type=transport
```

7. Save the changes in the configuration file.

8. Open the following configuration file in a text editor:

   `/etc/ipsec.secrets`

9. At the end of the configuration file, define the key to be used for encrypting the MGCP data of the relevant OpenScape Media Server. This is the key you noted down during the IPSec configuration of OpenScape Voice.

   In doing so, use the following format:

```
<IP addr. of the OpenScape Media Server> <IP addr. of the MGCP interface of OpenScape Voice>: PSK 0x<key>
```

   Example:

```
10.235.85.22 10.235.98.60: PSK 0xc3daff51c40778fe2a92f31ecb93e653
10.235.85.22 10.235.98.61: PSK 0xc3daff51c40778fe2a92f31ecb93e653
```

NOTE: In the example, both MGCP connections of OpenScape Voice (`10.235.98.60/61`) end on the same OpenScape Media Server (`10.235.85.22`). This is why the connections use the same key.

NOTE: Leave the configuration file otherwise unchanged.

---

10. Save the changes in the configuration file.
11. Open file `/etc/strongswan.conf` in a text editor
12. Modify the file to include the following

```
# strongswan.conf - strongSwan configuration file
charon
{
   # number of worker threads in charon
   threads = 16
   # plugins to load in charon
   # load = aes des sha1 md5 sha2 hmac gmp random pubkey
xcbc x509 stroke

  plugins {
     sql
     {
        # loglevel to log into sql database
        loglevel = -1
        # URI to the database
        # database = sqlite:///path/to/file.db
        # database = mysql://user:password@localhost/
database
     }

     duplicheck
     {
        # Enable duplicheck plugin (if loaded).
        # enable = yes
        enable = no

        # Whether to load the plugin. Can also be an
integer to increase the
        # priority of this plugin.
        load = no

        # Socket provided by the duplicheck plugin.
        # socket = unix${piddir}charon.dck
     }
  }
# filelog
# {
#    /log/ipsec.log
#    {
#       # add a timestamp prefix
#       time_format = %y%m%d-%H%M%S
#       # prepend connection name, simplifies grepping
#       ike_name = yes
#       # overwrite existing files
```

```
#       append = yes
#       # increase default loglevel for all daemon
#subsystems
#       default = 1
#       # flush each line to disk
#       flush_line = yes
#    }
# }

  stderr
  {
     # more detailed loglevel for a specific subsystem,
overriding the
     # default loglevel.
     ike = -1
     knl = -1
     enc = -1
     net = -1
  }
  # ...
  syslog {
    # prefix for each log message
    identifier = charon
    # use default settings to log to the LOG_DAEMON
facility
    daemon {
      default = -1
      ike = -1
      enc = -1
      net = -1
    }
    # very minimalistic IKE auditing logs to LOG_AUTHPRIV
    auth {
      default = -1
      ike = -1
    }
  }
}
pluto
{
  # plugins to load in pluto
  # load = aes des sha1 md5 sha2 hmac gmp random pubkey
}
libstrongswan
{
  #  set to no, the DH exponent size is optimized
  #  dh_exponent_ansi_x9_42 = no
}
```

13. For customers updating from SLES11SP2, racoon logging in `/var/log/messages` has to be disabled by commenting the log entry in `/etc/racoon/racoon.conf`.

```
========================================
/etc/racoon/racoon.conf
#log debug2;
```

14. To start the IPsec service, execute the following command as `root` in a shell:

```
ipsec start
```

NOTE: Every time you modify the IPSEC rules a new `ipsec restart` is necessary.
With `ipsec status` or `ipsec statusall` you can check the active IPSEC Connections.

---

15. To have the IPsec service started automatically when the computer system of the OpenScape Media Server reboots, execute the following command as `root` in a shell:

```
chkconfig ipsec on
```

NOTE: In SLES 12 installations IPSec can be enabled and started via the following commands:

```
systemctl enable strongswan.service
systemctl start strongswan.service
systemctl status strongswan.service
```

---

16. To check whether the IPsec service works correctly, execute the following command in a shell:

```
tcpdump –i any | grep ESP
```

If OpenScape Voice and OpenScape Media Server communicate via MGCP, the shell should put out messages in the following format:

```
17:09:23.063745 IP 10.1.250.20 > adsa11n1: ESP(spi=0xfb1c7d52,seq=0x16)
17:09:23.064081 IP adsa11n1 > 10.1.250.20: ESP(spi=0x39281790,seq=0x16)
17:09:23.064086 IP adsa11n1 > 10.1.250.20: ESP(spi=0x39281790,seq=0x16)
```

IPsec is now operable for MGCP connections between OpenScape Voice and OpenScape UC Application.

19.4 Support of IKEv2

OpenScape Voice platform supports IKE version 2 as well. Until V9 IPSec capabilities were provided through the “ipsec-tools” package (also known as “raccoon”) but due to a requirement for the JITC certification to be FIPs compliant, the raccoon package has been replaced by the StrongSwan. With this enhancement the following are also being supported:

1. IKE version 2
2. PFS group 14 (2048 bit)
3. Hmac SHA512

19.4.1 OSV side configuration

1. Start the RTP Command Line Interface (startCli) on one of the OpenScape Voice (Standard Duplex) nodes and log in there as **sysad**.
2. Select:

Main Menu >
Application-level Management >
Network Element Security Management >

An example of configuration is the following:

```
Total Number of IP Security Profiles Retrieved : 1

IP Sec Profile Name: Test_IPSEC_IKEv2

Comment:

Protocol: ESP

Transport Protocol: ALL

Local Port in Policy: ON

Remote Port in Policy: OFF

Mode: Transport

AH Authentication Algorithm: None

ESP Authentication Algorithm: HmacSha512

ESP Encryption Algorithm: Aes256

Packet Control: Apply

Direction: BiDirectional
```

```
SA life time (Seconds) : 3600
SA life time (KiloBytes): 0
SubNet Policy flag: OFF
Key Exchange Mechanism : Ike
-------------------------------------------------------------
Total Number of IKE Profiles Retrieved : 1
IKE Name: Test_IKEv2
Description:
IKE Version: 2
Exchange Mode: Main
Authentication Algorithm: HmacSha512
Encryption Algorithm: Aes256
Perfect Forwarding Secrecy: Enabled
ESP Authentication Method: PreSharedKey
Oakley Group: Group 14
SA life time (Seconds): 3600
SA life time (KiloBytes): 0
ReEstablish flag: ON
-------------------------------------------------------------
Total Number of SecEndPts Retrieved : 1
Name: Test_SE_IKEv2
Description:
FQDN:
Remote IP Address: 10.9.102.100
Remote NetMask:
Remote Port: 0
Local Host: csta_ip_alias_1
Local Port: 0
IPSec Profile: Test_IPSEC_IKEv2
IKE Profile: Test_IKEv2
```

```
Key Gen Method: User Input

Key Type: Ascii

Key Length: 16

Key: qwerty1234567890

------------------------------------------------------------
```

19.4.2 UC side configuration - CSTA

Follow the steps below:

1. Place the SLES DVD in the application computer drive.
2. If you have not integrated the SLES DVD as additional installation source yet, do it now via the `zypper ar` command.
3. Execute the following command to install the RPM `strongSwan`:

   `zypper in strongSwan`
4. Open the following configuration file in a text editor:

   `/etc/ipsec.conf`

Part of the /etc/ipsec.conf file

```
conn CSTA-connection-to-grt910an1

keyexchange=ikev2

left=10.9.101.60

right=10.9.102.100

leftprotoport=%any/%any

rightprotoport=%any/%any

leftfirewall=no

auto=start

authby=secret

keylife=24m

ikelifetime=1h

dpddelay=5

dpdtimeout=3

dpdaction=restart
```

```
type=transport

ike=aes256-sha512-modp2048

esp=aes256-sha512-modp2048
```

Part of the `/etc/ipsec.sercerts` file

NewOffboard:

~ # cat /etc/ipsec.secrets

#

```
1. ipsec.secrets

   #
```

2. This file holds the RSA private keys or the PSK preshared secrets for the IKE/ IPsec authentication. See the ipsec.secrets(5) manual page.

```
#

#10.9.102.100 10.9.101.58 : PSK "qwerty1234567890"

#: RSA /etc/ipsec.d/certs/ms.pem

10.9.102.100 10.9.101.60:
PSK0x7177657274793132333435363738393 0
```

3. To check whether the IPsec service works correctly, execute the following command in a shell:

NewOffboard:

```
~ # ipsec statusall

Status of IKE charon daemon (strongSwan 5.1.3, Linux
3.12.49-11-default, x86_64):

uptime: 27 seconds, since Jul 24 14:17:16 2017

malloc: sbrk 2846720, mmap 0, used 622192, free 2224528

worker threads: 10 of 16 idle, 6/0/0/0 working, job queue:
0/0/0/0, scheduled: 5

loaded plugins: charon curl soup ldap pkcs11 aes des blowfish
rc2 sha1 sha2 md4 md5 random nonce x509 revocation
constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey
sshkey pem openssl gcrypt af-alg fips-prf gmp agent xcbc cmac
hmac ctr ccm gcm attr kernel-netlink resolve socket-default
farp stroke smp updown eap-identity eap-sim eap-sim-pcsc
eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-
reauth eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius
```

```
eap-tls eap-ttls eap-peap eap-tnc xauth-generic xauth-eap
xauth-pam tnc-imc tnc-imv tnc-tnccs tnccs-20 tnccs-11 tnccs-
dynamic dhcp certexpire led radattr addrblock unity

Listening IP addresses:

10.9.102.100

Connections:

CSTA-connection-to-grt910an1: 10.9.102.100...10.9.101.60
IKEv2, dpddelay=5s

CSTA-connection-to-grt910an1: local: [10.9.102.100] uses
pre-shared key authentication

CSTA-connection-to-grt910an1: remote: [10.9.101.60] uses
pre-shared key authentication

CSTA-connection-to-grt910an1: child: dynamic === dynamic
TRANSPORT, dpdaction=restart

Security Associations (2 up, 0 connecting):

CSTA-connection-to-grt910an1[2]: ESTABLISHED 8 seconds ago,
10.9.102.100[10.9.102.100]...10.9.101.60[10.9.101.60]

CSTA-connection-to-grt910an1[2]: IKEv2 SPIs:
d6726c6721f5792c_i 39ca9c7f08f71f9e_r*, pre-shared key
reauthentication in 43 minutes

CSTA-connection-to-grt910an1[2]: IKE proposal: AES_CBC_256/
HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_2048

CSTA-connection-to-grt910an1

{2}: INSTALLED, TRANSPORT, ESP SPIs: c6e99176_i c31f2f2f_o

CSTA-connection-to-grt910an1{2}

: AES_CBC_256/HMAC_SHA2_512_256, 192 bytes_i (3 pkts, 5s
ago), 192 bytes_o (3 pkts, 5s ago), rekeying in 8 minutes

CSTA-connection-to-grt910an1

{2}

: 10.9.102.100/32 === 10.9.101.60/32

CSTA-connection-to-grt910an1[1]: CONNECTING,
10.9.102.100[10.9.102.100]...10.9.101.60[10.9.101.60]

CSTA-connection-to-grt910an1[1]: IKEv2 SPIs:
36c52aad8619b8bc_i* 1ce6390b2ba6785a_r
```

```
CSTA-connection-to-grt910an1[1]: IKE proposal: AES_CBC_256/
HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_2048

CSTA-connection-to-grt910an1[1]: Tasks active: IKE_CERT_PRE
IKE_AUTH IKE_CERT_POST IKE_CONFIG CHILD_CREATE
IKE_AUTH_LIFETIME IKE_MOBIKE
```

20 Advanced Locking ID Guidelines

This Appendix addresses OSV Advanced Locking IDs (ALIs) in the following order:

- "Native" OSV Server - whose license files are keyed to the MAC address
- Virtual OSV Server - whose license files are keyed to node.cfg parameter values

20.1 "Native" OSV Server

20.1.1 Overview

The license files are keyed to the MAC address of eth0 of the OSV server - be sure to apply the appropriate license file to each node. **The eth0 MAC address can be verified against the License Locking ID.**

Attention: If the eth0 HWaddr and Locking ID values do not match, the license will not be updated to the OSV node(s). Your next level of support should be contacted.

20.1.2 Displaying the Native OSV eth0 HWaddr (MAC address)

In this example, the **HWaddr** and **Locking ID** values in a bold font are document enhancements.

a) This example verifies a license file for node 1. On node 1, as the root user, execute ifconfig eth0;

```
root@node1:[~] #1000
# ifconfig eth0 |grep HWaddr
eth0 Link encap:Ethernet HWaddr 00:0E:0C:D7:9D:F0
```

The **HWaddr** can be verified against the license file **locking_id**. Open the node 1 license file in an editor and verify the eth0 **HWaddr** matches the license **locking_id** value.

```
<locking_mode>USER</locking_mode>
<locking_id>001517A98604</locking_id>
<alias>node1</alias>
```

b) For duplex systems be sure to verify the license file for node 2 also. In this example, the **HWaddr** and **locking_id** values in a bold font are document enhancements. On node 2, as the root user, execute ifconfig eth0;

```
root@node2:[~] #166
#  ifconfig eth0 |grep HWaddr
eth0      Link encap:Ethernet  HWaddr 00:15:17:A9:82:D6
```

The **HWaddr** can be verified against the license file **locking_id**. Open the node 2 license file in an editor and verify the eth0 **HWaddr** matches the **license locking_id** value.

```
<locking_mode>USER</locking_mode>
<locking_id>001517A982D6</locking_id>
<alias>node2</alias>
```

Attention: If the eth0 and/or eth1 HWaddr and locking_id values do not match the license will not be updated to the OSCV node(s). Your next level of support should be contacted.

20.1.3 Displaying the Native OSV server License Locking ID Information

To display the License Locking ID Info for the OSV servers first navigate the CLI menu as follows: item 6,1,1,10,4

```
*** License Locking Identification Information ***

Locking Ids for Node 1 :
License Advanced Locking ID : 001517A98604
System Advanced Locking ID  : 001517A98604

Locking Ids for Node 2 :
License Advanced Locking ID : 001517A982D6
System Advanced Locking ID  : 001517A982D6
```

License Advanced Locking ID: This is the Locking ID which was last successfully imported license for this node. If this does not show any value the node does not have a license installed.

System Advanced Locking ID: This is the Locking ID which is based on the node's eth0 MAC address. This should always show a value even if a license has not been installed.

Use this link to return to Section 2.7.2, “Including the License file on the Installation USB”, on page 67.

Use this link to return to Section 9.12.1.2, “Customize Node 1”, on page 567.

Use this link to return to Section 8.9, “Fallback Procedures”, on page 507.

20.2 Virtual OSV Server

20.2.1 Overview

For virtual OSV servers, the license files are keyed to the "Advanced Locking_ID." The Advanced Locking_ID (ALI) is based on locking the license to the destination system system using an ID based on multiple system and network parameters.

The Advanced Locking ID for virtual systems is created on an algorithm which uses information from the following parameters:

- GW IP address IPV4 or IPV6 address*
- Host Name (uppercase)
- Host IP address
- Primary DNS IP address
- Time Zone one character indicating the Time Zone

* In the event that IPV4 formats are used, they will be translated into IPV6 format.

The ALI is a 23 byte string.

The ALI can be generated using the Central Licensing Server (CLS) and displayed on the node after installation.

20.2.2 How to determine the parameters of the virtual machine Locking ID

The recommended procedure is to derive the License ALI input from parameters of the node.cfg file. This method allows the License ALI input parameters to be collected prior to and after an installation.

This procedure will list the node.cfg parameters that contain the ALI input values. Prior to the installation of an OSV the node.cfg file can be opened in an editor to determine the ALI parameter values. In an already running OSV the node.cfg file can be queried from the server command line. Examples of OSV command line queries are provided.

Attention: If two parameters in the ALI change **(not counting the time zone)**, the license is no longer valid. An alarm will alert the user that the license is no longer valid and that a 10 day license grace period has begun.

Note: If the examples provided below, the command and relevant element of the result are placed in a bold font by the author. The commands examples are executed as the root user.

---

1. Determine the Gateway IP Address (node.cfg parameter 'default_router'). This address will be either IPV6 (node.cfg parameters 'default_route_1_ipv6' default_router_2_ipv6') or IPV4 (node.cfg parameters 'default_router' default_router_2');

   a) An example 'grep' for the node 1 Gateway IP Address from the OSV command line;

   ```
   root@fsc200a:[~] #366
   # grep -i default_router /etc/hiq8000/node.cfg
   default_router: 10.235.132.1
   default_router_1_ipv6:
   root@fsc200a:[~] #367
   #
   ```

   b) An example 'grep' for the node 2 Gateway IP Address from the OSV command line;

   ```
   root@fsc200a:[~] #367
   # grep -i default_router_2 /etc/hiq8000/node.cfg
   default_router_2: 10.235.132.1
   default_router_2_ipv6:
   root@fsc200a:[~] #368
   #
   ```

   Attention: IF IPV6 default router IPs are listed, THEN the IPV6 addresses MUST BE EMPLOYED as the Gateway IP Address instead of the IPV4 addresses.

   In these examples **the node 1 Gateway IP address is 10.235.132.1** and **the node 2 Gateway IP address is 10.235.132.1**. These examples are from a co-located duplex OSV; in a geo-separated OSV the **Gateway** IPs of the nodes would usually be in different subnets.

2. Determine the Hostname (node.cfg parameter 'node_1_name' or 'node_2_name');

a) An example 'grep' for the node 1 Hostname from the OSV command line;

```
root@fsc200a:[~] #364
# grep -i node_1_name /etc/hiq8000/node.cfg
node_1_name: fsc200a
root@fsc200a:[~] #365
#
```

b) An example 'grep' for the node 2 Hostname from the OSV command line;

```
root@fsc200a:[~] #365
# grep -i node_2_name /etc/hiq8000/node.cfg
node_2_name: fsc200b
root@fsc200a:[~] #366
#
```

In these examples, **the node1 hostname is fsc200a** and **the node 2 hostname is fsc200b**.

3. Determine Host IP Address. Because the OSV allows its subnets to be shared by a bonding device the host IP must be the node nafo IP which is in the same subnet as the default gateway (a.k.a. default router).

   a) In the node.cfg file the 'numberOfInterfaces' parameter dictates the subnet that should contain the default gateway. An example 'grep' for the 'numberOfInterfaces' from the OSV command line;

```
root@fsc200a:[~] #361
# grep -i numberofinterfaces /etc/hiq8000/node.cfg
numberOfInterfaces: 3
root@fsc200a:[~] #362
#
```

b) If the 'numberOfInterfaces' parameter is 3 (Mgmt-Billing-Signaling-Separated) or 2 (Mgmt-Billing-Shared) then the default gateway should be in the Signaling subnet (nafo1). An example 'grep' for the nafo1 IPs follows (the output is truncated for a 'cleaner' display);

```
root@fsc200a:[~] #362
# grep -i nafo_udp /etc/hiq8000/node.cfg
nafo1: nafo_udp  bond1  bond1 10.235.132.52 10.235.132.53
255.255.255.0  10.235.132.0  10.235.132.255
root@fsc200a:[~] #363
#
```

In this example, **the node 1 nafo1 IP is 10.235.132.52** and **the node 2 nafo1 IP is 10.235.132.53**. This example is from a co-located duplex OSV; in a geo-separated OSV the nafo1 IPs of the nodes would usually be in different subnets.

c) If the 'numberOfInterfaces' parameter is 1 (Mgmt-Billing-Signaling-Shared) then the default gateway should be in the Mgmt (Admin) subnet (nafo0). An example 'grep' for the nafo0 IPs follows (the output is truncated for a 'cleaner' display);

```
root@fsc200a:[~] #363
#grep-inafo_alias/etc/hiq8000/node.cfg
nafo0: nafo_alias  bond0  bond0  10.235.131.6 10.235.131.7
255.255.255.0  10.235.131.0  10.235.131.255
root@fsc200a:[~] #364
#
```

In this example, **the node 1 nafo0 IP is 10.235.131.6** and **the node 2 nafo0 IP is 10.235.131.7**. This example is from a co-located duplex OSV; in a geo-separated OSV the naf01 IPs of the nodes would usually be in different subnets.

4. Determine Primary DNS IP Address (node.cfg parameter 'name_server_ip_1');

   An example 'grep' for the 'name_server_ip_1' from the OSV command line;

```
root@fsc200a:[~] #367
# grep -i name_server_ip_1 /etc/hiq8000/node.cfg
name_server_ip_1: 10.235.200.253
root@fsc200a:[~] #368
#
```

In this example, **the Primary DNS IP Address is 10.235.200.253**.

5. To determine Timezone (node.cfg file parameter 'timezone');

   An example 'grep' for the Timezone from the OSV command line;

```
root@fsc200a:[~] #355
# grep -i timezone /etc/hiq8000/node.cfg
timezone: US/Eastern
root@fsc200a:[~] #356
#
```

   In this example, **the Timezone is** US/Eastern.

Attention: The time zone found in the node.cfg must be converted to a Coordinated Universal Time (UTC) format, which is the format the CLS lists. In this example “US/Eastern” found in the node.cfg would be converted to “[UTC-05:00]: Toronto, Montreal New York City” for the CLS.

20.2.3 Displaying the Virtual OSV server License Locking ID Information

To display the License Locking ID Info for the OSV servers first navigate the Cli menu as follows: item 6,1,1,10,4

```
*** License Locking Identification Information ***


Locking Ids for Node 1 :
License Advanced Locking ID :
System Advanced Locking ID : MFY+WCJ:TL5QXCDED*9R3X+


Locking Ids for Node 2 :
License Advanced Locking ID : MFY+WWUNXS:MWT2VJNCCWX9
System Advanced Locking ID : MFY+WWUNXS:MWT2VJNCCWX9
```

License Advanced Locking ID: This is the Locking ID which was last successfully imported license for this node. If this does not show any value the node does not have a license installed.

System Advanced Locking ID: This is the Locking ID which is are keyed to node.cfg parameter values This should always show a value even if a license has not been installed.

Attention: Each node's License and System Advanced Locking IDs can have the same values, however they may not always be exactly the same; refer to Section Section 20.2.4, “Examples of License Locking Id Info and Accepted ALIs”.

The Locking ID provided by CLS should be exactly the same as the displayed **License Advanced Locking ID**. If the **License Advanced Locking ID** does not match the CLS Locking ID the last license installation was not successful and your next level of support should be contacted.

20.2.4 Examples of License Locking Id Info and Accepted ALIs

The '*get_ali'* script can be used to display the accepted ALIs of an OSV node.

Note: The 'get_ali' functionality will be available in:

- V7.00.01.ALL.07_PS0021E10 (and later released E-patch set levels).
- V7.00.01.ALL.07_PS0030 (and later released patch sets)

---

1. Use the following CLI result as a reference for item '2.';

```
      *** License Locking Identification Information ***

Locking Ids for Node 1 :
 License Advanced Locking ID : W++*9HA7W+2J47DWRN+YXXA
 System Advanced Locking ID  : W++*9HA7W+2RDYYCRN+YXXH ← Not matching scenario

Locking Ids for Node 2 :
 License Advanced Locking ID : W++*952XX5QCVCY5RN+YXX*
 System Advanced Locking ID  : W++*952XX5QCVCY5RN+YXX*
```

2. Displaying the accepted ALIs on each OSV node;

Node 1

```
# /opt/unisphere/srx3000/cla/bin/get_ali -f /unisphere/srx3000/callp/bin/OSCVoice_V7.gpcf

ALI1: AKHPXHA7W+2+QXN:RN+YXX4
ALI2: AKHPXHA7W+2F+SSCRN+YXXY
ALI3: 3YTSAHA7W+2J47DWRN+YXXP
ALI4: Q5SU:HA7W+2J47DWRN+YXXZ
ALI5: W+++9HA7W+2J47DWRN+YXXA  ← Matches the License Advanced Locking ID
ALI6: WPK3EHA7W+2J47DWRN+YXXS
ALI7: ZU35LHA7W+2J47DWRN+YXXQ
ALI8: 3YTSAHA7W+2RDYYCRN+YXXQ
ALI9: Q5SU:HA7W+2RDYYCRN+YXXR
ALI10: W+++9HA7W+2RDYYCRN+YXXH ← Matches the System Advanced Locking ID
ALI11: WPK3EHA7W+2RDYYCRN+YXXX
ALI12: ZU35LHA7W+2RDYYCRN+YXXV
```

Node 2

```
# /opt/unisphere/srx3000/cla/bin/get_ali -f /unisphere/srx3000/callp/bin/OSCVoice_V7.gpcf

ALI1: AKHPX52XX5Q3D3C9RN+YXXM
ALI2: AKHPX52XX5QV*UVRRN+YXX#
ALI3: 3YTSA52XX5QCVCY5RN+YXXP
ALI4: Q5SU:52XX5QCVCY5RN+YXXW
ALI5: W+++952XX5QCVCY5RN+YXX*  ← Both IDs share this ALI
ALI6: WPK3E52XX5QCVCY5RN+YXXX
ALI7: ZU35L52XX5QCVCY5RN+YXX*
ALI8: 3YTSA52XX5QWSKRXRN+YXXN
ALI9: Q5SU:52XX5QWSKRXRN+YXX2
ALI10: W+++952XX5QWSKRXRN+YXXN
ALI11: WPK3E52XX5QWSKRXRN+YXX2
ALI12: ZU35L52XX5QWSKRXRN+YXXT
```

Follow this link to return to Section 4.3.7.4, “Preparation of the VMware Guest Machines - One Physical Server Solution”, step 15 on page 297.

Follow this link to return to Section 13.2.2.2, “Update the node.cfg file for the OpenScape Voice system”, on page 585.

21 Configuring the OSV Nodes for Shutdown

21.1 Overview

Before rebooting or shutting down the voice server node(s), the system must be configured to state 2. After the node(s) are at state 2, they can be rebooted or shutdown.

For a duplex system, data can be lost when both nodes are deactivated and the node with an older database is reactivated first. An example scenario that could result in data loss follows (for this example the OSV nodes are referred to as A and B);

1. Both OSV nodes are at state 4 4.
2. OSV node A is set from state 4 to state 2.
3. OSV node B is set from state 4 to state 2.
4. OSV node A is brought to state 4 (before server B).

This example may cause a loss of data because node A was brought to state 4 first. The recommended node configuration sequence is "last node down is the first node up". In this example, that would be node B.

Note: The commands are to be executed as user "root".

21.2 Shutting Down the Node(s)

For integrated systems, begin at step 1.

For a standard duplex system, begin at step 2.

1. For integrated systems, stop Symphonia with this command (as user *root*):

   ```
   root@fsc301:[~] #1000
   # /etc/init.d/symphoniad stop
   Shutting down OpenSOA Framework
   ```

2. As user *root*, from the node that will be shutdown, configure the node to state 2 as indicated:

Duplex systems. Examples for each node follow:

Attention: For a correctly configured duplex system, each node can be configured individually without a loss of call processing. If you need call processing to remain active, do not shutdown both nodes of a duplex system at the same time.

Duplex system node 1, from node 1;
root@fsc301:[~] #910
 # /unisphere/srx3000/srx/startup/srxctrl 2 nc

or

Duplex system node 2, from node 2;
root@fsc302:[~] #910
 # /unisphere/srx3000/srx/startup/srxctrl 2 nc

Simplex systems:

Attention: For a simplex system this step will result in a complete loss of OSV call processing for the duration of the process.

---

root@fsc301:[~] #910
 # /unisphere/srx3000/srx/startup/srxctrl 2 0

The nodes (or node for simplex systems) should be at state 2 when the system displays a message similar to this:

--- srxctrl ended on Wed May 27 13:52:27 2009 ---

3. Verify the status of the nodes (or node for simplex systems) with the command:

   ```
   root@fsc301:[~] #911
   ```

   # /unisphere/srx3000/srx/startup/srxqry

   It is expected that the nodes (or node for simplex systems) will be at state 2 at this time.

4. From the console of each node, the voice server node can now be 'rebooted' or shutdown. Execute the commands as user *root*.

   1. Example command syntax for shutdown;

      ```
      # shutdown -P
      ```

      If a node is 'shutdown,' it can be restored by powering on the voice server. Use the power button to power up a server. It is expected that the node (or nodes) should be at state 4 when the system displays a message similar to this:

      --- srxctrl ended on Wed May 27 13:52:27 2009 ---

If the node(s) were shutdown for maintenance it is a good practice to run RapidStat after they are restored (to verify the node health state).

This link will take you to step b on page 736 of Section 24.2, “Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)”.

Note: You can use the command
`# shutdown -H`
when you want to halt the machine. This command shuts down the node but does not power off the machine.

---

2. Example command syntax for reboot;

   `# reboot`

   Example output after reboot:

   `ping bondX OK`, where X is the number of a configured bond

   `.....`

   `Executing hiQPolicy`

Note: You may get some Warning messages

---

22 Building an ISO file on the OSV or Applications Server

22.1 Overview

Some Linux based systems have a built in capability to generate ISO images from the command line. The OSC voice and applications servers can be employed for this purpose. Your ISO file structure should already be prepared (as defined in steps 1 through 4 of Section 4.3.4.2, “Saving the node.cfg, license and Patchsets to a Installation ISO Image”, on page 261.

After having prepared your ISO file structure execute the following command (as user *root*) to create the ISO image:

```
mkisofs -iso-level 3 -allow-multidot -input-charset UTF-8 -R -J
-o [out_file_name] pathspec
```

Option explanation (refer to Linux documentation for details.):

-iso-level 3 Sets the iso9660 conformance level. With level 3, no restrictions (other than ISO-9660:1988) do apply

-allow-multidot This options allows more than one dot to appear in iso9660 filenames.

input-charset Input charset that defines the characters used in local file names. In this case UTF-8.

-R Generate SUSP and RR records using the Rock Ridge protocol to further describe the files on the iso9660 file system.

-J Generate Joliet directory records in addition to regular iso9660 file names.

-o The name of the ISO output file to which the iso9660 filesystem image should be written.

pathspec … is the path of the directory tree to be copied into the iso9660 filesystem

22.2 Command Example

In this example, the command is in bold font to make the user's command line input more obvious.

Attention: The "*Warning: creating filesystem that does not conform to ISO-9660*" printed by mkisofs can be ignored. If you use the various extensions of the ISO-9660 file system, you are no longer strictly following the ISO-9660 standard.

Any other errors that are the result of a mkisofs command must be resolved before employing the ISO for a installation.

The root user is in the root home directory. To create an ISO output file in /root named vm1n1.iso from the path /root/n1cdiso/, execute the following command:

```
root@bocastvm1n1:[~] #316
# mkisofs -iso-level 3 -allow-multidot -input-charset UTF-8 -R -J -o vm1n1.iso /root/n1cdiso/
Warning: creating filesystem that does not conform to ISO-9660.
 15.23% done, estimate finish Wed Jul 27 10:57:10 2011
 30.49% done, estimate finish Wed Jul 27 10:57:10 2011
 45.73% done, estimate finish Wed Jul 27 10:57:10 2011
 60.94% done, estimate finish Wed Jul 27 10:57:10 2011
 76.19% done, estimate finish Wed Jul 27 10:57:10 2011
 91.40% done, estimate finish Wed Jul 27 10:57:10 2011
Total translation table size: 0
Total rockridge attributes bytes: 1257
Total directory bytes: 2048
Path table size(bytes): 24
Max brk space used 0
32826 extents written (64 MB)
root@bocastvm1n1:[~] #317
```

22.3 Example Session Log

In this session log, the commands are in bold font to make the user's command line input more obvious. This log presents ISO file creation examples for both nodes of a duplex system.

1. First a long list of the /root files by the user *root*. Notice the input file system path specification for node 1 (n1cdiso) and node 2 (n2cdiso) are already present.

```
root@bocastvm1n1:[~] #313
# 11
total 232
-rw------- 1 root root   4600 Jul 25 11:26 .bash_history
-rw-r--r-- 1 root root     17 Jul  7 14:39 .csocss_key
-rw-r--r-- 1 root root   1332 Nov 23  2005 .exrc
drwx------ 2 root root   4096 Feb 11 11:17 .gnupg
drwxr-xr-x 2 root root   4096 Feb 11 11:10 .kbd
-rw------- 1 root root     73 Jul 11 12:16 .lesshst
drwx------ 2 root root   4096 Jun 28 15:26 .ssh
-rw-r--r-- 1 root root    265 Feb 11 11:21 .suse_register.log
-rw------- 1 root root   4719 Jul 27 09:15 .viminfo
drwxr-xr-x 2 root root   4096 Feb 11 11:21 .wapi
-r-xr-xr-x 1 root root   2705 Feb 11 11:27 bgMonitor
drwxr-xr-x 2 root root   4096 Sep  5  2009 bin
drwxr-xr-x 2 root root   4096 Feb 11 11:48 config
-rw-r--r-- 1 root root    123 Feb 11 11:11 config.log
drwxr-xr-x 2 root root   4096 Feb 11 11:58 cqdata
dr-xr--r-- 2 root root   4096 Jun 30 17:42 imm
drwxr-xr-x 3 root root   4096 Jul 27 10:07 n1cdiso
drwxr-xr-x 3 root root   4096 Jul 27 10:51 n2cdiso
-rw-r--r-- 1 root root      0 Feb 11 11:21 normal
-r-xr-xr-x 1 root root  19024 Feb 11 11:27 rtpinstall.pl
-rwxr-x--- 1 root root 127891 Feb 11 11:21 rtpinstall.sh
-rw-r--r-- 1 root root      0 Feb 11 11:17 sles10-patched
```

2. A long list of the input path specification for node 1 (n1cdiso). Notice the node.cfg.primary and node 1 license file are in the top level of the n1cdiso path. The dev.8kps file and patch sets are listed in path n1cdiso/patch.

```
root@bocastvm1n1:[~] #314
# ll n1cdiso/*
-rw-r--r-- 1 root root  3836 Jul 27 10:07 n1cdiso/
H8KV6_0050563F5980.lic.xml
-rw-r--r-- 1 root root 10807 Jul 27 10:07 n1cdiso/
node.cfg.primary


n1cdiso/patch:
total 65348
-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E01.tar
-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E02.tar
-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E03.tar
-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E04.tar
-rw-r--r-- 1 root root 23285760 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E05.tar
-rw-r--r-- 1 root root 43386880 Jul 27 10:08
V6.00.01.ALL.05_PS0009.tar
-rw-r--r-- 1 root root        0 Jul 27 09:15 dev.8kps
root@bocastvm1n1:[~] #315
#
```

3. A long list of the input path specification for node 2 (n2cdiso). Notice the node.cfg.secondary and node 2 license file are in the top level of the n2cdiso path. The dev.8kps file and patch sets are listed in path n2cdiso/patch.

```
root@bocastvm1n1:[~] #315
# ll n2cdiso/*
-rw-r--r-- 1 root root   3836 Jul 27 10:07 n2cdiso/
H8KV6_0050563F5A60.lic.xml
-rw-r--r-- 1 root root 387072 Jul 27 10:51 n2cdiso/n1.iso
-rw-r--r-- 1 root root 387072 Jul 27 10:51 n2cdiso/n2.iso
-rw-r--r-- 1 root root  10807 Jul 27 10:07 n2cdiso/
node.cfg.secondary


n2cdiso/patch:
total 65348
```

```
-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E01.tar

-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E02.tar

-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E03.tar

-rw-r--r-- 1 root root    40960 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E04.tar

-rw-r--r-- 1 root root 23285760 Jul 27 10:08
V6.00.01.ALL.05_PS0009.E05.tar

-rw-r--r-- 1 root root 43386880 Jul 27 10:08
V6.00.01.ALL.05_PS0009.tar

-rw-r--r-- 1 root root        0 Jul 27 09:15 dev.8kps

root@bocastvm1n1:[~] #316

#
```

4. The ISO file for node 1 is created (vm1n1.iso) from path specification /root/n1cdiso/:

```
root@bocastvm1n1:[~] #316

# mkisofs -iso-level 3 -allow-multidot -input-charset UTF-8 -R -J -o vm1n1.iso /root/n1cdiso/

Warning: creating filesystem that does not conform to ISO-9660.
 15.23% done, estimate finish Wed Jul 27 10:57:10 2011
 30.49% done, estimate finish Wed Jul 27 10:57:10 2011
 45.73% done, estimate finish Wed Jul 27 10:57:10 2011
 60.94% done, estimate finish Wed Jul 27 10:57:10 2011
 76.19% done, estimate finish Wed Jul 27 10:57:10 2011
 91.40% done, estimate finish Wed Jul 27 10:57:10 2011
Total translation table size: 0
Total rockridge attributes bytes: 1257
Total directory bytes: 2048
Path table size(bytes): 24
Max brk space used 0
32826 extents written (64 MB)
root@bocastvm1n1:[~] #317
#
```

5. The ISO file for node 2 is created (vm1n2.iso) from path specification /root/n2cdiso/:

```
root@bocastvm1n1:[~] #317
# mkisofs -iso-level 3 -allow-multidot -input-charset UTF-8 -R -J -o vm1n2.iso /root/n2cdiso/
Warning: creating filesystem that does not conform to ISO-9660.
 15.09% done, estimate finish Wed Jul 27 10:57:28 2011
 30.13% done, estimate finish Wed Jul 27 10:57:28 2011
 45.19% done, estimate finish Wed Jul 27 10:57:28 2011
 60.27% done, estimate finish Wed Jul 27 10:57:28 2011
 75.31% done, estimate finish Wed Jul 27 10:57:28 2011
 90.39% done, estimate finish Wed Jul 27 10:57:28 2011
Total translation table size: 0
Total rockridge attributes bytes: 1415
Total directory bytes: 2048
Path table size(bytes): 24
Max brk space used 0
33204 extents written (64 MB)
root@bocastvm1n1:[~] #318
#
```

6. A long list of the /root files. Notice the node 1 (vm1n1.iso) and node 2 (vm1n2.iso)ISO files are present. **The vm1n1.iso and vm1n2.iso are ready for upload to the VM datastore. It is a good practice to save a backup copy of each file.**

```
root@bocastvm1n1:[~] #318
# ls -ltr
total 132436
-rw-r--r-- 1 root root     1332 Nov 23  2005 .exrc
drwxr-xr-x 2 root root     4096 Sep  5  2009 bin
drwxr-xr-x 2 root root     4096 Feb 11 11:10 .kbd
-rw-r--r-- 1 root root      123 Feb 11 11:11 config.log
drwx------ 2 root root     4096 Feb 11 11:17 .gnupg
-rw-r--r-- 1 root root        0 Feb 11 11:17 sles10-patched
-rwxr-x--- 1 root root   127891 Feb 11 11:21 rtpinstall.sh
-rw-r--r-- 1 root root        0 Feb 11 11:21 normal
-rw-r--r-- 1 root root      265 Feb 11 11:21 .suse_register.log
drwxr-xr-x 2 root root     4096 Feb 11 11:21 .wapi
```

```
-r-xr-xr-x 1 root root    19024 Feb 11 11:27 rtpinstall.pl
-r-xr-xr-x 1 root root     2705 Feb 11 11:27 bgMonitor
drwxr-xr-x 2 root root     4096 Feb 11 11:48 config
drwxr-xr-x 2 root root     4096 Feb 11 11:58 cqdata
drwx------ 2 root root     4096 Jun 28 15:26 .ssh
dr-xr--r-- 2 root root     4096 Jun 30 17:42 imm
-rw-r--r-- 1 root root       17 Jul  7 14:39 .csocss_key
-rw------- 1 root root       73 Jul 11 12:16 .lesshst
-rw------- 1 root root     4600 Jul 25 11:26 .bash_history
-rw------- 1 root root     4719 Jul 27 09:15 .viminfo
drwxr-xr-x 3 root root     4096 Jul 27 10:07 n1cdiso
drwxr-xr-x 3 root root     4096 Jul 27 10:51 n2cdiso
-rw-r--r-- 1 root root 67227648 Jul 27 10:57 vm1n1.iso
-rw-r--r-- 1 root root 68001792 Jul 27 10:57 vm1n2.iso
root@bocastvm1n1:[~] #319
#
```

Note: Click this link to return to step 5 on page 263 of Section 4.3.4.2, “Saving the node.cfg, license and Patchsets to a Installation ISO Image”.

---

23 Shutdown Agent Failover Model and Data Collection displays

23.1 Overview

This appendix provides display examples similar to those output when options 53 or 84 are chosen from the 'tools' menu.

23.2 Option 53. Failover Model - Displays the Network Configuration for Survivability

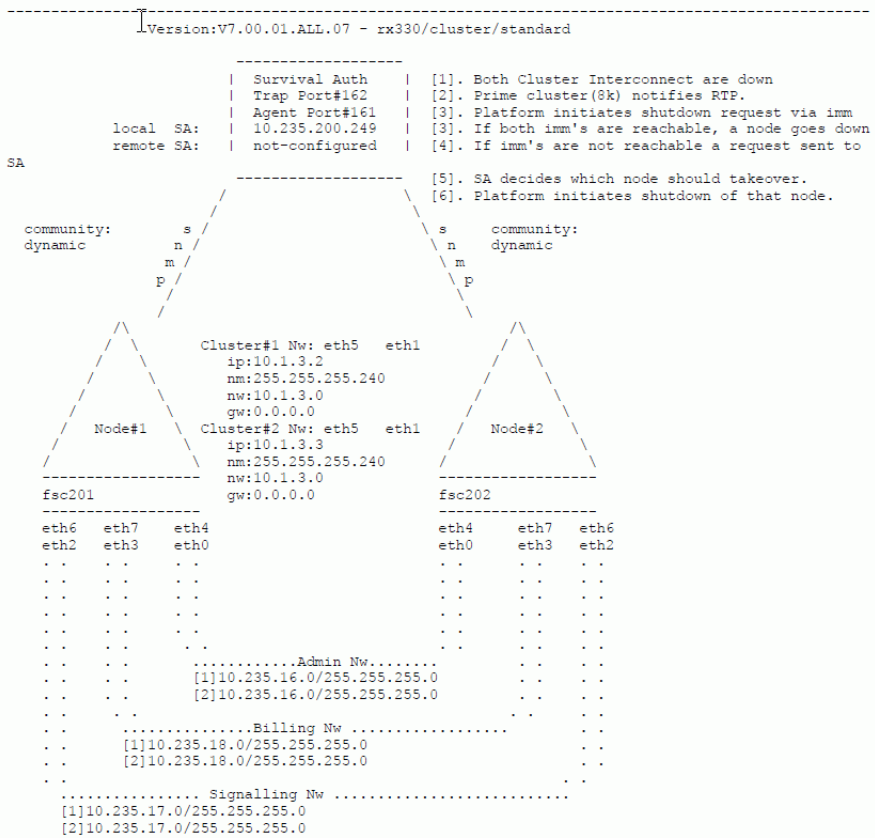
Note: It is only necessary to run the Failover model verification/check from one node because this option will verify/check both nodes of an OpenScape Voice cluster.

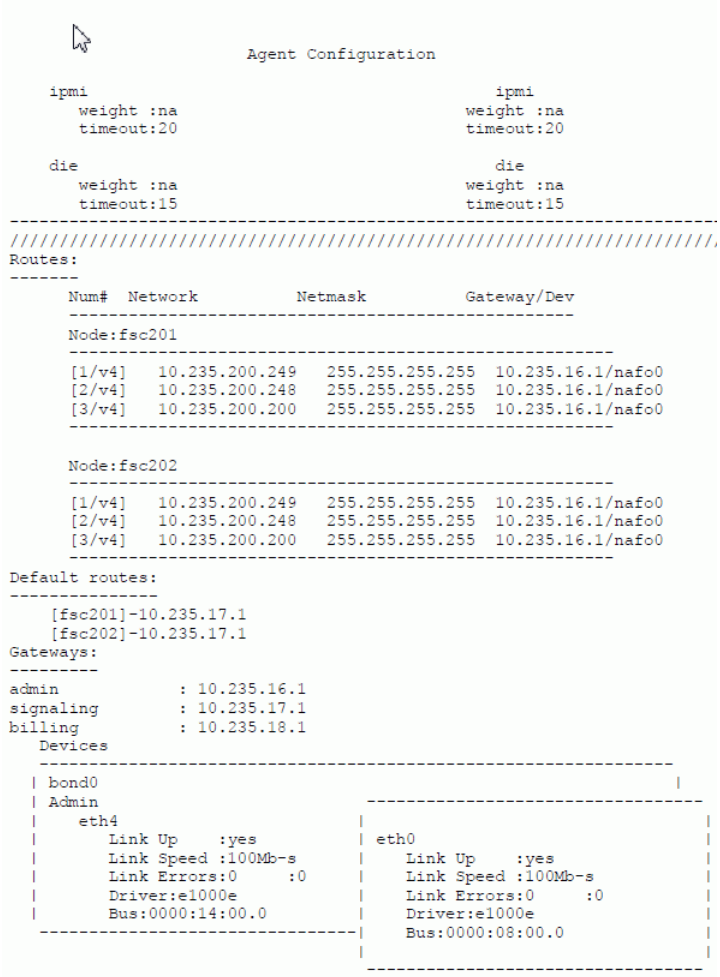
Failover model display example;

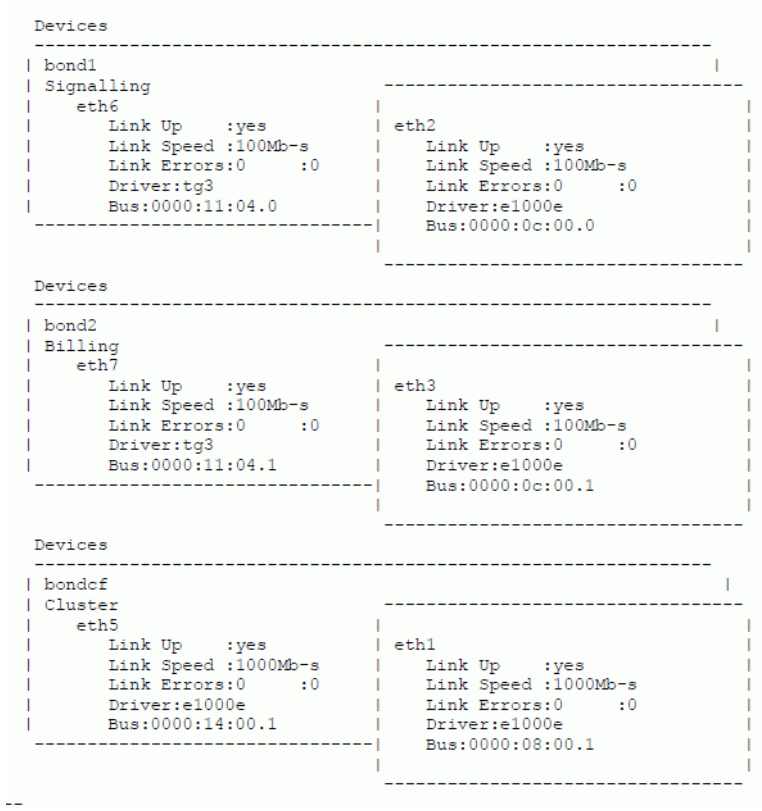
Note: BMC referred to below is your Board Management Controller. This refers to your RSA/IMM port.

```
root@fsc201:[~] #253
# su - srx

User srx, had no failed login attempts since last successful login.
srx on fsc201 using /dev/pts/1 ...
srx@fsc201:[/unisphere/srx3000/srx] #3
$ tools


   ###############################################################################
   #                    Welcome to the Hipath 8K Tools                           #
   #          These tools are dangerous! They can affect call processing         #
   #           Do not run if you are not familiar with the side effects          #
   ###############################################################################

Main Menu :

    1. UCE context util - displays UCE contexts (ctxutil)
    2. RDAL shared memory - displays and changes CAC bandwidth and call counts (rdalTool
    3. SIP-SM dump - displays and accesses SIP SM shared memory (sipsmdump)
    4. FQDN resolver - displays and manages the FQDN black list (fqdnresTool)
    5. CSTA SM dump non-interactive - displays CSTA SM shared memory (cstasmdump)
    6. CSTA SM dump interactive - displays CSTA SM shared memory (cstasmdump)
    7. MLHG print - displays MLHG shared memory (mlhgprint)
    8. NDAL memory display - numbering modification and CAC policies shared memory (ndal
    9. OMM print - displays OMM shared memory (ommprint)

   30. CDR decode - decodes CDR into readable text format (cdrdecode)
   31. XLA verify - displays translation information for calling/called numbers (xlaveri
   32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)
   33. XDM SM Display - displays the content of the XDM Shared Memory (XdmShmDisplay.exe

   50. RTP parameter delta - compares default vs. current RTP parameters
   51. Security Model - displays the network packets rules
   52. Network model - displays all network connections
   53. Failover model - displays the network configuration for survivability

   80. System information - collects low-level system information to diagnose platform i
   81. System information - collects SPT and RU log files, traces and data
   82. System information - collects SMU and EZIP log files and data
   83. System information - collects DB log files and data
   84. System information - collects Survival Authority log files and data

   99. Exit

selection: 53
Enter root password when prompted.
Password:
Analyzing for failover scenarios.
////////////////////////////////////////////////////////////////////////////////////////////
```

Note: (The print out of this log is continues over the next 5 pages.)


Version:V7.00.01.ALL.07 - rx330/cluster/standard
Survival Auth
Trap Port#162
Agent Port#161
local SA:
10.235.200.249
remote SA:
not-configured
[1]. Both Cluster Interconnect are down
[2]. Prime cluster(8k) notifies RTP.
[3]. Platform initiates shutdown request via imm
[3]. If both imm's are reachable, a node goes down
[4]. If imm's are not reachable a request sent to SA
[5]. SA decides which node should takeover.
[6]. Platform initiates shutdown of that node.
community:
dynamic
Cluster#1 Nw: eth5 eth1
ip:10.1.3.2
nm:255.255.255.240
nw:10.1.3.0
gw:0.0.0.0
Node#1
Cluster#2 Nw: eth5 eth1
ip:10.1.3.3
nm:255.255.255.240
nw:10.1.3.0
gw:0.0.0.0
Node#2
fsc201
fsc202
eth6 eth7 eth4
eth2 eth3 eth0
eth4 eth7 eth6
eth0 eth3 eth2
Admin Nw
[1]10.235.16.0/255.255.255.0
[2]10.235.16.0/255.255.255.0
Billing Nw
[1]10.235.18.0/255.255.255.0
[2]10.235.18.0/255.255.255.0
Signalling Nw
[1]10.235.17.0/255.255.255.0
[2]10.235.17.0/255.255.255.0


Agent Configuration
ipmi
weight :na
timeout:20
die
weight :na
timeout:15
ipmi
weight :na
timeout:20
die
weight :na
timeout:15
Routes:
Num# Network Netmask Gateway/Dev
Node:fsc201
[1/v4] 10.235.200.249 255.255.255.255 10.235.16.1/nafo0
[2/v4] 10.235.200.248 255.255.255.255 10.235.16.1/nafo0
[3/v4] 10.235.200.200 255.255.255.255 10.235.16.1/nafo0
Node:fsc202
[1/v4] 10.235.200.249 255.255.255.255 10.235.16.1/nafo0
[2/v4] 10.235.200.248 255.255.255.255 10.235.16.1/nafo0
[3/v4] 10.235.200.200 255.255.255.255 10.235.16.1/nafo0
Default routes:
[fsc201]-10.235.17.1
[fsc202]-10.235.17.1
Gateways:
admin : 10.235.16.1
signaling : 10.235.17.1
billing : 10.235.18.1
Devices
bond0
Admin
eth4
Link Up :yes
Link Speed :100Mb-s
Link Errors:0 :0
Driver:e1000e
Bus:0000:14:00.0
eth0
Link Up :yes
Link Speed :100Mb-s
Link Errors:0 :0
Driver:e1000e
Bus:0000:08:00.0


Devices
bond1
Signalling
eth6
Link Up :yes
Link Speed :100Mb-s
Link Errors:0 :0
Driver:tg3
Bus:0000:11:04.0
eth2
Link Up :yes
Link Speed :100Mb-s
Link Errors:0 :0
Driver:e1000e
Bus:0000:0c:00.0
Devices
bond2
Billing
eth7
Link Up :yes
Link Speed :100Mb-s
Link Errors:0 :0
Driver:tg3
Bus:0000:11:04.1
eth3
Link Up :yes
Link Speed :100Mb-s
Link Errors:0 :0
Driver:e1000e
Bus:0000:0c:00.1
Devices
bondcf
Cluster
eth5
Link Up :yes
Link Speed :1000Mb-s
Link Errors:0 :0
Driver:e1000e
Bus:0000:14:00.1
eth1
Link Up :yes
Link Speed :1000Mb-s
Link Errors:0 :0
Driver:e1000e
Bus:0000:08:00.1

```
User srx, had no failed login attempts since last successful login.
srx on fsc201 using /dev/pts/1 ...
Note: BMC reffered to below is your Board Management Controller.
      This reffers to your RSA/IMM port.

diag8k: Good, rsa/imm configuration found.
diag8k: Checking onboard rsa/imm configration.

[1].Configuration test.
  This tests the configuration of fsc201 for failover.
  - Node#fsc201 configured for BMC: success.
[2].Reachability test.[ icmp ]
  This tests the ping form fsc201 for each of the interfaces below.
  Note: Some routers block ping.
  Hint: Check your network if this test fails.
  - Node#1
   - BMC            : success
   - Gateway        : success
   - Cluster Ip     : success
  - Node#2
   - BMC            : success
   - Cluster Ip     : success
  - Survival Authority
   - Survival Auth  : success
[3].Checking the security rules [ iptables ]
  Hint: Check if the security rules to survival authority are present.
   ACCEPT     udp  --  10.235.200.248       10.235.16.6          udp dpt:161
   ACCEPT     udp  --  10.235.200.248       10.235.16.6          udp dpt:8163
   ACCEPT     tcp  --  10.235.200.248       10.235.16.6          tcp dpt:8768
   ACCEPT     tcp  --  10.235.200.248       10.235.16.6          tcp dpt:8767
   ACCEPT     tcp  --  10.235.200.248       10.235.16.6          tcp dpt:4443
   ACCEPT     udp  --  10.235.200.248       0.0.0.0/0            udp dpt:123
   ACCEPT     udp  --  10.235.200.248       0.0.0.0/0            state ESTABLI
   ACCEPT     udp  --  10.235.200.248       10.235.16.7          udp dpt:161
   ACCEPT     udp  --  10.235.200.248       10.235.16.7          udp dpt:8163
   ACCEPT     tcp  --  10.235.200.248       10.235.16.7          tcp dpt:8768
   ACCEPT     tcp  --  10.235.200.248       10.235.16.7          tcp dpt:8767
   ACCEPT     tcp  --  10.235.200.248       10.235.16.7          tcp dpt:4443
   ACCEPT     udp  --  0.0.0.0/0            10.235.200.248       state NEW,EST
[4].Contact BMC test[ ipmi ].
  This tests the ipmi protocol from both nodes as below.
  If this test fails, it means we are not able get an response for ipmi pdu f
  Hint: Check User/Password in /etc/opt/SMAW/SMAWhaext/sa_ipmi.cfg if this te
  - From:-fsc201/To:-fsc201: success.
  - From:-fsc201/To:-fsc202: success.
  - From:-fsc202/To:-fsc201: success.
  - From:-fsc202/To:-fsc202: success.
[5].Contact Survival Authority test[ snmp ].
  Hint: Check /tmp/expected.cfg if this test fails.
      : Also check the remote survival authority community string(dynamic).
  - fsc201: success.
  - fsc202: success.
```

```
Main Menu :

    1. UCE context util - displays UCE contexts (ctxutil)
    2. RDAL shared memory - displays and changes CAC bandwidth and call counts (rdalTool)
    3. SIP-SM dump - displays and accesses SIP SM shared memory (sipsmdump)
    4. FQDN resolver - displays and manages the FQDN black list (fqdnresTool)
    5. CSTA SM dump non-interactive - displays CSTA SM shared memory (cstasmdump)
    6. CSTA SM dump interactive - displays CSTA SM shared memory (cstasmdump)
    7. MLHG print - displays MLHG shared memory (mlhgprint)
    8. NDAL memory display - numbering modification and CAC policies shared memory (ndalMemDisplay
    9. OMM print - displays OMM shared memory (ommprint)

   30. CDR decode - decodes CDR into readable text format (cdrdecode)
   31. XLA verify - displays translation information for calling/called numbers (xlaverify)
   32. XDM unregister - manually unregisters DNs (XdmUnreg.exe)
   33. XDM SM Display - displays the content of the XDM Shared Memory (XdmShmDisplay.exe)

   50. RTP parameter delta - compares default vs. current RTP parameters
   51. Security Model - displays the network packets rules
   52. Network model - displays all network connections
   53. Failover model - displays the network configuration for survivability

   80. System information - collects low-level system information to diagnose platform issues
   81. System information - collects SPT and RU log files, traces and data
   82. System information - collects SMU and EZIP log files and data
   83. System information - collects DB log files and data
   84. System information - collects Survival Authority log files and data

   99. Exit

selection: 99
srx@fsc201:[/unisphere/srx3000/srx] #4
$
```

23.3 Option 84 System Information - Collects Survival Authority log files and data

Choose option 84 to collect info related to debugging. This option will collect data for both nodes and place the collected data of both nodes in a tar ball (on the node from which the data collection was initiated).

If the tool can not contact the other node a message advising as much will be presented on the terminal. In that case the tool should be invoked on the partner node also. The data will have to be collected from each node in this case.

System information display example;

```
SA Log collection
[*] Testing connectivity with other node
[*] Collecting /log from (srxl41a)...
[*] Collecting /var/log/messages and /var/log/boot.msg /var/log/
and ha logs from  partition (srxl41a)...
[*] Collecting /var/opt/SMAWhaext/log from (srxl41a)...
[*] Collecting /etc/opt/SMAW/SMAWhaext/*.cfg from (srxl41a)...
[*] Collecting RTP dump (srxl41a)...
[*] Collecting iptables rules (srxl41a)...
[*] Collecting network interface configuration - ifconfig
(srxl41a)...
```

```
[*] Collecting network routing configuration - ip route
(srxl41a)...
[*] Collecting network routing configuration - route (Node 1)...
[*] Collecting node.cfg (srxl41a)...
[*] Collecting crm_mon (srxl41a)...
[*] Collecting cibadmin (srxl41a)...
[*] Collecting /log from (srxl45b)...
[*] Collecting /var/log/messages and /var/log/boot.msg /var/log/
and ha logs from  partition (srxl45b)...
[*] Collecting /var/opt/SMAWhaext/log from (srxl45b)...
[*] Collecting /etc/opt/SMAW/SMAWhaext/*.cfg from (srxl45b)...
[*] Collecting RTP dump (srxl45b)...
[*] Collecting iptables rules (srxl45b)...
[*] Collecting network interface configuration - ifconfig
(srxl45b)...
[*] Collecting network routing configuration - ip route
(srxl45b)...
[*] Collecting network routing configuration - route (Node 1)...
[*] Collecting node.cfg (srxl45b)...
[*] Collecting crm_mon (srxl45b)...
[*] Collecting cibadmin (srxl45b)...
[*] Archiving collected files...
[*] The collected logs can be found in /tmp/
srxl41_20110729115207_sa_log_collection.tgz
[*] Done!
```

Note: Click this link to jump to Section 6.8.1.1, “Accessing the 'tools' menu”, on page 410.

---

24 VM Upgrade/Migration Help

24.1 Overview

Note: Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration” is not possible unless a second CD/DVD drive is available.

For an in-service OSV cluster node (or nodes); If a second CD/DVD drive is not already available, refer to Section 24.2, “Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)” and then return to Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration”.

For cases where the migration is from a Native to a Virtual Environment; Use steps 1 through 9 of Section 4.3.7.6, “Adding a CD/DVD Drive to the Virtual Machine”, on page 303 as a guide for Adding a CD/DVD Drive to the Virtual Machine. A link back to this step will be provided.

This section is intended as an aid to customers during Upgrade/Migration procedures. A basic knowledge of the VMware VSphere Client is a pre-requisite. This Appendix is subdivided into the following procedures:

Section 24.2, “Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)”

Section 24.3, “Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration”

- Section 24.3.2, “Making the OSV Image ISO file available from CD/DVD drives during a VM Upgrade/Migration”
- Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration”

Section 24.4, “Export Source System Data”

Section 24.5, “Install the OpenScape Voice V11 Image onto the Upgrade VM Target System”

Section 24.6, “Restore the Data of the Source System to the VM Target System”.

24.2 Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)

This procedure requires the VM be powered down. To avoid invoking the Survival Authority shutdown agent, the CD/DVD drive should be added 'one node at a time'. An overview of the procedure follows;

a) Run RapidStat to ascertain the cluster health and ensure that no problems with the shutdown agents exist before proceeding.

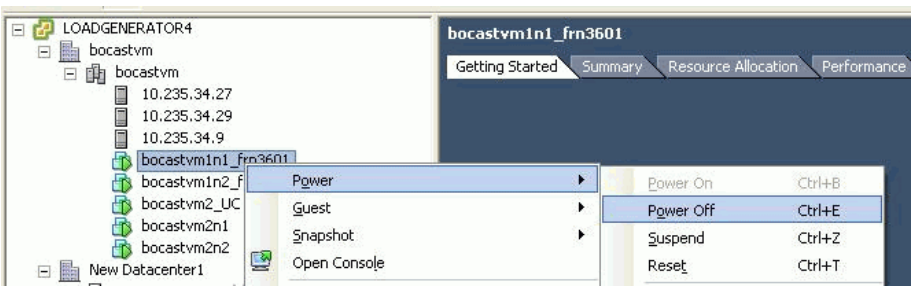
Attention: It is recommended that the user NOT proceed with this procedure until all Warning and Errors reported by the RapidStat are resolved. It may be appropriate to proceed in some Error or Warning message cases, but if there is any doubt, the next level of support should be consulted before proceeding.

---

b) One node of the cluster should be shut down gracefully.

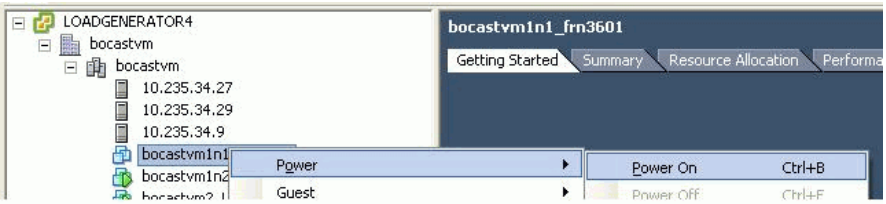
Start with node 1. Refer to Appendix 21, “Configuring the OSV Nodes for Shutdown”.

c) After node 1 shutdown is complete, power down the node 1 VM. In the Vsphere client right click the VM OSV node where the CD/DVD drive will be added, select **Power**, then **Power Off**. If VMWare tools have been installed, you may select **Power** and then **Shut Down Guest**. Wait for the task request to complete. In the following example, OSV VM bocastvm1n1_frn3601 is being powered down (the OSV VM does not have VMWare tools installed).



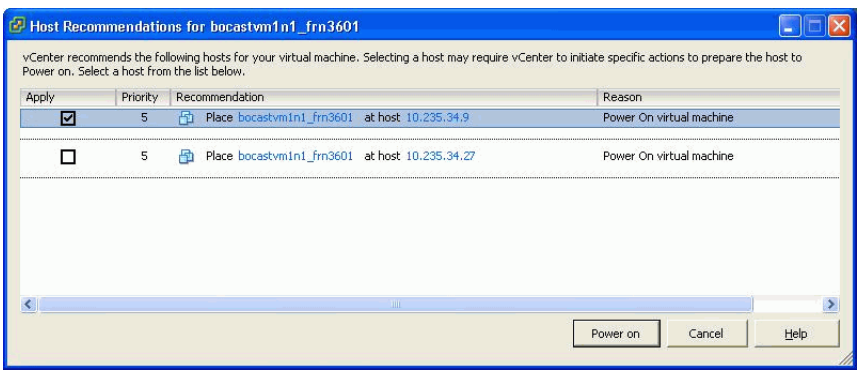
d) Use steps 1 through 9 of Section 4.3.7.6, “Adding a CD/DVD Drive to the Virtual Machine”, on page 303 as a guide for Adding a CD/DVD Drive to the Virtual Machine. A link back to this step will be provided.

e) After the CD/DVD drive is successfully added, in the Vsphere client “right click” the VM OSV node in which the CD/VD drive was added, select **Power**, then **Power On**. If VMWare tools have been installed, you may select **Power** and then **Restart Guest**. Wait for the task request to complete. In the following example bocastvm1n1_frn3601 is being powered up (the OSV VM does not have VMWare tools installed).



Attention: The step **f** (below) only applies to VMs with the **Data Resource Scheduler** active. If the **Data Resource Scheduler** is not active on step **g)**.

f) Depending on whether the VMware **Data Resource Scheduler** is active and what **Automation Level** is set, a window asking which host should be used for the OSV guest installation may be presented. Be sure to select the check box of the host you wish to **Apply** the OSV node1 guest to. An example follows. The user selects host 10.235.34.9 to **Apply** the OSV guest to;



g) After selecting your installation host, click the **Power On** button.

h) After the OSV VM node completes loading, ensure that both nodes of the cluster are at state 4. As user *root* execute the following command;

```
# /unisphere/srx3000/srx/startup/srxqry
```

It is expected that the nodes (or node for simplex systems) will be at state 4 at this time.

i) Run RapidStat to ascertain the cluster health and ensure that no problems with the shutdown agents exist before adding a CD/DVD drive to the second node of the cluster.

j) Repeat step **b)** through step **h)** on node 2 of the cluster.

k) Run RapidStat to ascertain the cluster health and ensure no problems with the shutdown agents exist before adding a CD/DVD drive to the second node of the cluster.

24.3 Making the OSV Image and Installation ISO files available from CD/DVD drives during a VM Upgrade/Migration

24.3.1 Overview

Note: Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration” is not possible unless a second CD/DVD drive is available.

For an in-service Virtual OSV cluster nodes (or node); if a second CD/DVD drive is not already available refer to Section 24.2, “Adding a CD/DVD drive to an in-service OSV cluster node (or nodes)” and then return to Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration”.

For cases where the migration is from a Native to a Virtual Environment; use steps 1 through 9 of Section 4.3.7.6, “Adding a CD/DVD Drive to the Virtual Machine”, on page 303 as a guide for Adding a CD/DVD Drive to the Virtual Machine. A link back to this step will be provided.

These procedures describe making the OSV Image and Installation ISO files available for the VM Upgrade/Migration. This section is broken down further into two separate set of instructions;

- Section 24.3.2, “Making the OSV Image ISO file available from CD/DVD drives during a VM Upgrade/Migration”
- Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration”

24.3.2 Making the OSV Image ISO file available from CD/DVD drives during a VM Upgrade/Migration

These steps guide the user through making the OSV Image ISO file available for the upgrade.

Red highlights are added to the snapshot (at the end of these steps) to assist in locating the parameters.

a) From the Vsphere client or VCenter, right click the VM OSV node1 that is to be updated/migrated (**a**), select Edit Settings from the menu list. The Virtual Machine Properties window is presented.

b) Select the **Hardware** tab. A CD/DVD Drive 1 should already be created (**b**). Select this drive.

c) In the **Device Status box** (**c**) select **Connected** and **Connect at power on**.

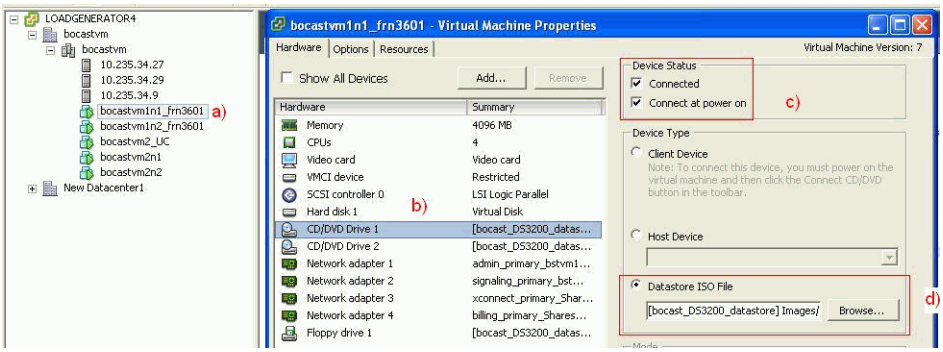
d) Select **Datastore ISO File** (**d**) and browse to the OpenScape Voice ISO image to be installed and click/select the file.

The OSV ISO file is now ready for installation.

Attention: Repeat steps **a) through d)** for node 2 of a duplex system.

To make the **Installation ISO files available from CD/DVD drives** proceed to Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration”.

e) Repeat **steps a) through d)** for node 2 of a duplex system.



24.3.3 Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration

These steps guide the user through making the Installation ISO file available for the upgrade.

Your VM should already have the second CD/DVD drive created. If your VM does not already have an additional CD/DVD Drive added to the Virtual Machine, refer to the Note on page 738, of Section 24.3.1, “Overview”. Choose the appropriate doclink from the Note text. Return to this section when the CD/DVD add is completed.

Red highlights are added to the snapshot (at the end of these steps) to assist in locating the parameters

a) From the Vsphere client, right click the VM OSV node1 that is to be upgraded/migrated (**a**), select Edit Settings from the menu list. The Virtual Machine Properties window is presented.

b) Select the **Hardware** tab. A CD/DVD Drive 2 should already be created (**b**). Select this drive.

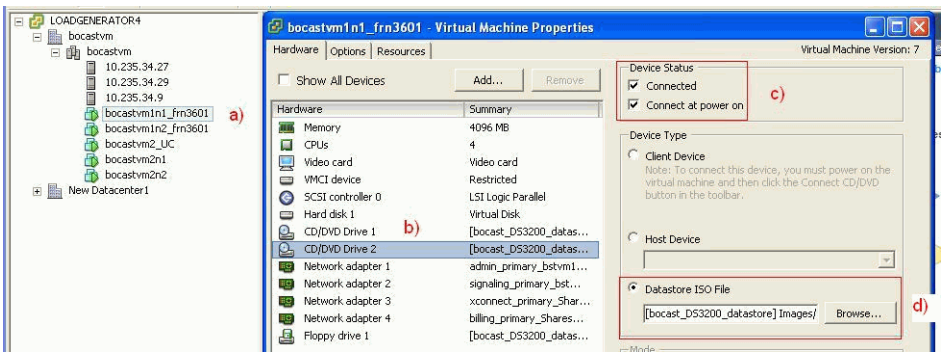
c) In the **Device Status box** (**c**) select **Connected** and **Connect at power on**.

d) Select **Datastore ISO File** (**d**) and browse to the Installation ISO file to be installed and click/select the file.

The Installation ISO file is now ready for installation.

Be sure to select the correct Installation ISO file for your node.

Attention: Repeat steps **a) through d)** for node 2 of a duplex system.



Note: Click this link to jump to step 9 on page 308 of Section 4.3.7.6, “Adding a CD/DVD Drive to the Virtual Machine”, on page 303.

24.4 Export Source System Data

For a full description of exporting source system data, see Section 9.4, “Exporting Source System Data”.

24.5 Install the OpenScape Voice V11 Image onto the Upgrade VM Target System

24.5.1 Overview

Attention: If the hardware of the source release is reused for this migration scenario, before the OSV Image can be installed the ESXi must be installed and the virtual environment configuration built. This will extend the system down time. Section 4.3, “Virtualization Environment Setup”, on page 241 should be referenced for details.

The OSV ISO Image and Installation ISO files should have already been made available in a previous step of this procedure. Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/Migration”, on page 739, addresses the necessary steps.

The server(s) have to be prepared for the target release image installation. The first steps detail the graceful shutdown of the OSV servers and the image installation process for the VMs.

This section addresses both Simplex and Duplex VM installations. For Simplex environments only follow the instructions for node 1.

The Image installation procedure follows OSV Native Hardware shutdown steps.

It is recommended that Section 24.5 be reviewed in its entirety before proceeding with the virtual machine installation.

Note: To switch between the WMware console window and desktop environments;
- click into the Console window to enter the Console.
- 'CTRL-ALT' will leave the Console.

24.5.2 Shutdown of the Native Hardware OSV Nodes

a) If the native hardware of the source release OSV is replaced as part of this procedure, the source release OSV system must be shutdown so no network conflicts will exist when the virtual machines are brought on-line. The source release OSV nodes must be configured to state 2 and shutdown. Login into node 1 and enter the following command as the root user;

   Duplex OSV command;

 # /unisphere/srx3000/srx/startup/srxctrl 2 2

Simplex OSV command;

 # /unisphere/srx3000/srx/startup/srxctrl 2 0

The nodes (or node in the case of a simplex OSV) should be at state 2 when the system displays a message similar to this:

```
--- srxctrl ended on Wed May 27 13:52:27 2009 ---
```

b) Verify the status of the nodes (or node for simplex systems) with the command:

 # /unisphere/srx3000/srx/startup/srxqry

It is expected that the nodes will be at state 2 at this time.

c) From the console of each node, shutdown the nodes (or node in the case of a simplex OSV) with the command:

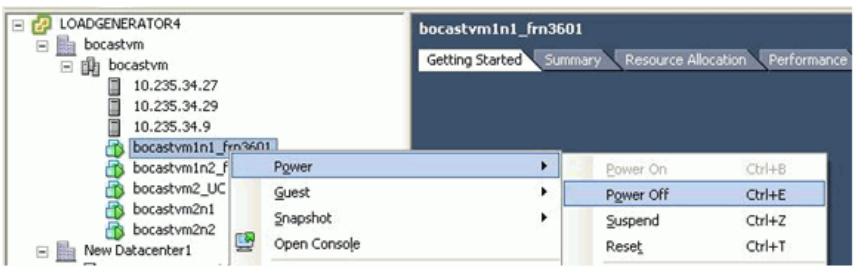
 # shutdown -P

d) From the console select "Alt-F10".

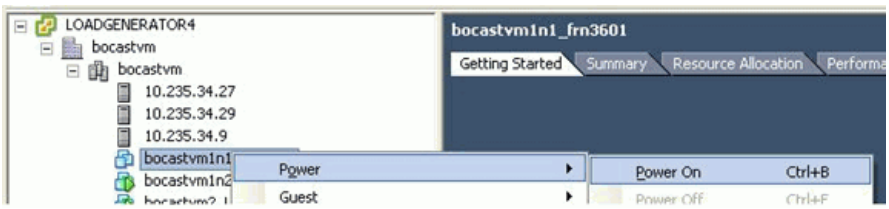
The console will indicate "system halted" (minus the double quotes) when the node is shutdown.

24.5.3 Target Release Image Install

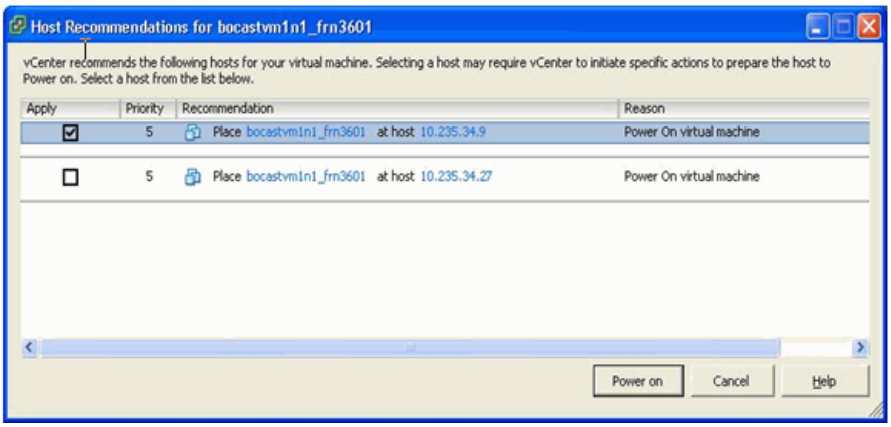
a) The target release OSV image install process can start. In the Vsphere client right click the VM OSV node1 to be upgraded, select **Power** then **Power Off**. Wait for the **Power Off** request to complete. If the VM is already powered down proceed to step b).

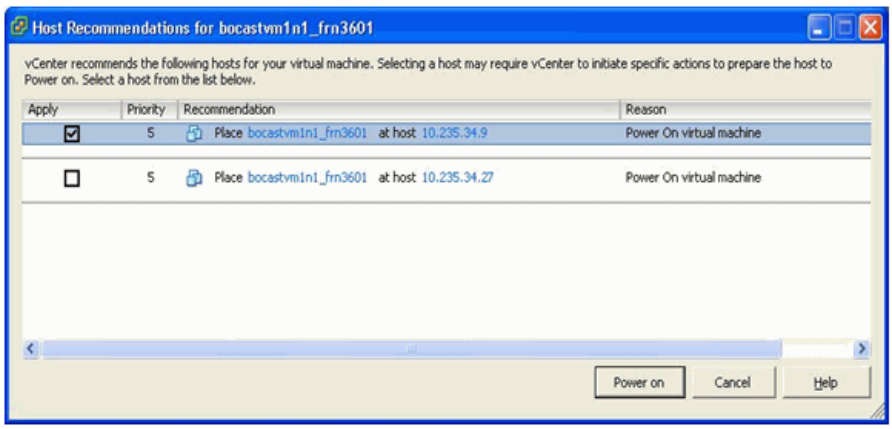


b) In the Vsphere client, right click the VM OSV node1 to be upgraded, select **Power** then **Power On**.



Depending on whether the VMware **Data Resource Scheduler i**s active and what **Automation Level** is set, a window asking which host should be used for the OSV guest installation may be presented. Be sure to select the check box of the host you wish to **Apply** the OSV node1 guest to. After selecting your installation host, click the **Power On** button. An example follows. The user selected host 10.235.34.9 to **Apply** the OSV guest to;

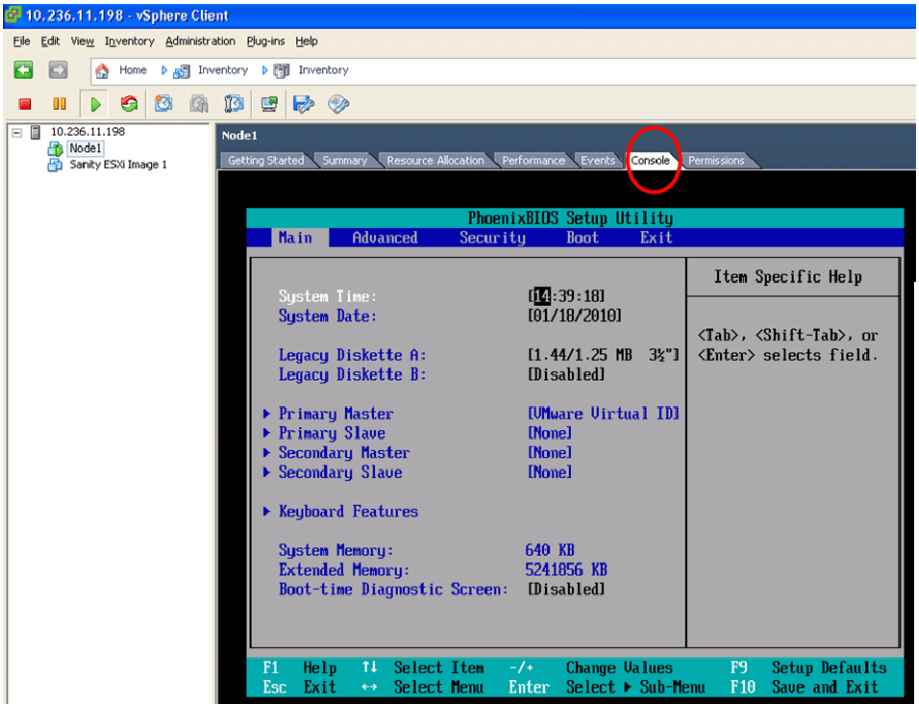




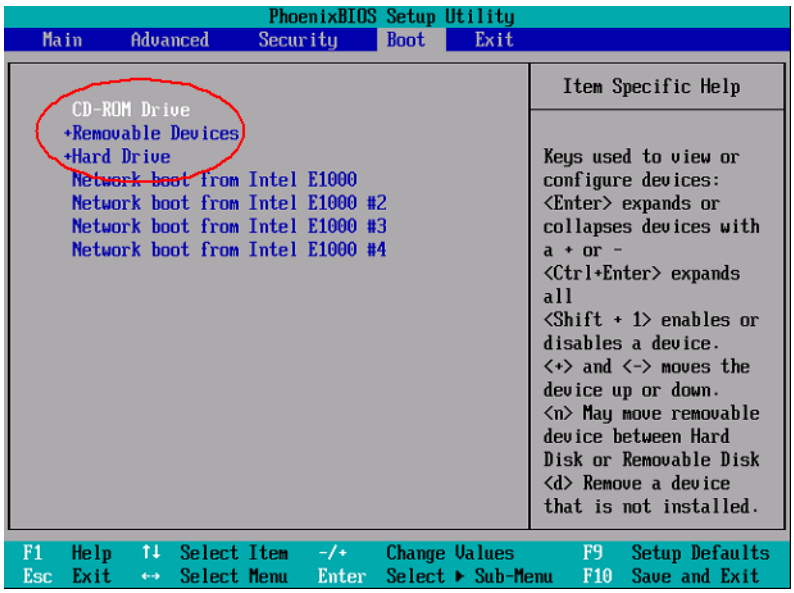
c) Open up the vSphere Client's **Console** tab, click in the console window and hit return to connect to the guest Linux environment OSV will run in.

If this is a first time install for the VM then the BIOS settings screen should appear. Steps c) through k) should be executed in this scenario. Verify/ update the System Date and Time. After verifying the System Date and Time proceed to step d).

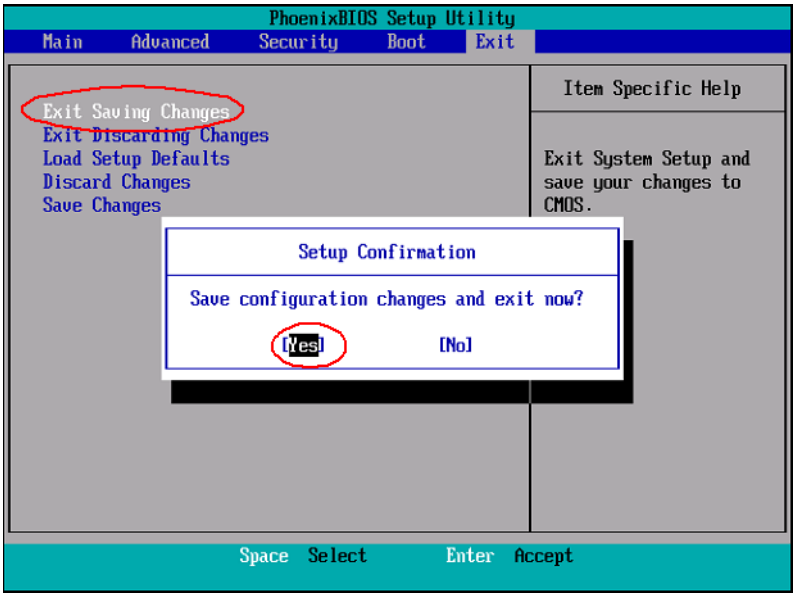
If this is NOT the first install for this VM the BIOS setting checks will not appear. Execute steps f) through k) for this scenario. To switch between the WMware console window and desktop environments;
- click into the Console window to enter the Console.
- '**CTRL-ALT**' will leave the Console



d) Select the BIOS screen's **BOOT** tab and move the CD ROM to the top of the list and the Floppy to the second position.



e) Press the **Esc** key to exit this menu, then select **Exit Saving Changes**. In the Setup Confirmation window select **Yes** to "Save configuration changes and exit now?"



Select **Yes**

f) Select **OpenScape Voice Service System**

g) The End User License Agreement (EULA) is displayed in a new window on the console screen. Review and accept the EULA as follows:

- Review the EULA using the Page Up/Page Down or arrow keys; when you are finished reviewing the EULA, select **Done** and press the Enter key.
- A window is opened with the question: "**Do you accept the License Agreement?**" with the options '**Yes**' and '**No**'.
- In the EULA acceptance window, use the Tab or arrow keys to select **Yes** to proceed with the image installation. Selecting '**No**' will halt the image installation.
- If you select '**No**' by mistake, to continue with the image installation, reboot the server and when prompted to accept the EULA select **Yes**.

Note: If you followed the instructions of Section 24.3.3, “Making the Installation ISO file available from CD/DVD drives during a VM Upgrade/ Migration”, on page 739, you can disregard the request to "**Please insert USB stick now**". The Installation ISO file will be automatically read in.

If the installation file is not automatically recognized perhaps the virtual CD/DVD drive or floppy is not connected (or powered on).

---

h) A '*Virtual Resource Configuration*' popup will be displayed. If the user has configured the virtual machine according to the OSV Installation and Upgrade Guide, select the **<Yes>** option and the Upgrade continues. **Proceed to step** **i on page 746)**, of this tasklist.

The user may select **<No>** to verify the virtual machine resource configuration. The node will return the '*Rescue login*' prompt. At the '*Rescue login*' prompt type '**root**' to login (no password will be required). After the virtual machine resource configuration is verified, restart the installation procedure.

i) A '*Network Information*' window is displayed. Review the information, then select <**Done>**. At the next step, you will have the option to continue or abort the install process. **Proceed to step** **j on page 746,** of this tasklist.

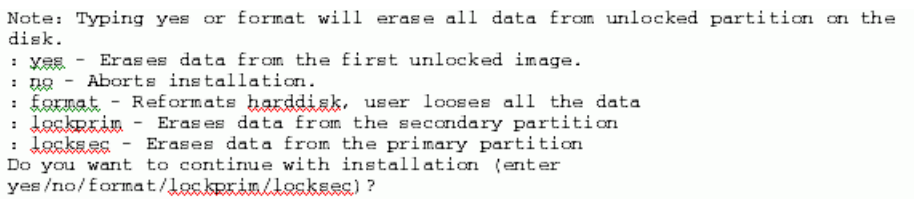
j) Users have the option to install the image on the partition of their choice. On boot, they are prompted with "**yes/no/format/lockprim/locksec**" options. A sample snapshot of the output and an explanation of the options is next.

Attention: The Format option should not be employed during Upgrade or Migration procedures. The source release partition needs to be maintained in case a "Fallback" to the source release is required.

Note: Format and repartition are necessary for fresh installation.

Attention: For an upgrade or a migration procedure, the option 'yes' is typically used.

Sample screenshot;



Options:

yes: Erases data from the first unlocked partition and the image is installed on that unlocked partition. For an upgrade or a migration procedure, this option is typically used.

no: Aborts the installation.

Format: Reformats hard disk, user loses all the data and the image is installed on the primary partition.

Lockprim: Erases data from the secondary partition and the image is installed on the secondary partition.

Locksec: Erases data from the primary partition and the image is installed on the primary partition.

Any questions regarding these new options should be addressed to yournext level of support.

Type **yes** and **press enter** and the Image installation will start.

k) Repeat steps a) through j) of this appendix for Node 2; making sure the Installation ISO contains the node.cfg.secondary.

Note: For specific details of the Image installation please refer to the Release Notes of the Image DVD.

---

l) The installation of both nodes completes.

The installation process is completed when messages similar to the following example are displayed on the Console monitor:

```
Image Status: Completed installation at <Day MM Date
hh:mm:sec Timezone Year>

System verification done

Master Resource Control: runlevel 3 has been reached

Skipped services in run level 3: acpid nfs
Authorized uses only. All activity may be monitored and
reported.

<hostname> login: 0: OK Command execution
```

The text "OK Command execution" appears on the Console monitor in a simple installation or only on one of the Console monitors in a duplex installation. During the imaging process, there are times when the above message appears before the server is rebooted. Please ignore this message. Wait for the message to appear after the "logon" prompt on the Console monitor.

Note: To clarify the "Image Status" text layout, an example is presented: Image Status: Completed installation at Tue Dec 21 13:31:13 EST 2010.”.

24.6 Restore the Data of the Source System to the VM Target System

For a full description of restoring the source system data of the VM source, see Section 9.6, “Importing the Source System Data to the Target System” and Section 9.6.1, “Restore the data of the VM source”.

Attention: Unless directed otherwise by Release Notes, the target OpenScape voice server patch level must be on latest patch set. An integrated system should ensure the applications server is updated with the latest released DVD/PatchSet/HotFix.

Note: By default the source release passwords for system-defined OpenScape Voice accounts (for example, srx, and root) are imported to the target release.

---

25 Upgrading ESXi

25.1 Upgrade VMware ESXi 5.1 to ESXi 5.5

See the VMware Upgrade guides for upgrading from ESXi 5.1 to ESXi 5.5. These guides are available at the VMware homepage (www.vmware.com). Only those VMware features supported in previous releases are supported by OSV at this time.

25.2 Upgrade VMware ESXi 5.5 to ESXi 6

See the VMware Upgrade guides for upgrading from ESXi 5.5 to ESXi 6. These guides are available at the VMware homepage (www.vmware.com). Only those VMware features supported in previous releases are supported by OSV at this time.

25.3 Upgrade VMware ESXi 6 to ESXi 6.5

See the VMware Upgrade guides for upgrading from ESXi 6 to ESXi 6.5. These guides are available at the VMware homepage (www.vmware.com). Only those VMware features supported in previous releases are supported by OSV at this time.

25.4 Upgrade Example for Reference Purposes

For reference purposes, this section provides an example of an update from **ESXi 5.0 to ESXI 5.1.**

25.4.1 Upgrade Steps

Note: Page number references refer to the pages of the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

---

1. Back up your vCenter configuration as per the document (pages 7-9 in the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper).
   a) ssl certificates
   b) vpxd.cfg
   c) database
2. Run v5.0 Agent-PreUpgrade Check (page 9, then go to page 17).
3. Upgrade your 64-bit vCenter 4.1 server to vCenter 5.0 (pages 17-20, then go to page 28).
4. Backup up your ESXi4.1 host (page 33).
   a) Install vCLI if necessary.
   b) Backup the host using vCLI command “vicfg-cfgbackup.”
5. Upgrade your ESXi 4.1 to ESXi 5.0 Hosts with the ESXi. Installer (page 37-41):
   a) Place the host into maintenance mode and then power off the host.
   b) Select the Boot Device and follow the installer steps.
   c) Confirm the upgrade.
   d) Unmount the installation media and reboot the host
6. Reconnect the host to the vCenter (page 41).
   a) Take the host out of maintenance mode.
   b) Reconnect the host to the v5.0 vCenter.
7. Upgrading the virtual machines.
   a) Upgrade the VMware Tools (page 42).
   b) Upgrade the Virtual machine hardware version (page 43).

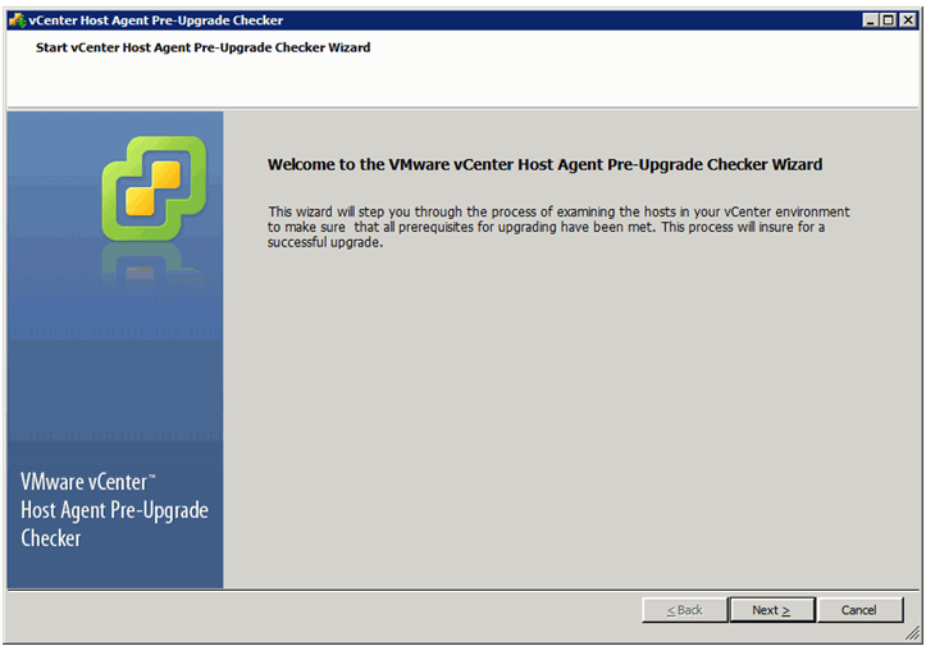
25.4.2 Screen Shots

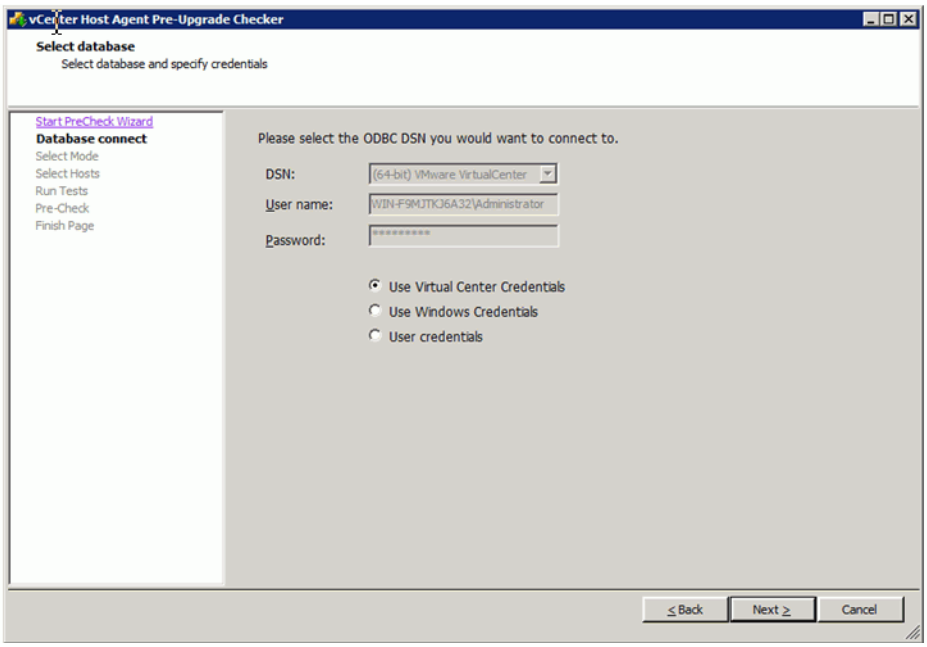
Note: Page number references refer to the pages of the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

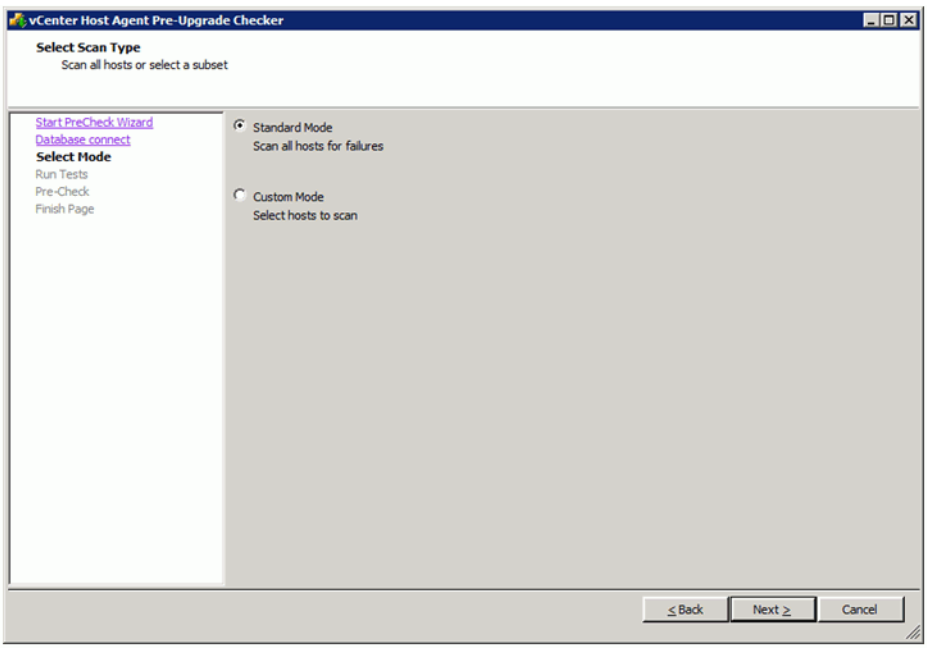
This section provides screen shots of the upgrade procedure.

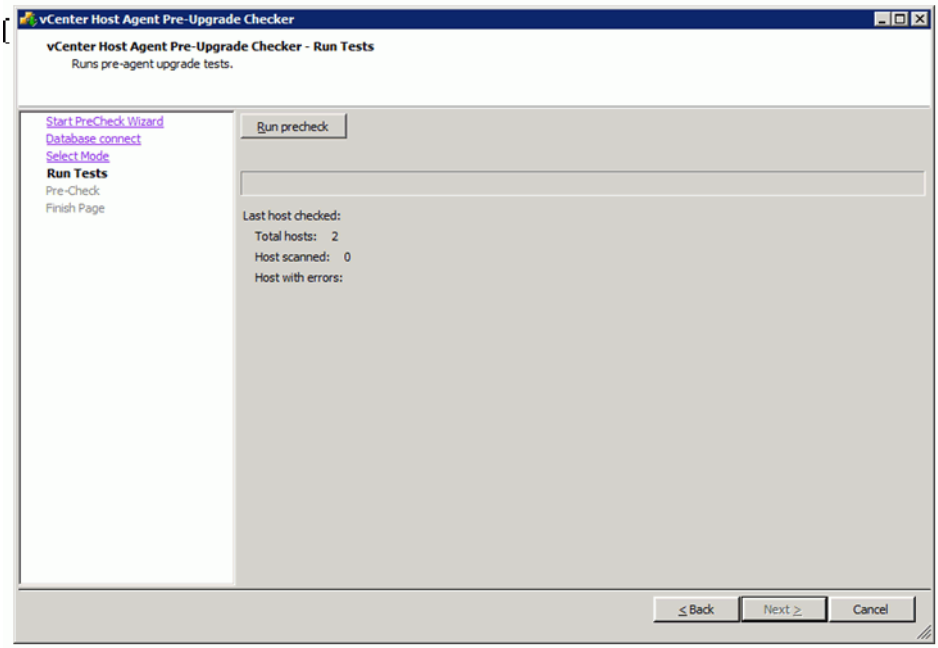
The IP addresses inside the screen shots are for example purposes only.

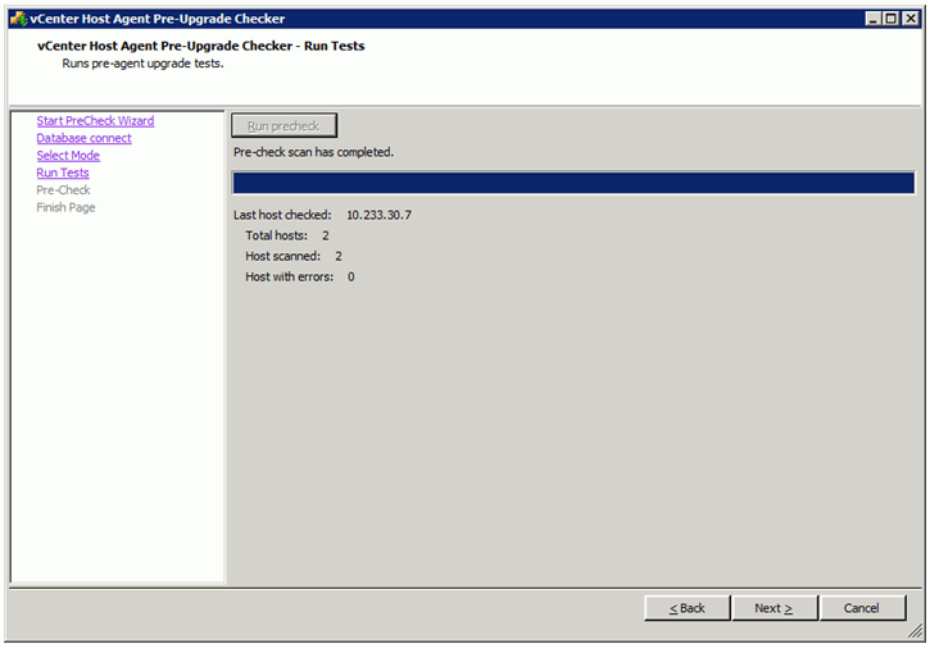
V5.0 Agent Pre-Upgrade Checker: (page 9)

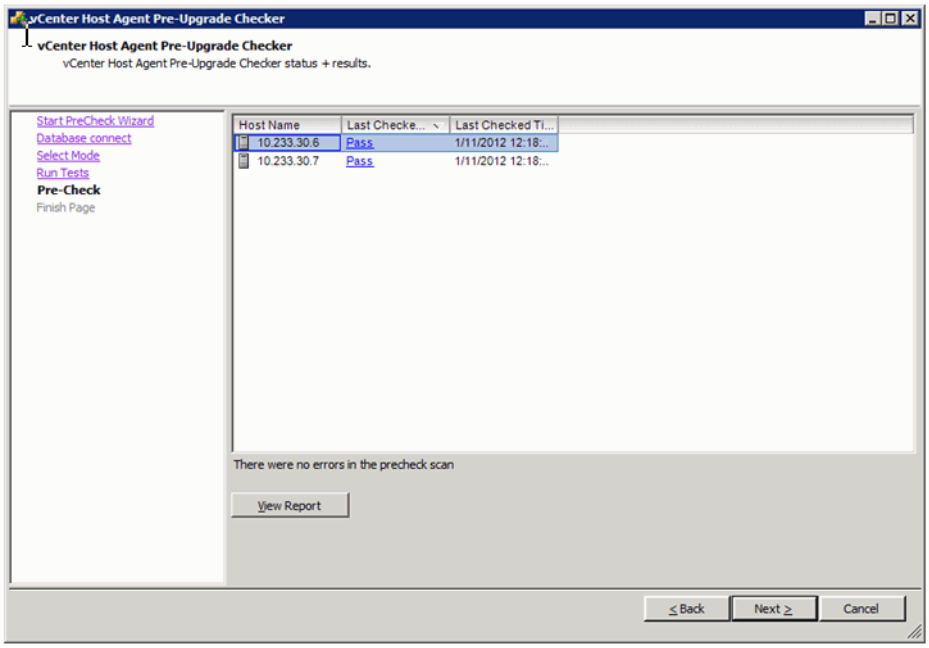


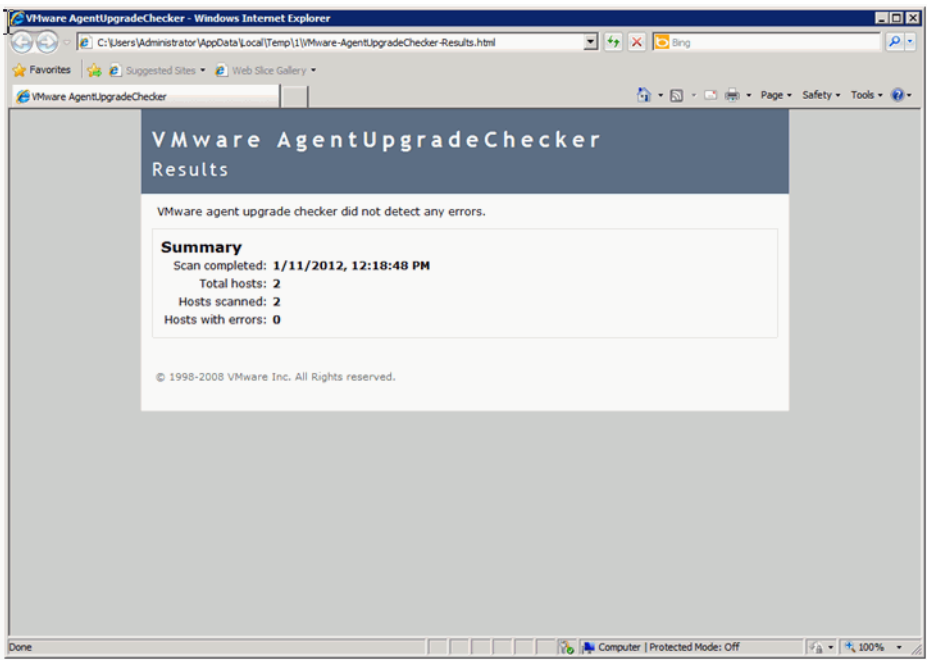

vCenter Host Agent Pre-Upgrade Checker
Select database
Select database and specify credentials
Start PreCheck Wizard
Database connect
Select Mode
Select Hosts
Run Tests
Pre-Check
Finish Page
Please select the ODBC DSN you would want to connect to.
DSN:
(64-bit) VMware VirtualCenter
User name:
WIN-F9MJTKJ6A32\Administrator
Password:
Use Virtual Center Credentials
Use Windows Credentials
User credentials
< Back
Next >
Cancel

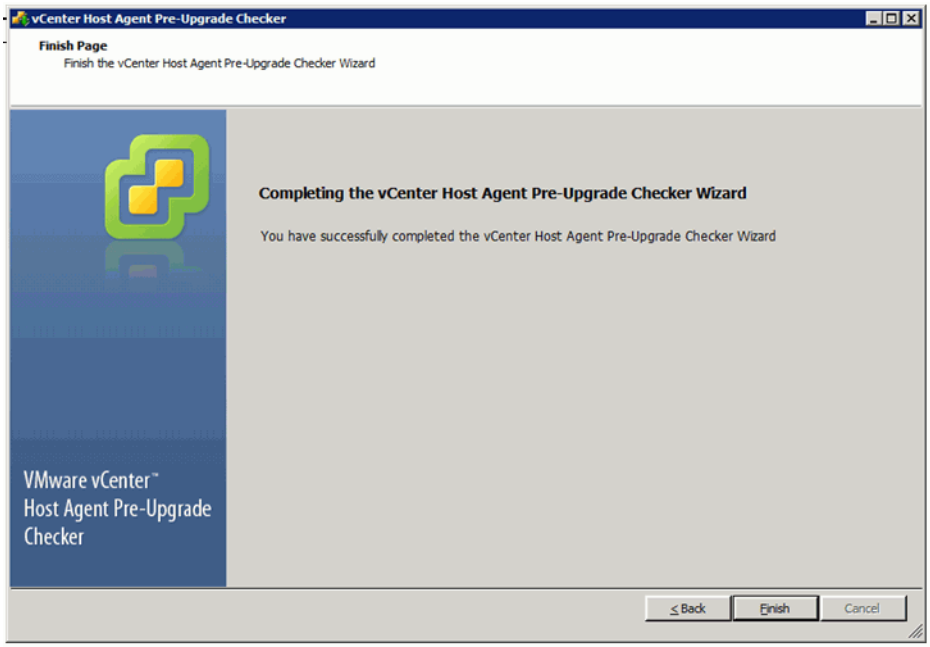

vCenter Host Agent Pre-Upgrade Checker
Select Scan Type
Scan all hosts or select a subset
Start PreCheck Wizard
Database connect
Select Mode
Run Tests
Pre-Check
Finish Page
Standard Mode
Scan all hosts for failures
Custom Mode
Select hosts to scan
< Back
Next >
Cancel


vCenter Host Agent Pre-Upgrade Checker
vCenter Host Agent Pre-Upgrade Checker - Run Tests
Runs pre-agent upgrade tests.
Start PreCheck Wizard
Database connect
Select Mode
Run Tests
Pre-Check
Finish Page
Run precheck
Last host checked:
Total hosts: 2
Host scanned: 0
Host with errors:
< Back
Next >
Cancel

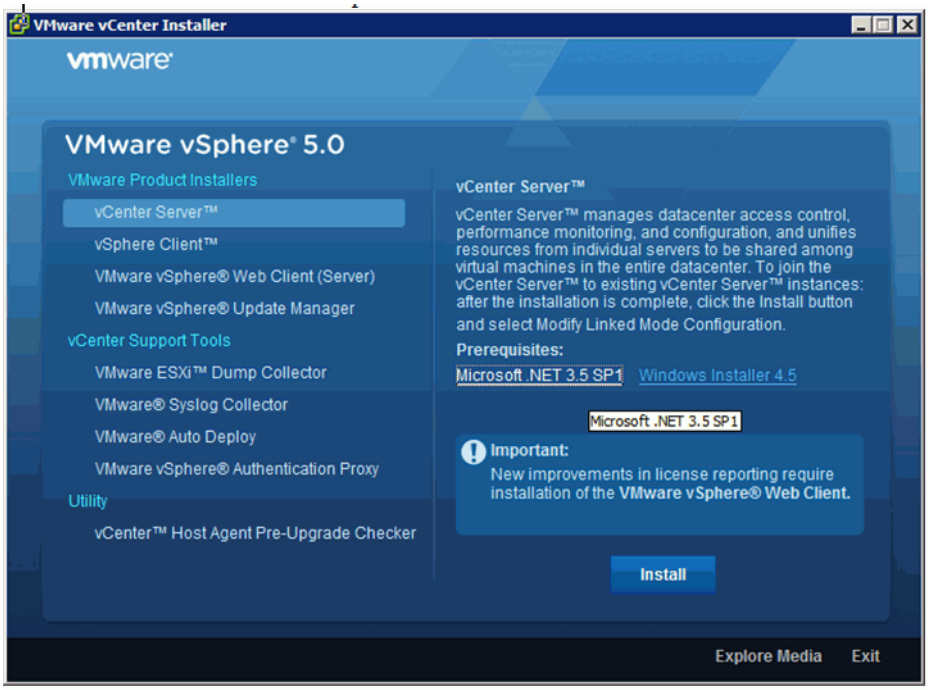

vCenter Host Agent Pre-Upgrade Checker
vCenter Host Agent Pre-Upgrade Checker - Run Tests
Runs pre-agent upgrade tests.
Start PreCheck Wizard
Database connect
Select Mode
Run Tests
Pre-Check
Finish Page
Run precheck
Pre-check scan has completed.
Last host checked: 10.233.30.7
Total hosts: 2
Host scanned: 2
Host with errors: 0
< Back
Next >
Cancel

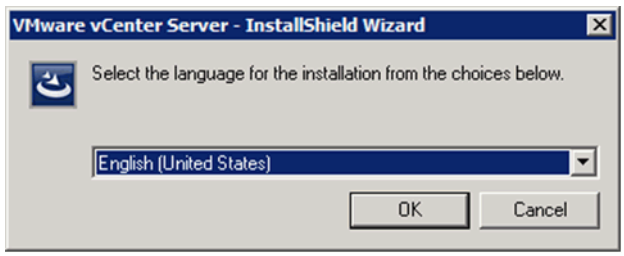

vCenter Host Agent Pre-Upgrade Checker
vCenter Host Agent Pre-Upgrade Checker
vCenter Host Agent Pre-Upgrade Checker status + results.
Start PreCheck Wizard
Database connect
Select Mode
Run Tests
Pre-Check
Finish Page
Host Name
Last Checke...
Last Checked Ti...
10.233.30.6
Pass
1/11/2012 12:18:...
10.233.30.7
Pass
1/11/2012 12:18:...
There were no errors in the precheck scan
View Report
≤ Back
Next ≥
Cancel


VMware AgentUpgradeChecker - Windows Internet Explorer
C:\Users\Administrator\AppData\Local\Temp\1\VMware-AgentUpgradeChecker-Results.html
Favorites
VMware AgentUpgradeChecker
VMware AgentUpgradeChecker
Results
VMware agent upgrade checker did not detect any errors.
Summary
Scan completed: 1/11/2012, 12:18:48 PM
Total hosts: 2
Hosts scanned: 2
Hosts with errors: 0
© 1998-2008 VMware Inc. All Rights reserved.
Done
Computer | Protected Mode: Off
100%

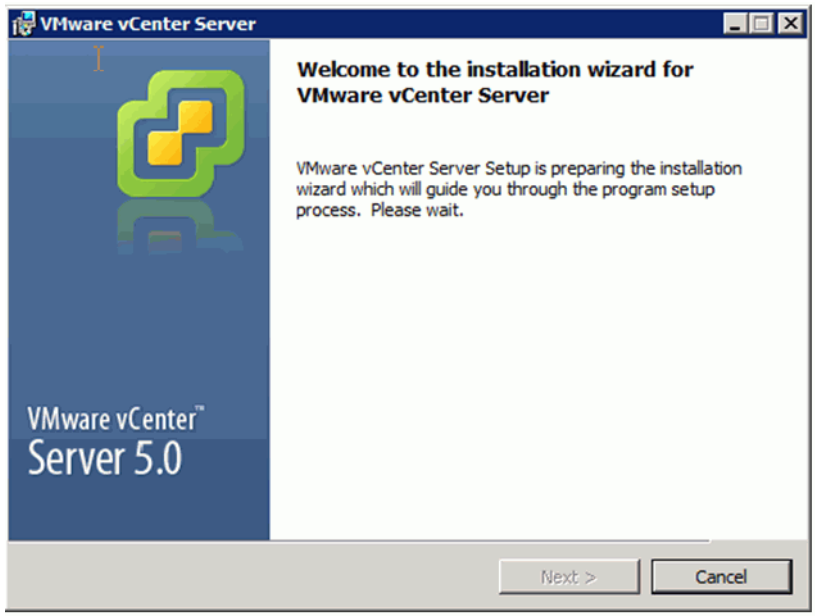


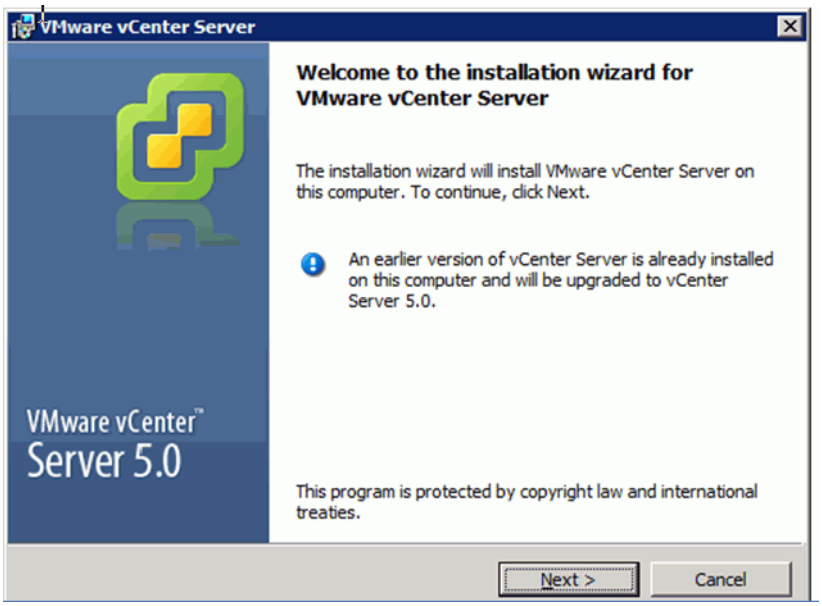
Make sure that microsoft.net 3.5 sp1 is installed:

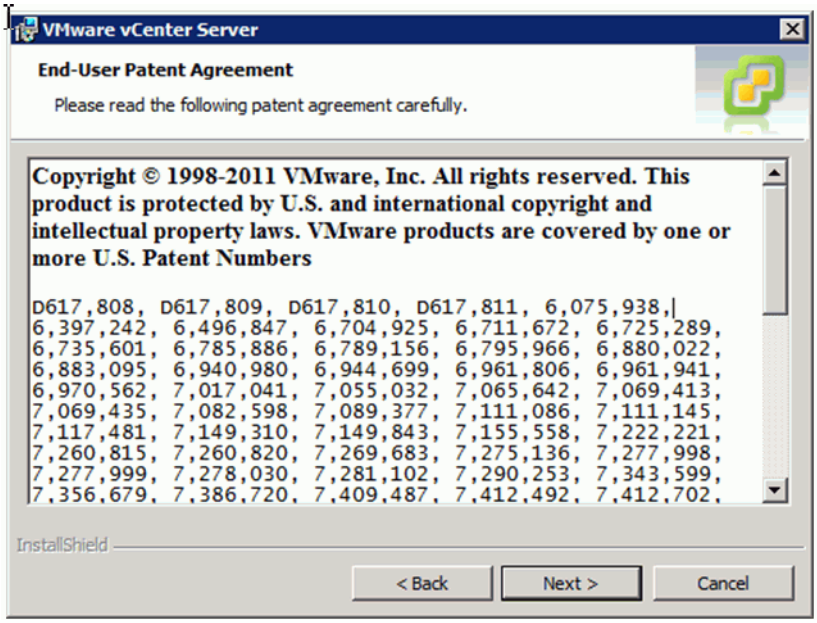


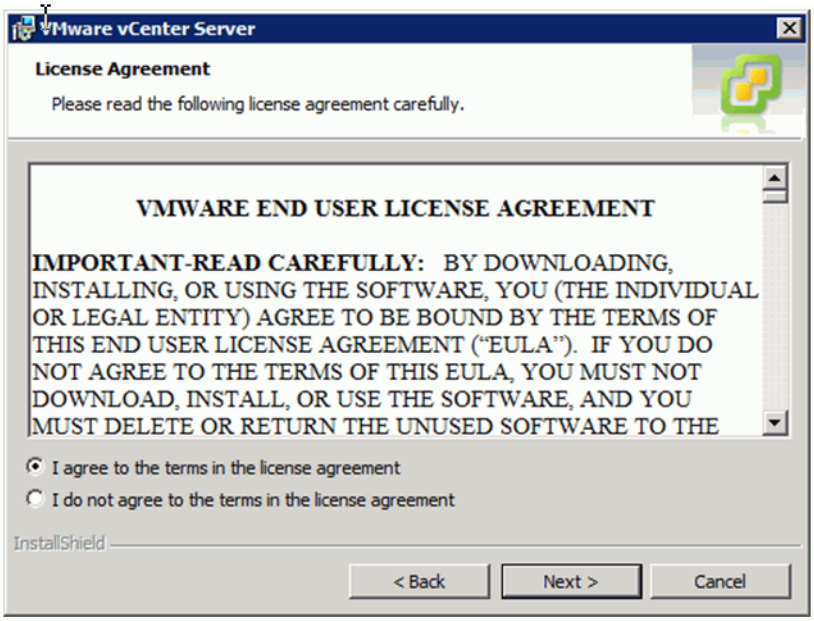


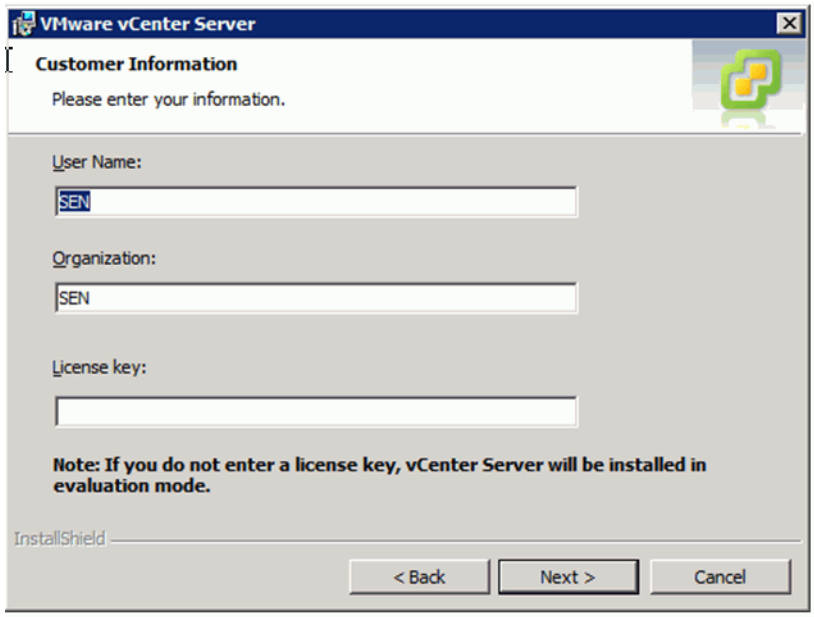
A few minutes later:

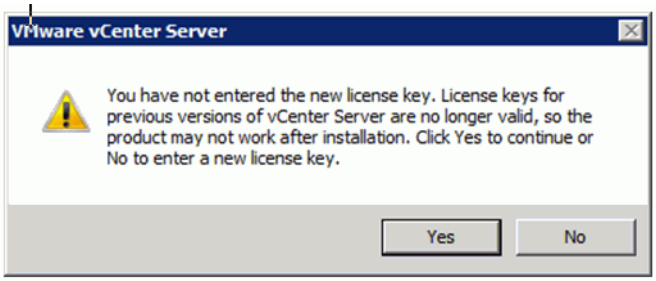

VMware vCenter Server
Welcome to the installation wizard for VMware vCenter Server
VMware vCenter Server Setup is preparing the installation wizard which will guide you through the program setup process. Please wait.
VMware vCenter™ Server 5.0
Next >
Cancel


VMware vCenter Server
Welcome to the installation wizard for VMware vCenter Server
The installation wizard will install VMware vCenter Server on this computer. To continue, click Next.
An earlier version of vCenter Server is already installed on this computer and will be upgraded to vCenter Server 5.0.
This program is protected by copyright law and international treaties.
VMware vCenter™ Server 5.0
Next >
Cancel

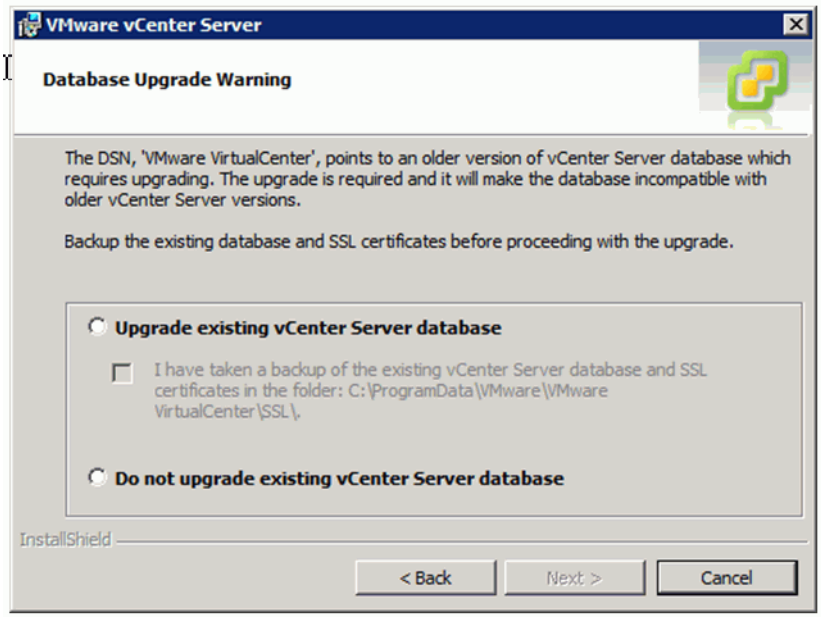

VMware vCenter Server
End-User Patent Agreement
Please read the following patent agreement carefully.
Copyright © 1998-2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more U.S. Patent Numbers
D617,808, D617,809, D617,810, D617,811, 6,075,938, 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,883,095, 6,940,980, 6,944,699, 6,961,806, 6,961,941, 6,970,562, 7,017,041, 7,055,032, 7,065,642, 7,069,413, 7,069,435, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,310, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,290,253, 7,343,599, 7,356,679, 7,386,720, 7,409,487, 7,412,492, 7,412,702,
InstallShield
< Back
Next >
Cancel

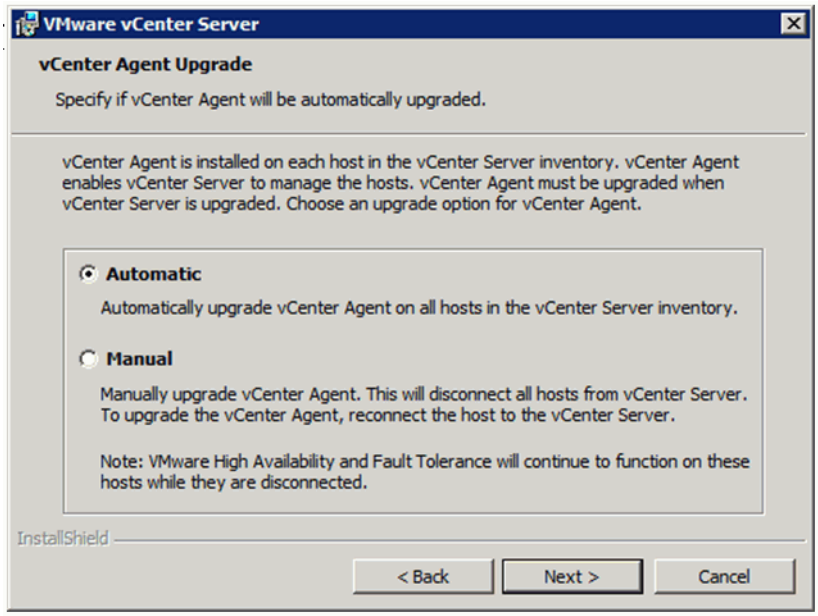

VMware vCenter Server
License Agreement
Please read the following license agreement carefully.
VMWARE END USER LICENSE AGREEMENT
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE
I agree to the terms in the license agreement
I do not agree to the terms in the license agreement
InstallShield
< Back
Next >
Cancel



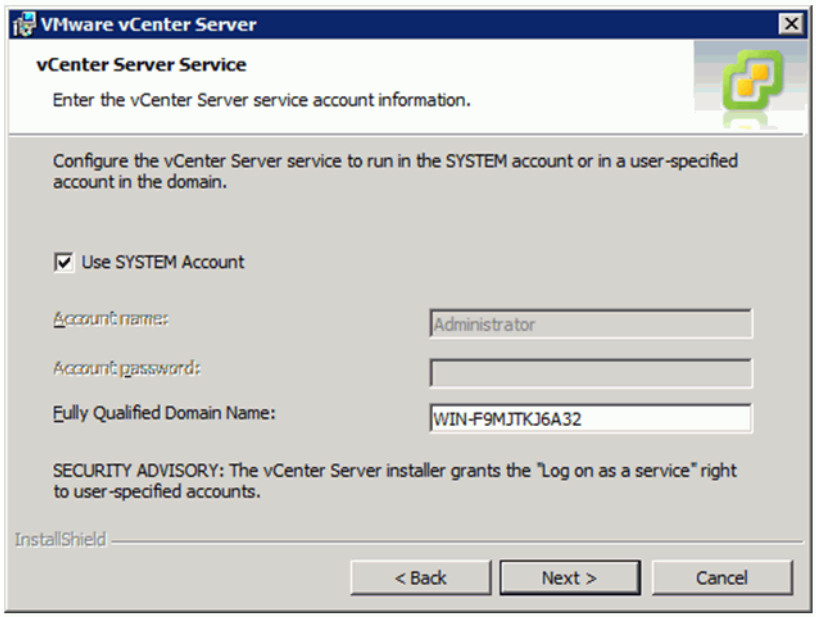


Enter **yes** (Enter license later.)

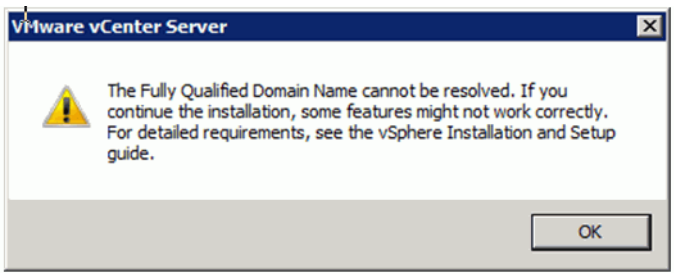

VMware vCenter Server
Database Upgrade Warning
The DSN, 'VMware VirtualCenter', points to an older version of vCenter Server database which requires upgrading. The upgrade is required and it will make the database incompatible with older vCenter Server versions.
Backup the existing database and SSL certificates before proceeding with the upgrade.
Upgrade existing vCenter Server database
I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\.
Do not upgrade existing vCenter Server database
InstallShield
< Back
Next >
Cancel


VMware vCenter Server
vCenter Agent Upgrade
Specify if vCenter Agent will be automatically upgraded.
vCenter Agent is installed on each host in the vCenter Server inventory. vCenter Agent enables vCenter Server to manage the hosts. vCenter Agent must be upgraded when vCenter Server is upgraded. Choose an upgrade option for vCenter Agent.
Automatic
Automatically upgrade vCenter Agent on all hosts in the vCenter Server inventory.
Manual
Manually upgrade vCenter Agent. This will disconnect all hosts from vCenter Server. To upgrade the vCenter Agent, reconnect the host to the vCenter Server.
Note: VMware High Availability and Fault Tolerance will continue to function on these hosts while they are disconnected.
InstallShield
< Back
Next >
Cancel

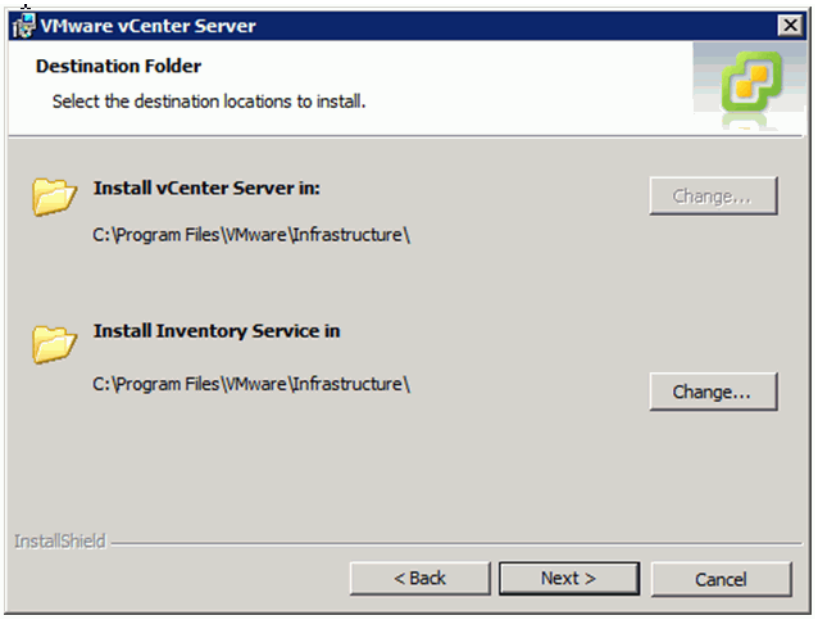
Next

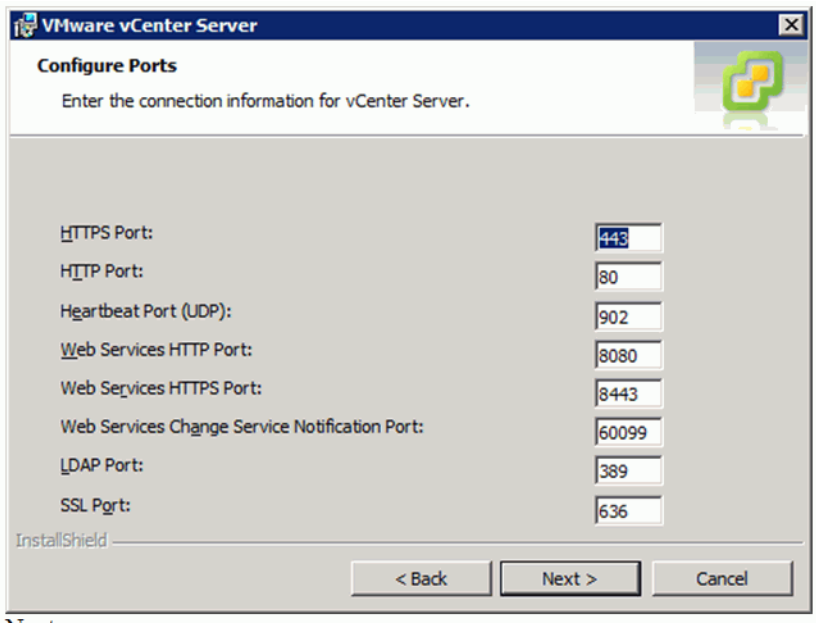


Next

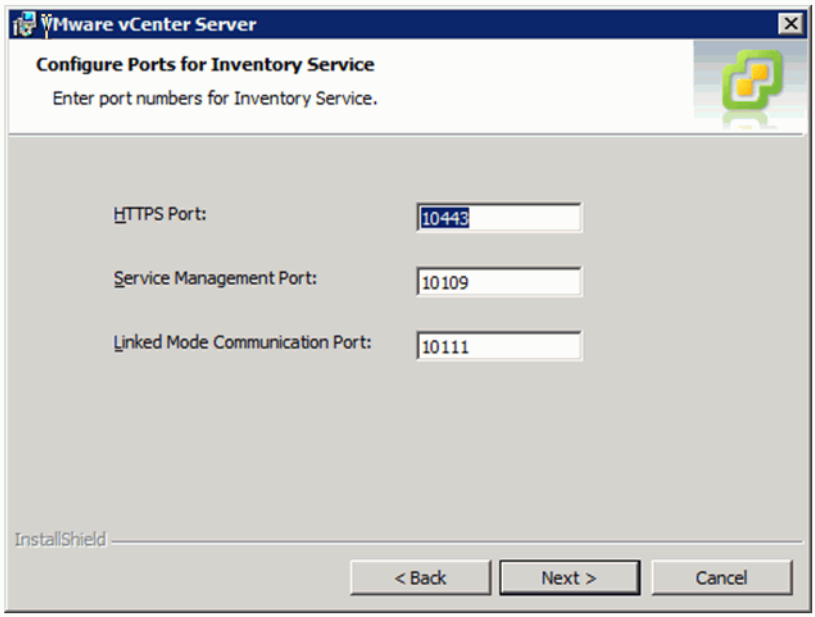


Or you can unselect the "use system account" and specify the username and password.

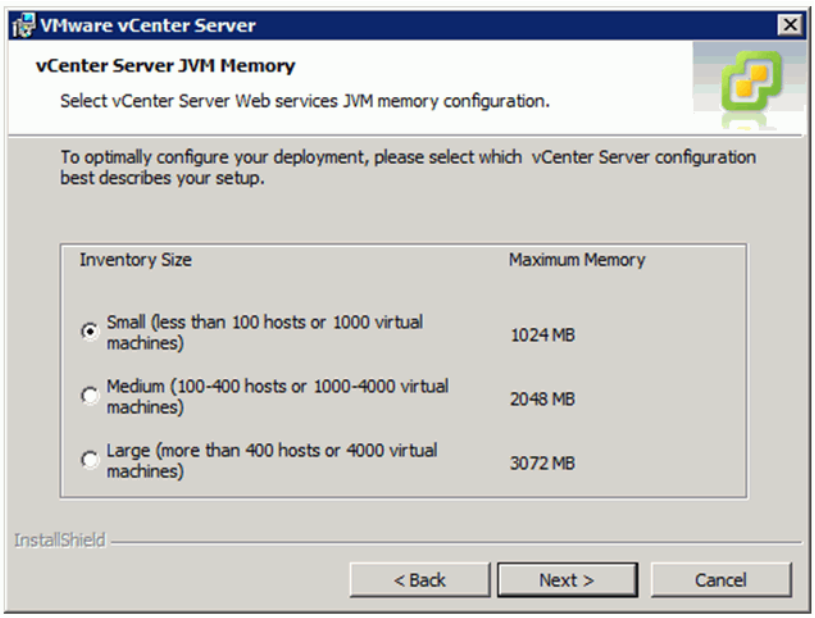

VMware vCenter Server
Destination Folder
Select the destination locations to install.
Install vCenter Server in:
C:\Program Files\VMware\Infrastructure\
Change...
Install Inventory Service in
C:\Program Files\VMware\Infrastructure\
Change...
InstallShield
< Back
Next >
Cancel


VMware vCenter Server
Configure Ports
Enter the connection information for vCenter Server.
HTTPS Port:
443
HTTP Port:
80
Heartbeat Port (UDP):
902
Web Services HTTP Port:
8080
Web Services HTTPS Port:
8443
Web Services Change Service Notification Port:
60099
LDAP Port:
389
SSL Port:
636
InstallShield
< Back
Next >
Cancel

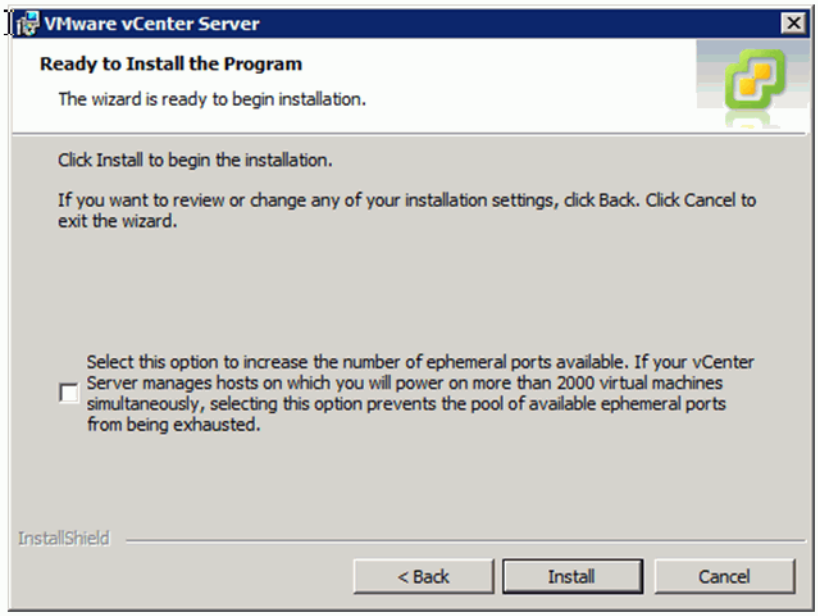
Next


VMware vCenter Server
Configure Ports for Inventory Service
Enter port numbers for Inventory Service.
HTTPS Port:
10443
Service Management Port:
10109
Linked Mode Communication Port:
10111
InstallShield
< Back
Next >
Cancel

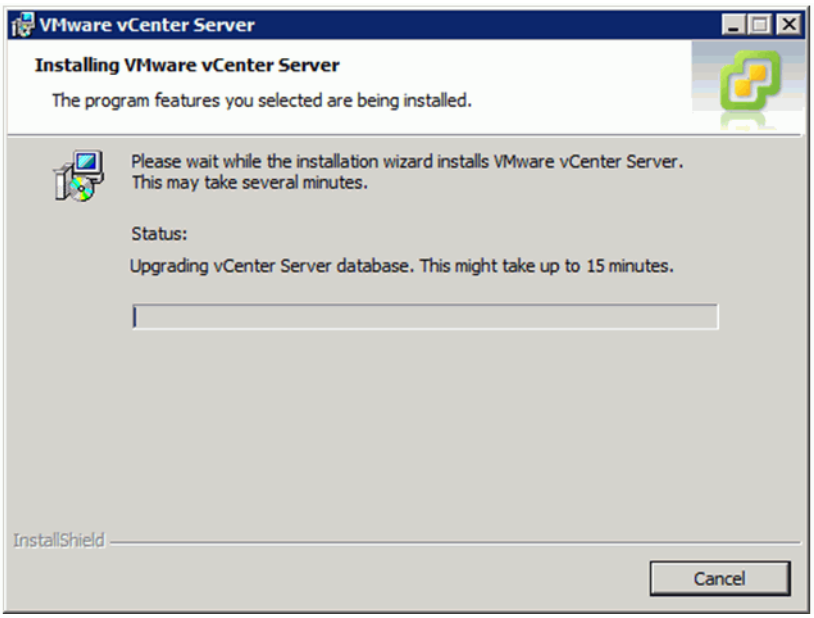
Next


VMware vCenter Server
vCenter Server JVM Memory
Select vCenter Server Web services JVM memory configuration.
To optimally configure your deployment, please select which vCenter Server configuration best describes your setup.
Inventory Size
Maximum Memory
Small (less than 100 hosts or 1000 virtual machines)
1024 MB
Medium (100-400 hosts or 1000-4000 virtual machines)
2048 MB
Large (more than 400 hosts or 4000 virtual machines)
3072 MB
InstallShield
< Back
Next >
Cancel

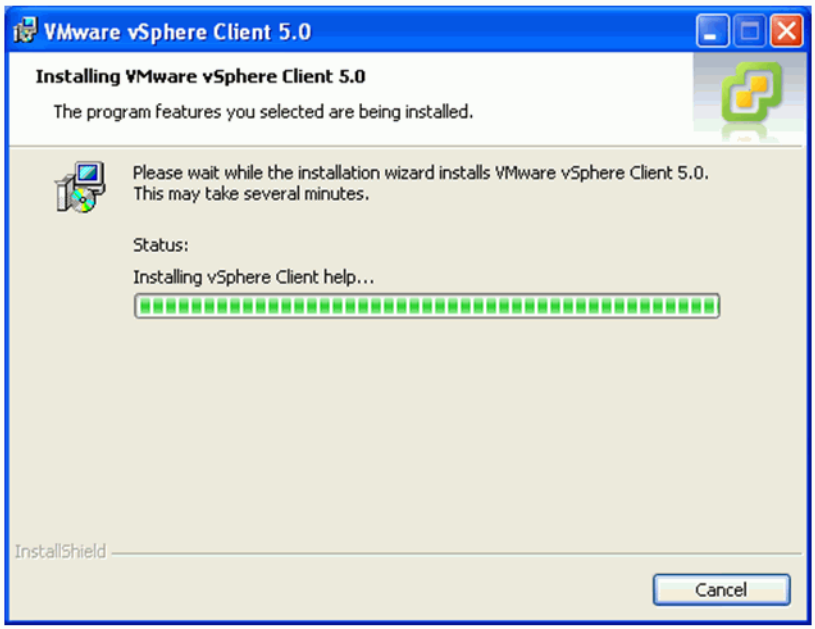
Next



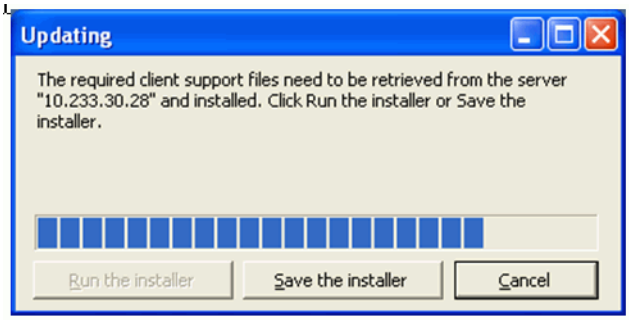
Install



Install the vSphere 5.0, from the vcenter iso file.



Once you try to use the V4.1 vSphere client to access the v5.0 center it will upgrade the client so you must make sure is it already installed.



Using the vSphere client login into the vcenter host 10.223.30.28 and verify you can still access the host and virtual machines that are in V4.1.

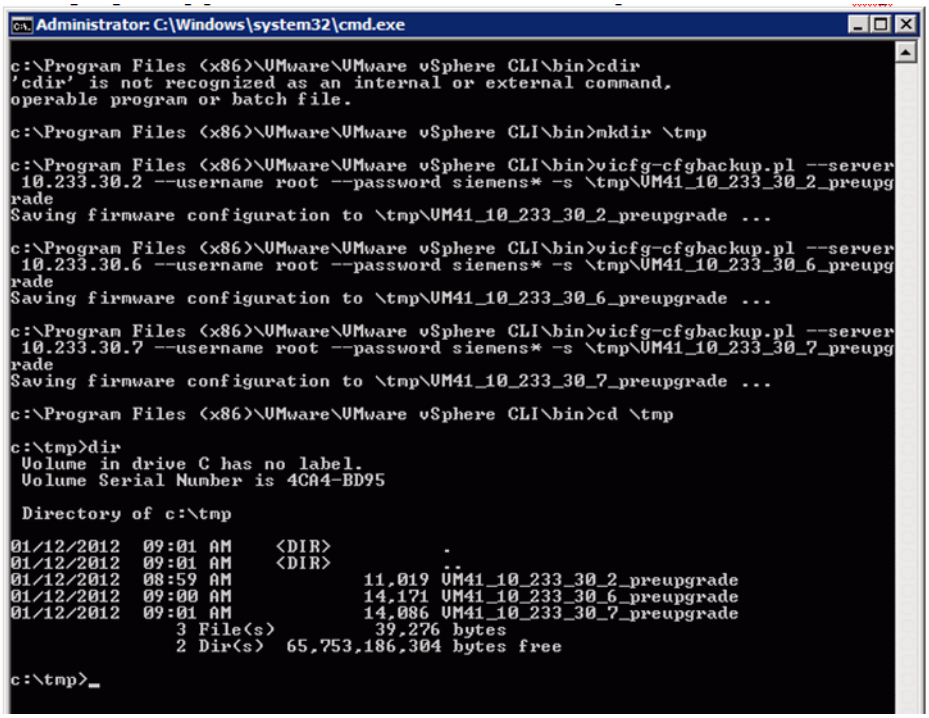
OKAY

25.4.3 Backing up our ESXi Host Configuration

Note: Page number references refer to the pages of the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

Note: Refer to page 32.

1. Install vCli.
2. Use vsp4_41_vcli_inst_script.pdf to install the vCLI
3. vicfg-cfgbackup.pl –server 10.233.30.2 –username root –password siemens* -s \tmp\



Copied these files to an external server.

25.4.4 Requirements

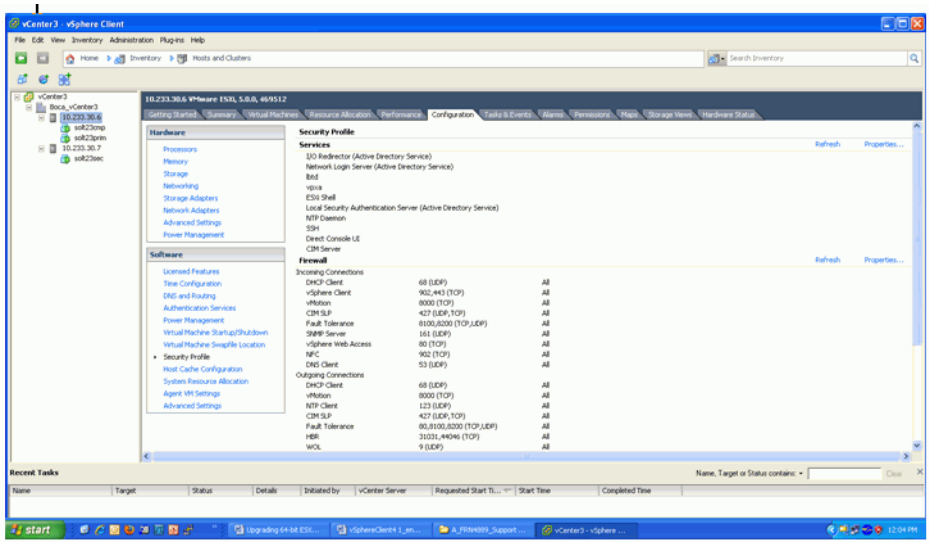
Note: Page 37 in the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

To verify the VMFS partition begins beyond the 1GB mark (sector 1843200)

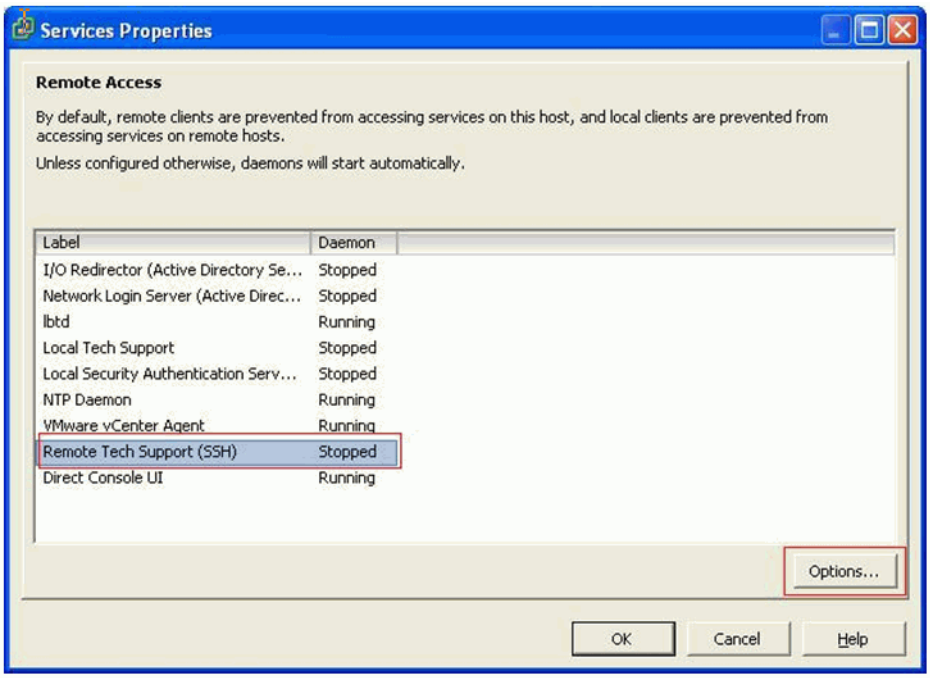
Using Vcenter: enable remote SSH to the host then execute the **fdisk -lu** command.

25.4.4.1 How to Enable Remote SSH

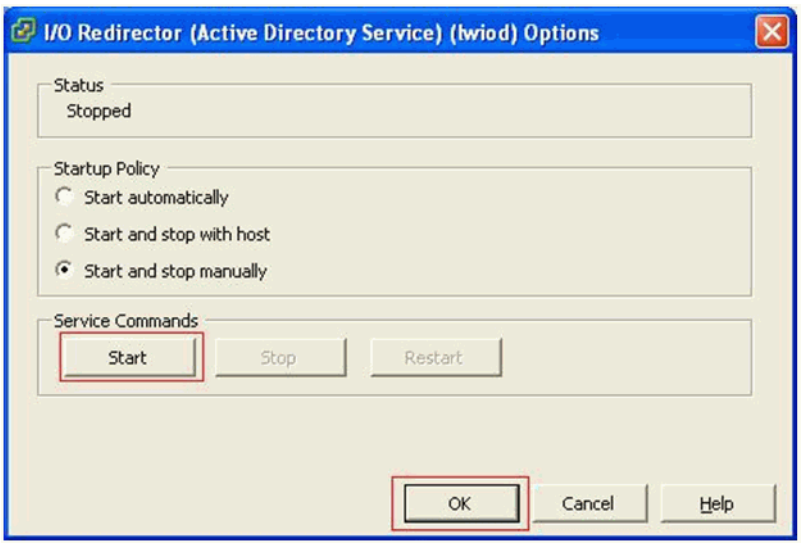
From the vSphere Client, select your **Host,** the **Configuration** tab**, Software Security Profile** and then **Properties**



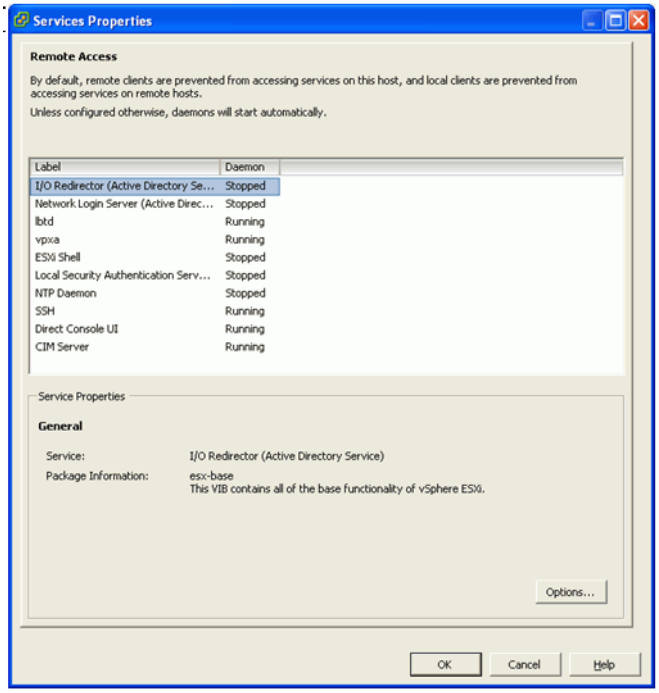
From the Service Properties window select the **Remote Tech Support (SSH)** Label (the Daemon should be Stopped) label then the **Options** button.



From the I/O Redirector Options window select your **Startup Policy** then the **Start** button … wait for the command to complete … after the command is successful select the **OK** button.



At the Service Properties window the **Remote Tech Support (SSH)** Label Daemon should be Running. Select the OK button. This completes the procedure. Remote access via SSH to the host should be enabled. The login credentials should be the same as those created for console access to the ESXi host.



SSH into host and execute the **fdisk –lu** command:

Verify the requirement**s** are met (page 33).

Verify the VMFS partition begins beyond the 1 GB mark (starts after sector 1843200) partitions as follows:

Disk /dev/disks/naa.600508e00000000052ad34814ce7e70d: 298.9 GB, 298999349248 bytes
64 heads, 32 sectors/track, 285148 cylinders, total 583983104 sector Units = sectors
of 1 * 512 = 512 bytes

Device Boot Start End Blocks Id System
/dev/disks/naa.600508e00000000052ad34814ce7e70dp1 8192 1843199 917504 5 Extended
/dev/disks/naa.600508e00000000052ad34814ce7e70dp2 1843200 10229759 4193280 6 FAT16
/dev/disks/naa.600508e00000000052ad34814ce7e70dp3 10229760 583983103 286876672 fb VMFS
/dev/disks/naa.600508e00000000052ad34814ce7e70dp4 * 32 8191 4080 4 FAT16 <32M
/dev/disks/naa.600508e00000000052ad34814ce7e70dp5 8224 520191 255984 6 FAT16
/dev/disks/naa.600508e00000000052ad34814ce7e70dp6 520224 1032191 255984 6 FAT16

```
/dev/disks/naa.600508e00000000052ad34814ce7e70dp7       1032224
1257471    112624    fc  VMKcore
/dev/disks/naa.600508e00000000052ad34814ce7e70dp8       1257504
1843199    292848    6  FAT16
```

25.4.5 Start the Upgrade using ESXi 5.0 Hypervisor DVD

Note: Page number references in this section refer to the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

25.4.5.1 Upgrading the Virtual Machines VMware Tools

Upgrade the VMware Tools:

For more details refer to the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

1. Right click the virtual machine.
2. Select **Guest**
3. Select **Install/Upgrade VMware Tools**

Upgrade Virtual Hardware:

For more details refer to the VMware vSphere 5.0 Upgrade Best Practices - Technical White Paper.

Attention: Do not upgrade the virtual hardware for virtual machines running in a mixed cluster made up of ESXi4.1 hosts and ESXi5.0 hosts. Only upgrade a virtual machine's virtual hardware version after all the hosts in the cluster have been upgraded to ESXi 5.0.

To upgrade the virtual hardware of a single virtual machine:

1. Start the vSphere Client or vSphere Web Client and log in to the vCenter Server.
2. Power off the virtual machine.
3. Right-click the virtual machine and select the menu option to upgrade virtual hardware.
   - In vSphere Client, the option is **Upgrade Virtual Hardware**.
   - In vSphere Web Client, the option is **Configuration** > **Upgrade Virtual Hardware**

The software upgrades the virtual hardware to the latest supported version.

Note: The Upgrade Virtual Hardware option appears if the virtual hardware on the virtual machine is not the latest supported version.

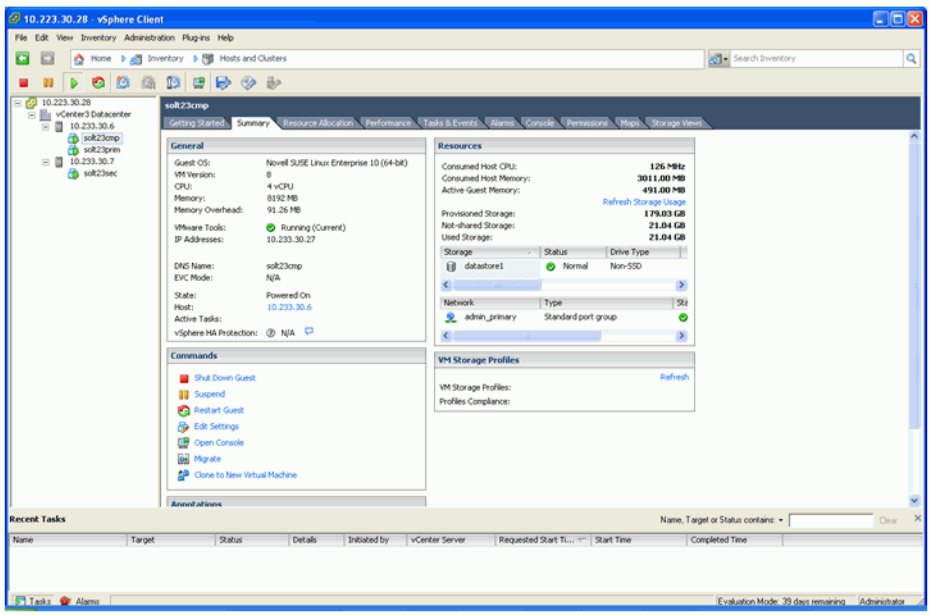
---

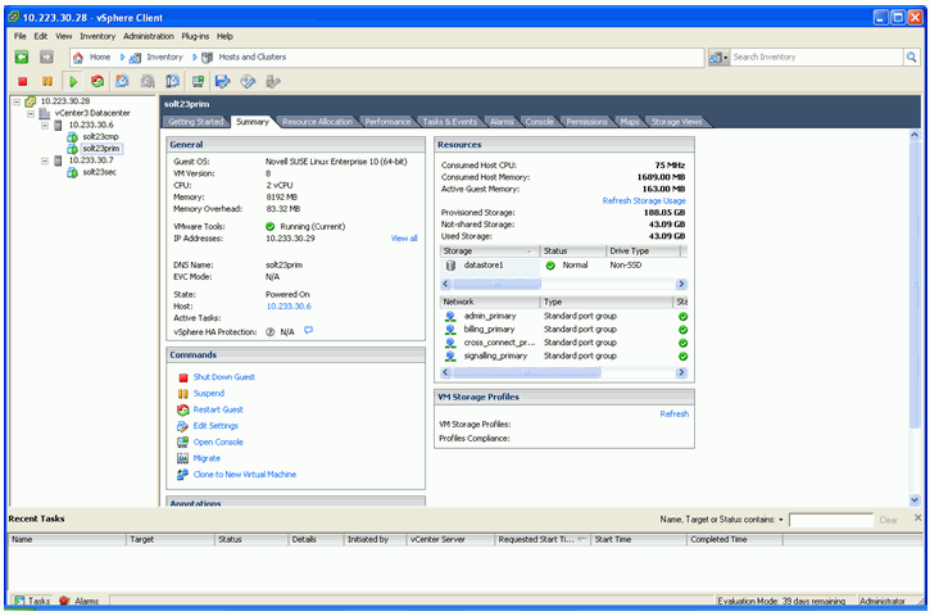
4. Click **Yes** to continue with the virtual hardware upgrade.
5. Power on the virtual machine.

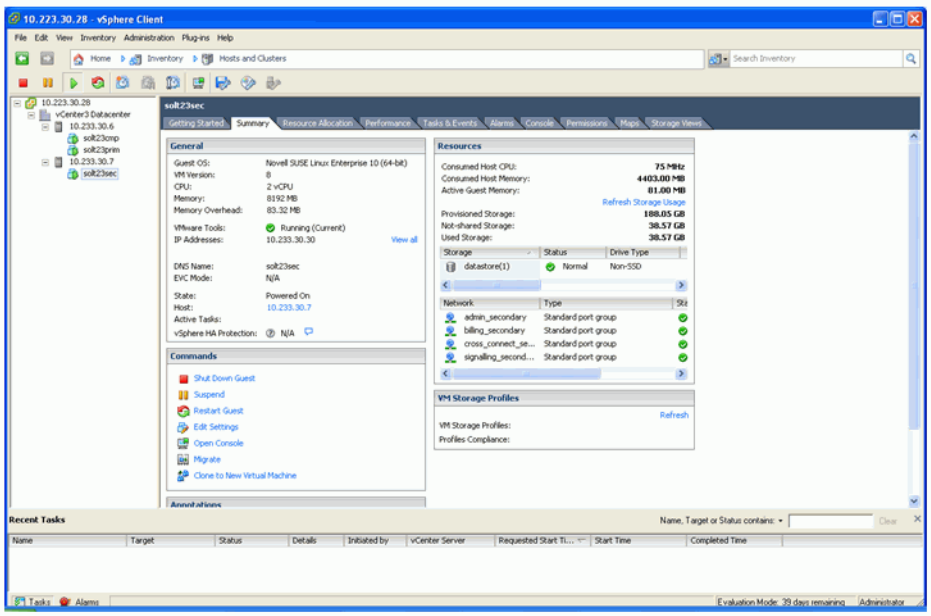
Note: If the virtual machine has a Microsoft Windows guest operating system, the operating system detects a new device, configures the device, and prompts you to reboot the guest operating system. If any unknown devices are recognized, the operating system prompts you to configure the device manually.

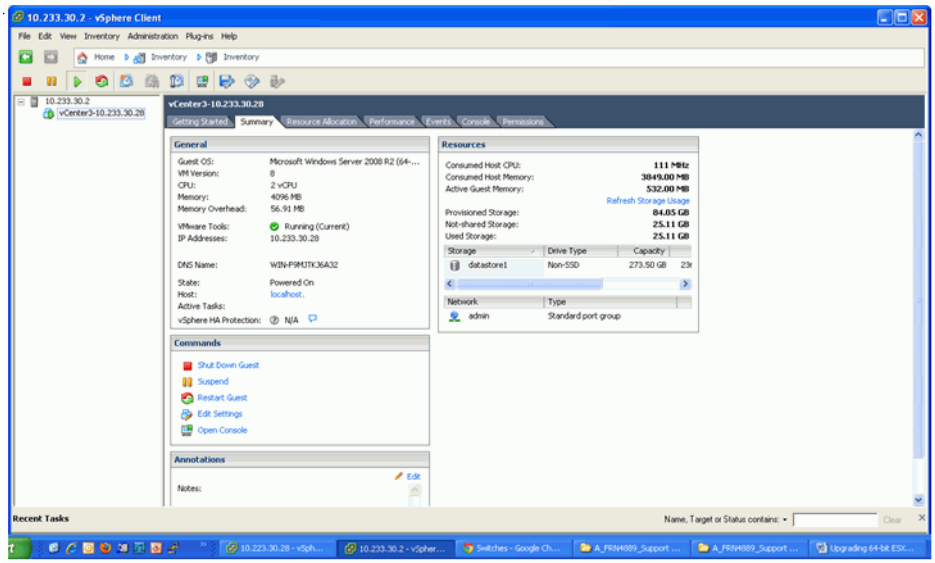
---

6. For Windows guest operating systems, reboot the guest operating system to make the changes take effect.




10.223.30.28 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
10.223.30.28
vCenter3 Datacenter
10.233.30.6
solt23cmp
solt23prim
10.233.30.7
solt23sec
solt23prim
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views
General
Guest OS: Novell SUSE Linux Enterprise 10 (64-bit)
VM Version: 8
CPU: 2 vCPU
Memory: 8192 MB
Memory Overhead: 83.32 MB
VMware Tools: Running (Current)
IP Addresses: 10.233.30.29 View all
DNS Name: solt23prim
EVC Mode: N/A
State: Powered On
Host: 10.233.30.6
Active Tasks:
vSphere HA Protection: N/A
Commands
Shut Down Guest
Suspend
Restart Guest
Edit Settings
Open Console
Migrate
Clone to New Virtual Machine
Resources
Consumed Host CPU: 75 MHz
Consumed Host Memory: 1689.00 MB
Active Guest Memory: 163.00 MB
Refresh Storage Usage
Provisioned Storage: 188.05 GB
Not-shared Storage: 43.09 GB
Used Storage: 43.09 GB
Storage Status Drive Type
datastore1 Normal Non-SSD
Network Type
admin_primary Standard port group
billing_primary Standard port group
cross_connect_pr... Standard port group
signalling_primary Standard port group
VM Storage Profiles
Refresh
VM Storage Profiles:
Profiles Compliance:
Recent Tasks
Name, Target or Status contains:
Name Target Status Details Initiated by vCenter Server Requested Start Ti... Start Time Completed Time
Tasks Alarms
Evaluation Mode: 39 days remaining Administrator


10.223.30.28 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
10.223.30.28
vCenter3 Datacenter
10.233.30.6
solt23cmp
solt23prim
10.233.30.7
solt23sec
solt23sec
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views
General
Guest OS: Novell SUSE Linux Enterprise 10 (64-bit)
VM Version: 8
CPU: 2 vCPU
Memory: 8192 MB
Memory Overhead: 83.32 MB
VMware Tools: Running (Current)
IP Addresses: 10.233.30.30 View all
DNS Name: solt23sec
EVC Mode: N/A
State: Powered On
Host: 10.233.30.7
Active Tasks:
vSphere HA Protection: N/A
Commands
Shut Down Guest
Suspend
Restart Guest
Edit Settings
Open Console
Migrate
Clone to New Virtual Machine
Resources
Consumed Host CPU: 75 MHz
Consumed Host Memory: 4403.00 MB
Active Guest Memory: 81.00 MB
Refresh Storage Usage
Provisioned Storage: 188.05 GB
Not-shared Storage: 38.57 GB
Used Storage: 38.57 GB
Storage Status Drive Type
datastore(1) Normal Non-SSD
Network Type
admin_secondary Standard port group
billing_secondary Standard port group
cross_connect_se... Standard port group
signalling_second... Standard port group
VM Storage Profiles
Refresh
VM Storage Profiles:
Profiles Compliance:
Recent Tasks
Name, Target or Status contains:
Name Target Status Details Initiated by vCenter Server Requested Start Ti... Start Time Completed Time
Tasks Alarms
Evaluation Mode: 39 days remaining Administrator


10.233.30.2 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.233.30.2
vCenter3-10.233.30.28
vCenter3-10.233.30.28
Getting Started Summary Resource Allocation Performance Events Console Permissions
General
Guest OS: Microsoft Windows Server 2008 R2 (64-...
VM Version: 8
CPU: 2 vCPU
Memory: 4096 MB
Memory Overhead: 56.91 MB
VMware Tools: Running (Current)
IP Addresses: 10.233.30.28
DNS Name: WIN-P9MJTKJ6A32
State: Powered On
Host: localhost.
Active Tasks:
vSphere HA Protection: N/A
Resources
Consumed Host CPU: 111 MHz
Consumed Host Memory: 3849.00 MB
Active Guest Memory: 532.00 MB
Refresh Storage Usage
Provisioned Storage: 84.05 GB
Not-shared Storage: 25.11 GB
Used Storage: 25.11 GB
Storage Drive Type Capacity
datastore1 Non-SSD 273.50 GB
Network Type
admin Standard port group
Commands
Shut Down Guest
Suspend
Restart Guest
Edit Settings
Open Console
Annotations
Edit
Notes:
Recent Tasks
Name, Target or Status contains:
Clear

26 Modifying the */etc/hosts* file

Note: These procedures should be followed for */etc/hosts* file updates that are executed as part of normal operating procedures. **Not as part of the Upgrade/ Migration section titled** **Section 8.4.7, "Verify the Hosts File Configuration", on page 465****.**

Attention: In a Simplex OSV configuration, this activity will result in a complete loss of service for the duration of the process.

Attention: For a correctly configured duplex system, each node can be configured individually without a loss of call processing. If you need call processing to remain active, do not shutdown both nodes of a duplex system at the same time.

Note: Although these actions should not result in an outage for a Duplex OSV system it is recommended that this update activity for Simplex **and Duplex OSV** systems be conducted in a maintenance window.

Before starting this procedure it is recommended the current */etc/hosts* file be backed up or saved to an external server for safe keeping, in case the OSV behavior after this update requires that the original */etc/hosts* file be restored.

There are two purposes for modifying the Hosts file

1. Adding additional Hosts
2. Modifying an existing Host entry

After the modification the node (or nodes of a duplex OSV) will have to be configured from state 4 to state 3, and then back to state 4 to ensure the caches are refreshed with the new data.

Please review this entire procedure before proceeding with the actual updates.

Attention: Any questions regarding this appendix should be addressed to your next level of support.

This appendix is subdivided into these sections:

- Section 26.1, "Adding Additional Hosts", on page 776

- Section 26.2, “Modifying an Existing Host Entry”, on page 777
- Section 26.3, “Configuring the Nodes to Complete the Update Process”, on page 777

Attention: If the procedure is completed and it is then decided the original /etc/hosts file configuration must be restored; the configuration steps of **Section 26.3, “Configuring the Nodes to Complete the Update Process”, on page 777** must be repeated to ensure the OSV cache is updated correctly.

26.1 Adding Additional Hosts

Logic has been implemented for the */etc/hosts* file wherein a new banner, "Please add new hosts under this line", indicates to OpenScape Voice tools (e.g. Upgrade/Migration tools) that the Ipaddress-hostname entries that appear below the banner are created by the user. Employing the banner as such allows these OpenScape Voice tools to carry forward user-created entries in the *hosts* file during activities that require the *hosts* file to be rebuilt. **The hosts above the banner are created from the node.cfg file during installation and should be modified by the EZIP (IFGUI Update) function only.**

Verify the OpenScape Voice */etc/hosts* file (or files for Duplex systems) configuration with the following commands (execute on both nodes in Duplex system):

cd /etc

cat **hosts**

A truncated example of a */etc/hosts* file with the new banner (and no user-created entries) is as follows:

10.235.54.10 rtp_com0_eth6
10.235.54.30 rtp_com1_eth6
##
Please add new **hosts** under this line
##

For Duplex systems, the */etc/hosts* file of both nodes will need to be updated and kept in sync. Duplicate entries in the */etc/hosts* file should be avoided.

In the following example, the nmcsnmptrap and host_pc are user-created entries in the *hosts* file containing the new banner. If a user-created entry needs to be moved from above the banner, place it as the last line (bottom of the list below the banner) in the */etc/hosts* file. Remember to update both */etc/hosts* files in a Duplex system.

```
10.235.54.10 rtp_com0_eth6
10.235.54.30 rtp_com1_eth6
##########################################
# Please add new hosts under this line
##########################################
10.235.200.230  nmcsnmptrap
10.235.200.29 host_pc
```

26.2 Modifying an Existing Host Entry

If the entry is above the "Please add new hosts under this line" banner, this is a system generated entry. **The hosts above the banner are created from the node.cfg file during installation and should be modified by the EZIP (IFGUI Update) function only. This will ensure that the node.cfg and the *hosts* file will remain consistent.** Additionally, after modifying these parameters, EZ-IP will notify the user if the nodes are to be rebooted.

If the entry is below the "Please add new hosts under this line" banner this is a user added host entry (or entries). The entry may be directly modified but the signaling managers will not become aware of this change because the signaling manager has already successfully resolved this host and the information is now cached.

26.3 Configuring the Nodes to Complete the Update Process

Attention: For a correctly configured duplex system, each node can be configured individually without a loss of call processing. If you need call processing to remain active, do not shutdown both nodes of a duplex system at the same time.

Attention: In a Simplex configuration, this activity will result in a complete loss of service for the duration of the process.

Note: Although these actions should not result in an outage for a Duplex OSV system it is recommended that this update activity for Simplex **and Duplex OSV** systems be conducted in a maintenance window.

The */etc/hosts* file entry may be directly modified but the signaling managers will not become aware of this change because the signaling manager has already successfully resolved this host and the information is now cached. The only

method of forcing the signaling manager to update its cache is by process restart(s). As it may not be intuitively obvious which signaling managers are referencing that host (e.g. SIP, CSTA etc.), it is recommended that each node be brought to run level 3 and back to level 4 via the srxctrl command one node at a time in a Duplex OSV.

26.3.1 Example Configuration Sequences

26.3.1.1 Node 1

The srxctrl command is found at /unishpere/srx3000/srx/startup/srxctrl.

a) From node 1, configure node 1 to state 3 by executing the following commands (as user *root*);

 # /unisphere/srx3000/srx/startup/srxctrl 3 0

The node should be at state 3 when the system displays a message similar to this:

--- srxctrl ended on Wed May 27 13:52:27 2009 ---

Verify the status of the node with the command:

 # /unisphere/srx3000/srx/startup/srxqry

It is expected that the node will be at state 3 at this time.

b) Configure node 1 to state 4 by executing the following commands (as user *root*);

 # /unisphere/srx3000/srx/startup/srxctrl 4 0

The node should be at state 4 when the system displays a message similar to this:

--- srxctrl ended on Wed May 27 13:52:27 2009 ---

Verify the status of the node with the command:

 # /unisphere/srx3000/srx/startup/srxqry

c) It is expected that the node will be at state 4 at this time. **For all OSV configurations confirm all processes are running (srxqry -v) and call processing is in progress.**

 # /unisphere/srx3000/srx/startup/srxqry -v

This completes the configuration sequence in a Simplex OSV.

For Duplex OSV systems: After confirming node 1 is at sate 4, all processes are running and the node is processing calls proceed to Section 26.3.1.2, “Node 2”, on page 779.

26.3.1.2 Node 2

The srxctrl command is found at /unishpere/srx3000/srx/startup/srxctrl.

a) From node 2, configure node 2 to state 3 by executing the following commands (as user *root*);

 # /unisphere/srx3000/srx/startup/srxctrl 3 0

The node should be at state 3 when the system displays a message similar to this:

--- srxctrl ended on Wed May 27 13:52:27 2009 ---

Verify the status of the node with the command:

 # /unisphere/srx3000/srx/startup/srxqry

It is expected that the node will be at state 3 at this time.

b) Configure node 2 to state 4 by executing the following command (as user *root*);

 # /unisphere/srx3000/srx/startup/srxctrl 4 0

The node should be at state 4 when the system displays a message similar to this:

--- srxctrl ended on Wed May 27 13:52:27 2009 ---

Verify the status of the node with the command:

 # /unisphere/srx3000/srx/startup/srxqry

c) It is expected that the node will be at state 4 at this time. **For all OSV configurations confirm all processes are running (srxqry -v) and call processing is in progress.**

 # /unisphere/srx3000/srx/startup/srxqry -v

This completes the configuration sequence for a Duplex OSV.

Attention: If the procedure is completed and it is then decided the original */etc/hosts* file configuration must be restored; after the original hosts file is restored the configuration steps of Section 26.3.1.1, “Node 1” and Section 26.3.1.2, “Node 2” must be repeated, to ensure the OSV cache is updated correctly.

---

27 Modifying the */etc/sysconfig/proxy-osv* file

The reason to modify the *proxy-osv* file is to enable the CloudLink Daemon (CLD) and the CloudLink Gateway running on OSV, to have internet access using a proxy configuration.

Before starting this procedure it is recommended the current */etc/sysconfig/proxy-osv* file be backed up or saved to an external server for safe keeping, in case the OSV behavior after this update requires that the original file be restored.

After the modification, duplex OSV nodes will have to be configured from state 4 to state 3, and then back to state 4 to ensure the caches are refreshed with the new data. This procedure must be performed on both nodes of the duplex OSV.

Please review this entire procedure before proceeding with the actual updates.

Proxy configuration file:

The proxy settings are managed in */etc/sysconfig/proxy-osv* file. This file adheres to the same syntax as the standard */etc/sysconfig/proxy* file, commonly used in Linux environments. The supported variables include:

HTTP_PROXY: Specifies the proxy server for HTTP connections. Examples:

HTTP_PROXY="http://<proxy-server>:<port>"

HTTP_PROXY="http://123.123.123.123:8080"

HTTPS_PROXY: Specifies the proxy server for HTTPS connections. Examples:

HTTPS_PROXY="http://<proxy-server>:<port>"

HTTPS_PROXY="http://123.123.123.123:8080"

NO_PROXY: Defines a comma-separated list of hosts, IPs, or domains to bypass the proxy. In NO_PROXY, the IP of CMP should also be added, using port 8289.

Examples:

NO_PROXY="localhost, 127.0.0.1, example.com"

NO_PROXY="localhost, 127.0.0.1"

NO_PROXY="localhost, 127.0.0.1, 11.12.13.14:8289"

Note: On OSV upgrades, the *proxy-osv* file will be migrated. Thus, once configured, the proxy configuration will not be affected by any upgrade or re-configuration actions performed in the system.

---

28 Guidelines for Language and Application Package adds to Simplex Systems

28.1 Overview

You should have arrived at this section from one of the following sections;

- Section 2.2.4, “OpenScape Voice Installation Checklist”, step 30 on page 36
- Section 5.2.3.4, “Adding Additional Packages/Languages”, on page 307
- Section 8.5, “Upgrade of an OSV Integrated Simplex System”, step 16 on page 482
- Section 9.1.1, “Simplex to Simplex Migration”, step 16.

This section contains Language package tables and examples for the installation of additional language packages in integrated simplex OSVs. All supported packages for each additional language should be installed.

Attention: If it is decided to install the additional packages at a later date it is recommended this activity take place in a maintenance window because the affected Applications server will be out-of-service for the duration of the package add(s). Any features provided by the Applications server will be unavailable for the duration of the package addition(s).

Sections U.2 through Section U.8 list the available language packages. Command examples are included.

Section U.9 describes the steps to install media server announcements in a Simplex OSV. This section may be used a guideline for installing other language or application packages.

Section U.10 describes the steps to clean up the repository after the package adds are complete. These steps should not be executed until it is verified the package adds are complete. If a repository is not already set up; Section 28.9, “Procedure Example for Media Server Languages”, on page 789 has a link to Section 5.2.10, “Providing a Setup Medium for the Applications”. After the Section 5.2.10 procedure is complete, a link back to Section 28.9 is provided.

It is recommended the installation repository be created with the 'Base', 'Repository' and the additional application and language packages that are required. Please include the English language package ISO in the installation repository. These files would be found in the initial build package for the current

Applications version. Example given; If the Applications server is at the V10 FR0 H1 (BUILD 12 H1) level, the required ISO files will be in the repository for V10FR0 (BUILD 12).

28.1.1 Language Package Add Syntax

The syntax of the language add command is;

sh support/installIntegratedSimplex.sh addLang <component> <lang lang>

Section U.2 through Section U.8 list language package command examples.

28.1.2 Applications Package Add Syntax

If applications files are required and this is an integrated Simplex OSV use the following syntax to install the application;

sh support/installIntegratedSimplex.sh addApp <application>

Examples of the addApp command;

 # sh support/installIntegratedSimplex.sh addApp Nrec
 # sh support/installIntegratedSimplex.sh addApp uc-asr
 # sh support/installIntegratedSimplex.sh addApp mediaserver_voiceportalspeech

28.2 Supported Languages for Announcement Texts of the Media Server for PBXs

Country	Language	Language Code	Individual System Announcements	Pre-configured Fallback Language	ISO File[1]
Argentina	Spanish (Argentina)	es_ar	✓		Spanish
Australia	English (AU)	en_au		en	English
Brazil	Portuguese (Brazil)	pt_br	✓		Portuguese
Belgium	Flemish	nl_be		nl	AdditionalLanguages
Bulgaria	Bulgarian	bg	✓		AdditionalLanguages
Bosnia-Herzegovina	Bosnian	bs		sr	AdditionalLanguages
Chile	Spanish (Chile)	es_cl		es_ar	Spanish
People's Republic of China	Chinese (simplified)	zh	✓		Chinese
Denmark	Danish	da	✓		AdditionalLanguages
Germany	German	de	✓		German
Ecuador	Spanish (Ecuador)	es_ec		es_mx	Spanish
Estonia	Estonian	et	✓		AdditionalLanguages
Finland	Finnish	fi	✓		AdditionalLanguages
France	French	fr	✓		French
Greece	Greek	el	✓		AdditionalLanguages
Great Britain	English (UK)	en	✓		English
Hongkong	Chinese (Hongkong)	zh_hk		en_us	Chinese
India	English (India)	en_in		en	English
Indonesia	Indonesian	id		en_us	AdditionalLanguages
Italy	Italian	it	✓		Italian
Japan	Japanese	Yes		en_us	AdditionalLanguages
Canada	French (Canada)	fr_ca	✓		French
Colombia	Spanish (Colombia)	es_co		es_mx	Spanish
Korea	Korean	ko		en_us	AdditionalLanguages
Croatia	Croatian	hr	✓		AdditionalLanguages
Latvia	Latvian	lv	✓		AdditionalLanguages
Lithuania	Lithuanian	lt		en	AdditionalLanguages
Malaysia	Malay	ms		en_us	AdditionalLanguages
Morocco	French	fr_ma		fr	French
Mexico	Spanish (Mexico)	es_mx	✓		Spanish
Netherlands	Dutch	nl	✓		AdditionalLanguages
Norway	Norwegian	no	✓		AdditionalLanguages
Austria	German	de_at		de	German
Peru	Spanish (Peru)	es_pe		en_mx	Spanish
Philippines	English (Philippines)	en_ph		en_us	English
Poland	Polish	pl	✓		AdditionalLanguages
Portugal	Portuguese (Portugal)	pt	✓		Portuguese
Romania	Romanian	ro	✓		AdditionalLanguages
Russia	Russian	ru[2]	✓		AdditionalLanguages
Sweden	Swedish	sv	✓		AdditionalLanguages
Serbia	Serbian	sr	✓		AdditionalLanguages
Singapore	Chinese (Singapore)	zh_sg		en_us	Chinese
Slovakia	Slovakian	sk	✓		AdditionalLanguages
Slovenia	Slovenian	sl	✓		AdditionalLanguages
Spain	Spanish	es	✓		Spanish
South Africa	English (ZA)	en_za		en	English
Taiwan	Chinese (Taiwan)	zh_tw		en_us	Chinese
Thailand	Thai	th		en_us	AdditionalLanguages
Czech Republic	Czech	cs	✓		AdditionalLanguages
Turkey	Turkish	tr	✓		AdditionalLanguages
Hungary	Hungarian	hu	✓		AdditionalLanguages
USA	English (US)	en_us	✓		English
Venezuela	Spanish (Venezuela)	es_ve		es_mx	Spanish
United Arab Emirates	Arabian	ar	✓		AdditionalLanguages

Single package install example;

```
# sh support/installIntegratedSimplex.sh addLang
mediaserver_announcements en_za
```

Multiple package install example;

```
# sh support/installIntegratedSimplex.sh addLang
mediaserver_announcements de es
```

28.3 Language Codes of the supported TTS Languages

Language	Country	Language Code	ISO File[1]
Chinese (Mandarin)	China	zh_cn	Chinese
German	Germany	de_de	German
English	Great Britain	en_gb	English
English	USA	en_us	English
French	France	fr_fr	French
Italian	Italy	it_it	Italian
Portuguese (Portugal)	Portugal	pt_pt	Portuguese
Portuguese (Brazil)	Brazil	pt_br	Portuguese
Russian	Russia	ru_ru[2]	AdditionalLanguages
Spanish	Spain	es_es	Spanish

Single package install example;

```
# sh support/installIntegratedSimplex.sh addLang uc-tts de_de
```

Multiple package install example;

```
# sh support/installIntegratedSimplex.sh addLang uc-tts es_es
fr_fr
```

28.4 Media Server Autoattendant Packages Codes

Language	Country	Language Code	ISO File[1]
Chinese (Mandarin)	China	ZH_CN	Chinese
German	Germany	DE_DE	German
English	Great Britain	EN_GB	English
English	USA	EN_US	English
French	France	FR_FR	French
Italian	Italy	IT_IT	Italian
Portuguese	Portugal	PT_PT	Portuguese
Portuguese	Brazil	PT_BR	Portuguese
Russian	Russia	RU_RU[2]	AdditionalLanguages
Spanish	Spain	ES_ES	Spanish

Single package install example;

```
# sh support/installIntegratedSimplex.sh addLang
mediaserver_autoattendant_languagepack DE-DE
```

Multiple package install example;

```
# sh support/installIntegratedSimplex.sh addLang
mediaserver_autoattendant_languagepack ES-ES FR-FR
```

28.5 Media Server Voice Portal Language Package Codes

Language	Country	Language Code	ISO File[1]
Chinese (Mandarin)	China	ZH_CN	Chinese
German	Germany	DE_DE	German
English	Great Britain	EN_GB	English
English	USA	EN_US	English
French	France	FR_FR	French
Italian	Italy	IT_IT	Italian
Portuguese	Portugal	PT_PT	Portuguese
Portuguese	Brazil	PT_BR	Portuguese
Russian	Russia	RU_RU[2]	AdditionalLanguages
Spanish	Spain	ES_ES	Spanish

Single package install example;

```
#sh support/installIntegratedSimplex.sh addLang
mediaserver_voiceportal_languagepack DE-DE
```

Multiple package install example;

```
# sh support/installIntegratedSimplex.sh addLang
mediaserver_voiceportal_languagepack ES-ES FR-FR
```

28.6 Language Codes of the supported Conferencing Languages

Language	Country	Language Code	ISO File[1]
Chinese (Mandarin)	China	zh_cn	Chinese
German	Germany	de_de	German
English	Great Britain	en_gb	English
English	USA	en_us	English
French	France	fr_fr	French
Italian	Italy	it_it	Italian
Portuguese	Portugal	pt_pt	Portuguese
Portuguese	Brazil	pt_br	Portuguese
Spanish	Spain	es_es	Spanish
Dutch	Netherlands	nl_nl	AdditionalLanguages
Russian	Russia	ru_ru[2]	AdditionalLanguages
Turkish	Turkey	tr_tr	AdditionalLanguages

Single package install example;

```
# sh support/installIntegratedSimplex.sh addLang
scs_conferencing_languagepack de_de
```

Multiple package install example;

```
# sh support/installIntegratedSimplex.sh addLang
scs_conferencing_languagepack es_es fr_fr
```

28.7 Language Codes of the supported ASR Languages

Language	Country	Language Code	ISO File[1]
German	Germany	de_de	German
English	USA	en_us	English

```
# sh support/installIntegratedSimplex.sh addLang uc-asr en_us
# sh support/installIntegratedSimplex.sh addLang uc-asr de_de
```

28.8 Language Codes of the supported Voiceportalspeech Languages

Language	Country	Language Code	ISO File[1]
German	Germany	DE_DE	German
English	USA	EN_US	English

```
# sh support/installIntegratedSimplex.sh addLang
mediaserver_voiceportalspeech_languagepack EN-US

# sh support/installIntegratedSimplex.sh addLang
mediaserver_voiceportalspeech_languagepack DE-DE
```

28.9 Procedure Example for Media Server Languages

This section may be used as guideline for installing other language or application packages.

28.9.1 Adding Additional Packages/Languages

For media server announcement and treatments, refer to *OpenScape Voice Vx Administration, Administrator Documentation* (where *x* i*s the software release version*), the section titled *Media Services*.

For Integrated systems, the default installation applies only the English language for the Media Server telephone prompts. If you wish to install further languages, execute the following steps:

All commands are to be executed as user *root*.

1. Verify that the installation files (ISO files) you require for languages are provided in osc-setup with the 'list repository' (lr) command;

   Command example;

   ```
   # osc-setup lr
   ```

   ```
   Logging to: /var/log/OpenScapeUC/osc-setup-2012-04-12_10-04-
   42.log
   ```

   ```
   osc-setup version: "1.4.5-17"
   ```

   ```
   SUSE VERSION: 11 SERVICEPACK: 1
   Registered repository (url):
   1   dir:///software/tmpREPO
   Operation took:  0 seconds
   ```

2. If the installation repository does not exist proceed to step 4 on page 791.

   If the installation repository exists, use the osc-setup search (se) option to list the available packages (in this case announcements);

   ```
   osc-setup se --match-any announ
   ```

Command example:

```
# osc-setup se --match-any announ
Loading repository data...
Reading installed packages...

S | Name | Summary | Type
--+--------------+-------------------------------------------------------------------
| mediaserver_announcements_ar | Mediaserver_announcements_ar | package
| mediaserver_announcements_bg | Mediaserver_announcements_bg | package
...
i | mediaserver_announcements_en_us | Mediaserver_announcements_en_us | package
| mediaserver_announcements_en_za | Mediaserver_announcements_en_za | package
...
```

Note: An 'i' in the column S column indicates that package is already installed.

3. If the language is not listed, proceed to step 4 on page 791.

   If the required language is listed then execute the following command for installing another language;

   ```
   sh support/installIntegratedSimplex.sh addLang <component>
   <lang[,lang]>
   ```

   Change directory to the installation repository and run the command. Examples follow;

   a) Adding 1 language;

      ```
      # /etc/init.d/symphoniad stop
      # cd /software/tmpRepo
      # sh support/installIntegratedSimplex.sh addLang
      mediaserver_announcements en_za
      ```

   b) Adding multiple languages;

      ```
      # /etc/init.d/symphoniad stop
      # cd /software/tmpRepo
      # sh support/installIntegratedSimplex.sh addLang
      mediaserver_announcements en_za,de,es
      ```

   Note: This language is used for the media server announcements provided for the PBX.

   If you were able to install all language packages, then proceed with step 5 on page 791, otherwise continue with step 4 on page 791.

4. If the language is not available then the 'Repository' and required language ISO files will have to be staged for installation. See Section 5.2.10, “Providing a Setup Medium for the Applications”, on page 341 for details of this procedure.

   Attention: It is recommended the installation repository be created with the 'Base', 'Repository' and the additional language package ISOs that are required. Please include the English language package ISO in the installation repository. These files would be found in the initial build package for the current Applications version.

   Note: Providing an ISO file as repository retrospectively deletes the provision of the current repository. Install all required RPMs from the repository to be deleted before removing it.

   The language package can be installed (after establishing the repository) with the same syntax demonstrated in step 3 on page 790 of this procedure. Remember to stop the symphoniad before adding a new package.

   ```
   support/installIntegratedSimplex.sh addLang {LANGUAGE_PKG}
   ```

5. Start the Applications server;

   Command example:

   `# /etc/init.d/symphoniad start`

   The file osgi.log can be monitored for error messages while symphoniad starts (or restarts). After executing a 'symphoniad start' or 'symphoniad restart' command there is a period of time in which the applications services are set into operation. As user *root* the applications services startup can be monitored by the following command:

   For integrated applications servers;
   tailf /log/osgi.log

   For External (offboard) applications servers;
   tailf /var/siemens/common/log/osgi.log

   Monitor the file osgi.log for the services startup sequence. When the osgi.log file reports "* Start processing all bundles done.* " the system is ready. The startup sequence should not have been interrupted by error messages. The file osgi.err (located in the same path as the osgi.log file) should be empty also.

   Press **'ctrl+c'** to exit the tail function.

   Questions should be addressed to your next level of support.

6. If the update process is complete, the system should be cleaned of ISOs and repositories. Proceed to Section 28.10, “Cleaning up after the Installation”, on page 792.

Note: If you do not wish to remove the repository structure at this time you may follow these links to your respective procedure/section;

- Step 30 on page 36 of Table 1, “OpenScape Voice Installation Checklist”.
- Section 5.2.3.4, “Adding Additional Packages/Languages”, on page 307
- Step 16 on page 482 of Table 20 “Simplex Upgrade”.
- Step 16 of Table 23 "Simplex to Simplex Migration".

28.10 Cleaning up after the Installation

If the installation process is complete the system should be cleaned of ISOs and repositories.

1. Unmount all isos and clean internal linked repo (**This does not remove repositories from repolist!**). This command cannot be used with other commands.

   # osc-setup cr --clean

2. De-register the temporary repository from the list of registered repositories. The osc-setup lr (list repository) command will present a list of repositories.

   Note: The repository can be either the repository URI or its index (starting from 1) as reported by the list repositories command (**osc-setup lr**). If the repository is not defined the first repository from list will be removed.

   # osc-setup rr dir:///software/tmpREPO

3. De-register any ISO repository from the list of registered repositories.

   Note: A repository can be removed with the URI or Alias. All of the examples used the Alias OSC.

   Command example(s) with Alias;

   # zypper rr OSC

   Command example with URI;

   # zypper rr iso:///?iso=/software/oscISOs/OpenScapeUcSuiteApps-Repository-V7R1.0.0-060000.iso

4. Clean all local caches created with zypper.

   Command example;

   # zypper clean

5. List the zypper repositories to ensure the 'OSC' repository does not exist.

   # zypper lr

6. Remove data from the /software/tmpREPO path;

   Command example;

   # rm -rf /software/tmpREPO

7. Remove data from the /software/oscISOs/ path;

   Command example;

   # rm -rf /software/oscISOs/

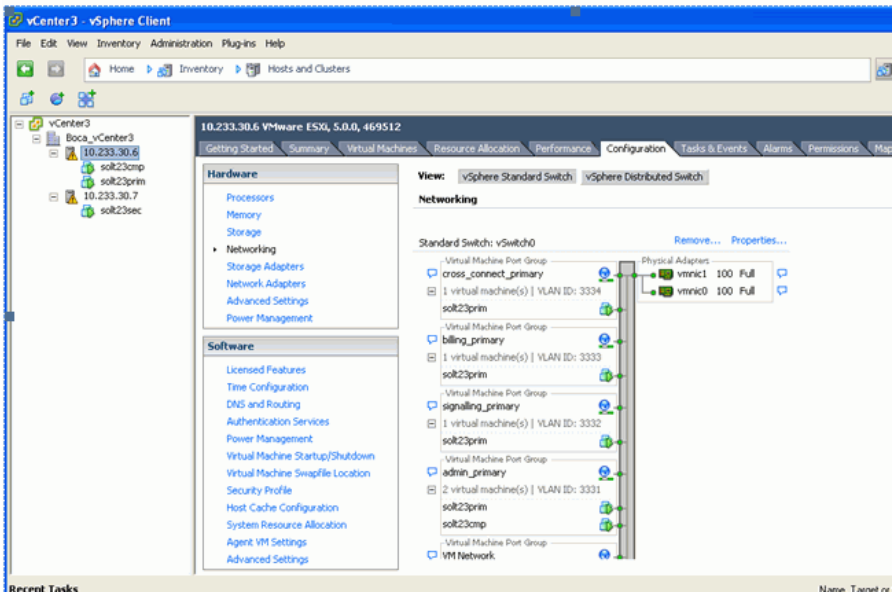
Follow these links back to your procedure;

- If you arrived here from the “OpenScape Voice Installation Checklist”, return to step 30 on page 36 of Table 1.
- If you arrived here from Section 5.2.3.4, “Adding Additional Packages/Languages”, return to Section 5.2.3.4, “Adding Additional Packages/Languages”, on page 307.
- If you arrived here from the “Simplex Upgrade”, return to step 16 on page 482 of Table 20.
- If you arrived here from the "Section 9.1, “Migration Scenarios”", return to step 16 of Table 23.

29 Guidelines for Configuring NIC Teaming on the VM Host

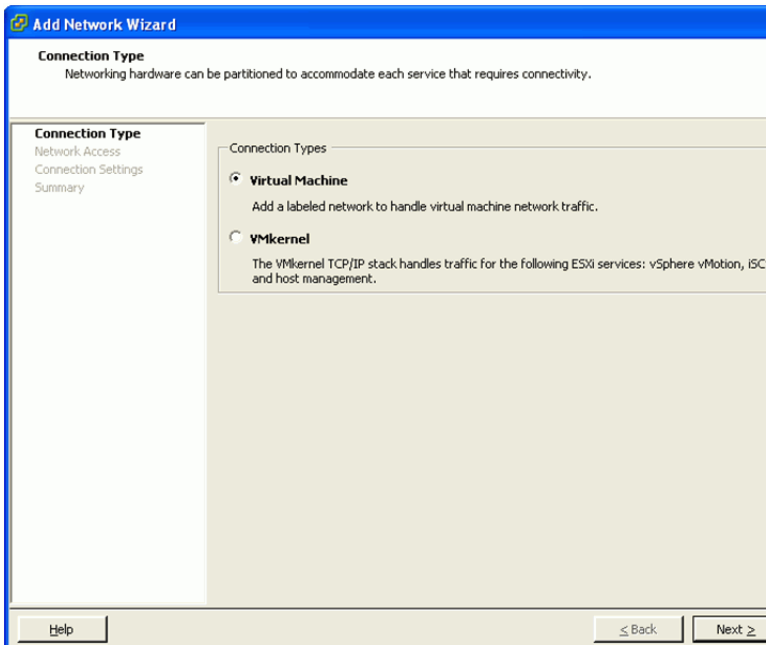
Setting Up Traffic over Single NIC Team

1. Select the ESXi host machine.

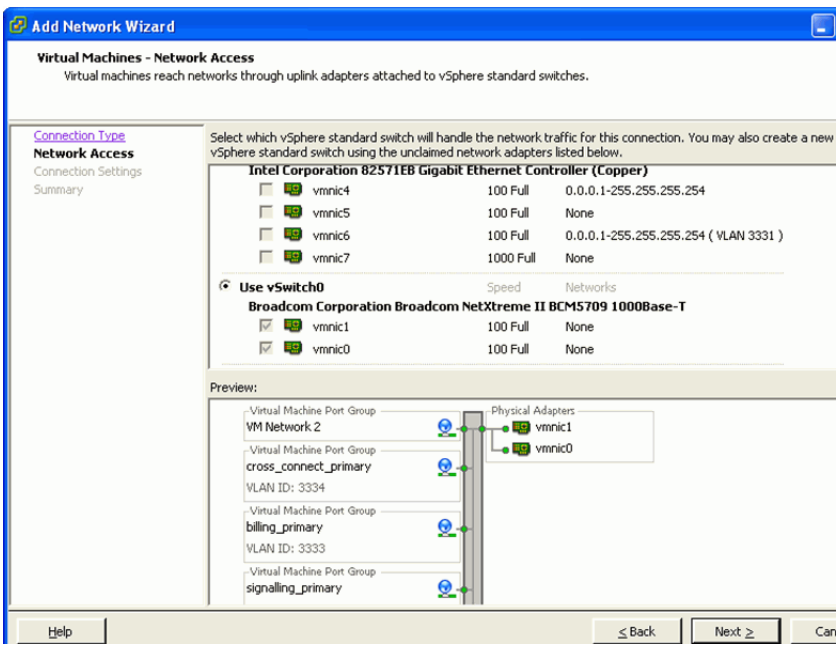


2. Select Configuration Tab.
3. Select Add Networking under the Hardware pane (top left).
4. Select Add Networking (top right).

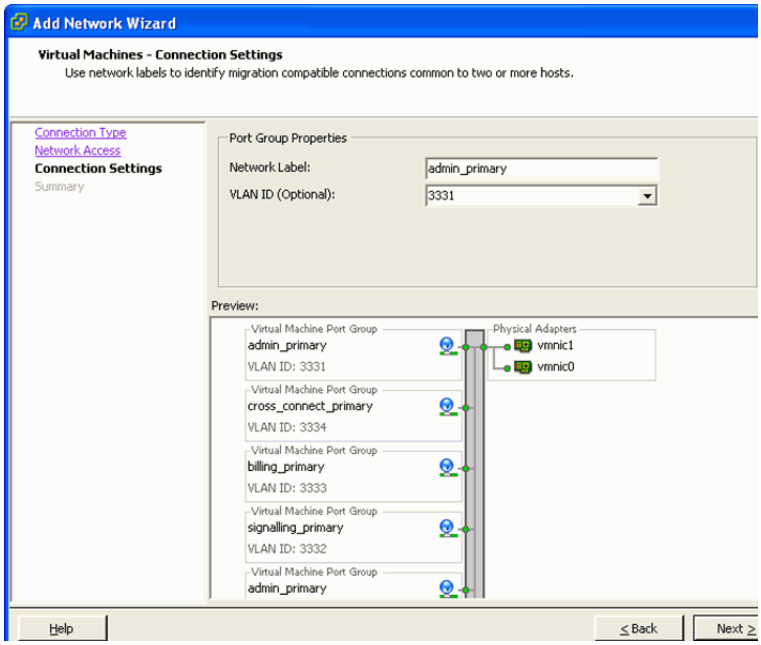
a) Select Virtual machine



b) Select the network adapter to handle the specific traffic (e.g. vmnic0. vmnic1).

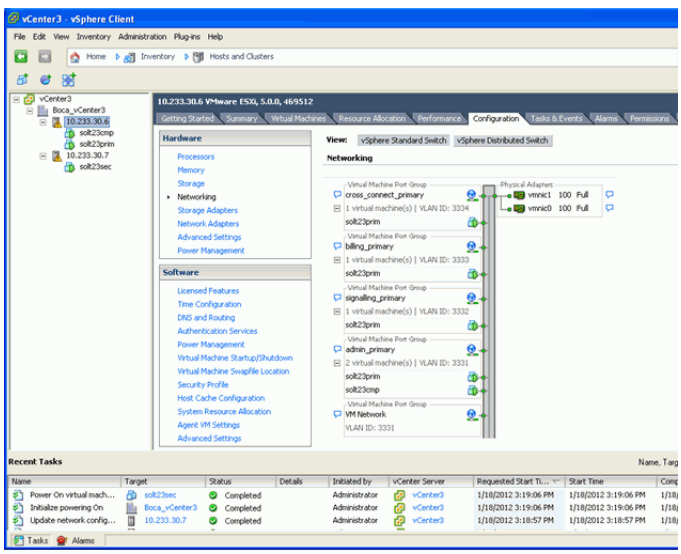


c) Specify the network label and optional vlan id (2-4094).

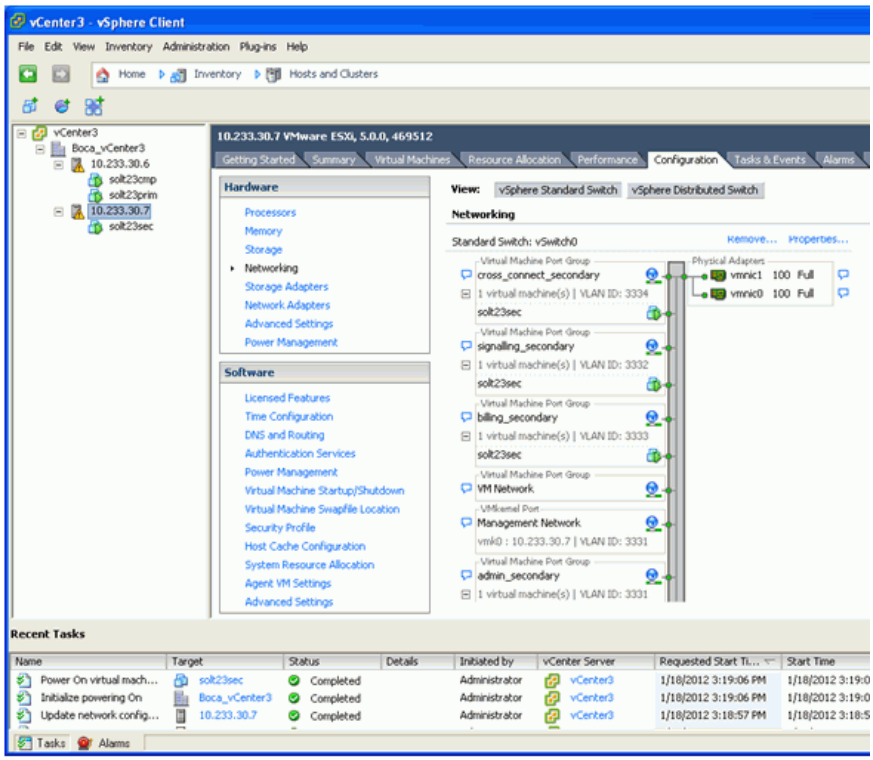


d) Click Finish

e) Repeat these steps for the signaling_primary, billing_primary and cross_connect_primary networks choosing the same vmnics but different VLAN ids:

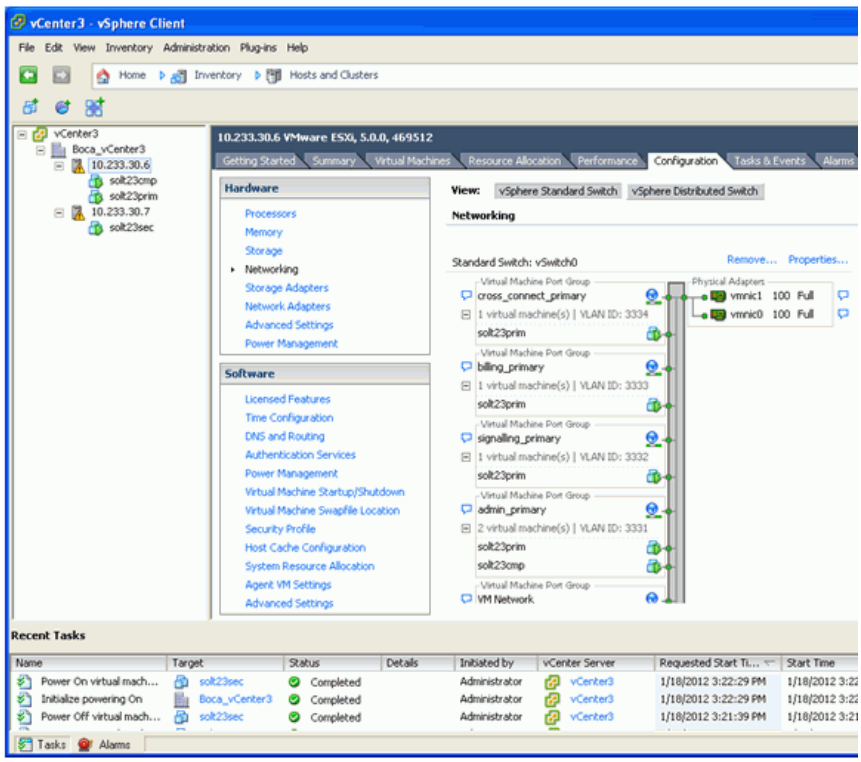


f) Repeat the same steps for the secondary node (duplex system).

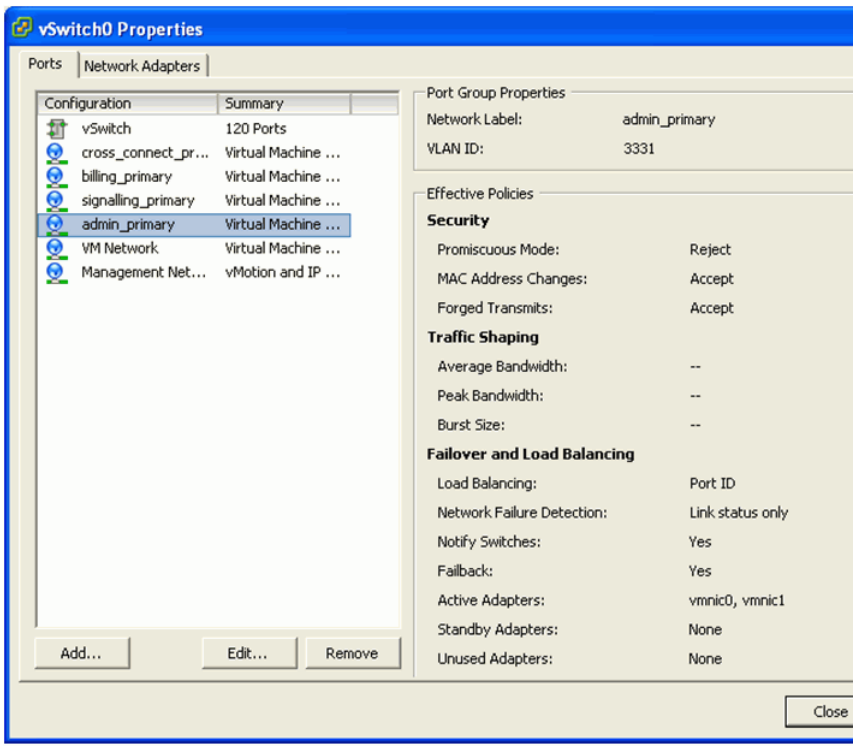


Configuring the NIC Team:

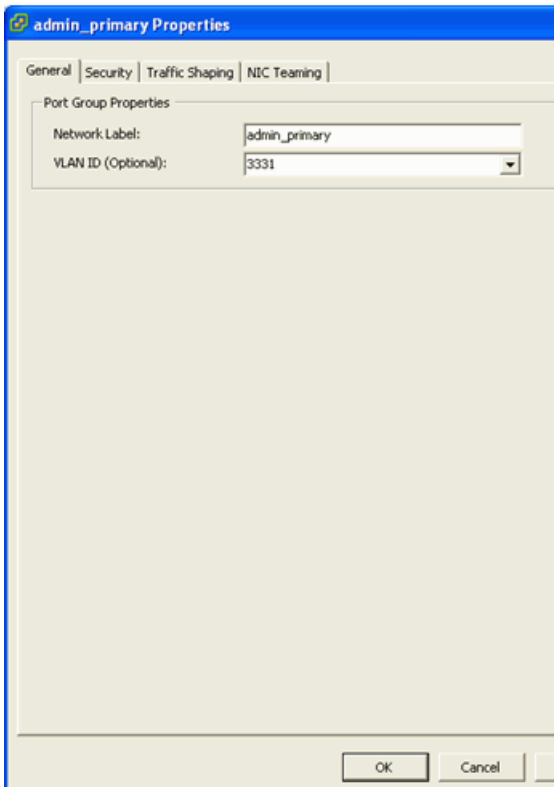
1. Select Configuration Tab.
2. Select Add Networking under the Hardware pane (top left).



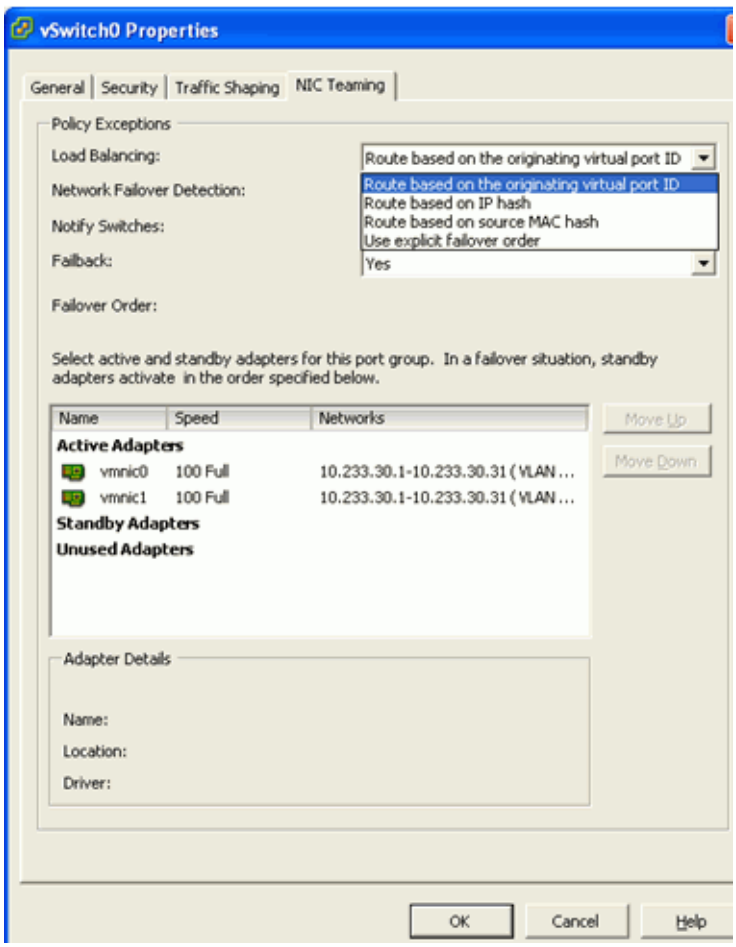
3. Select the properties link next to the virtual switch on which the port group is located.

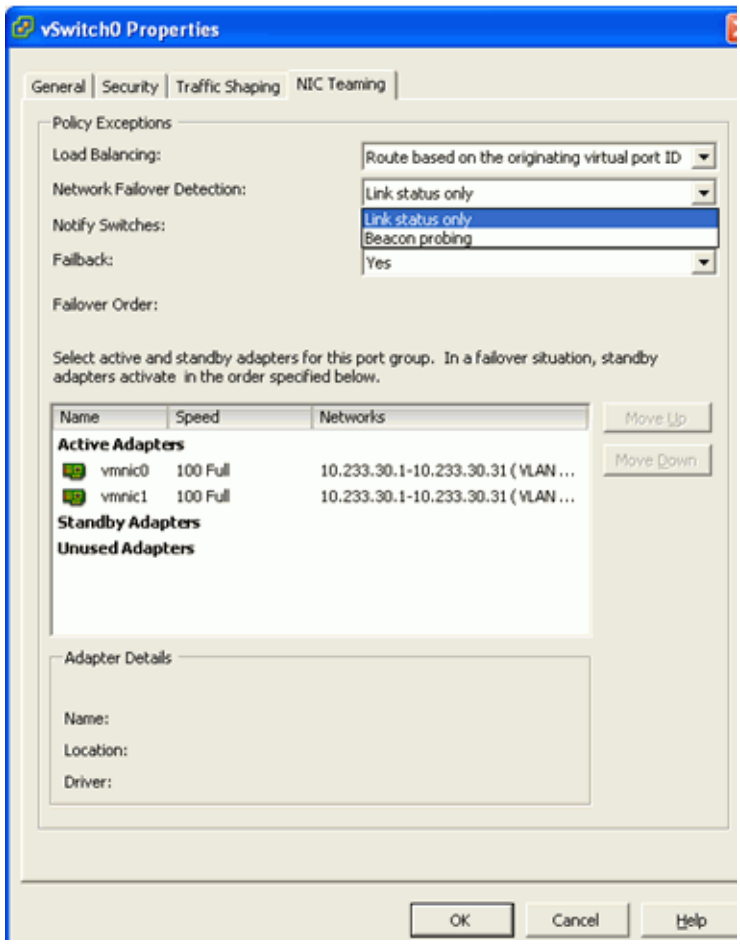


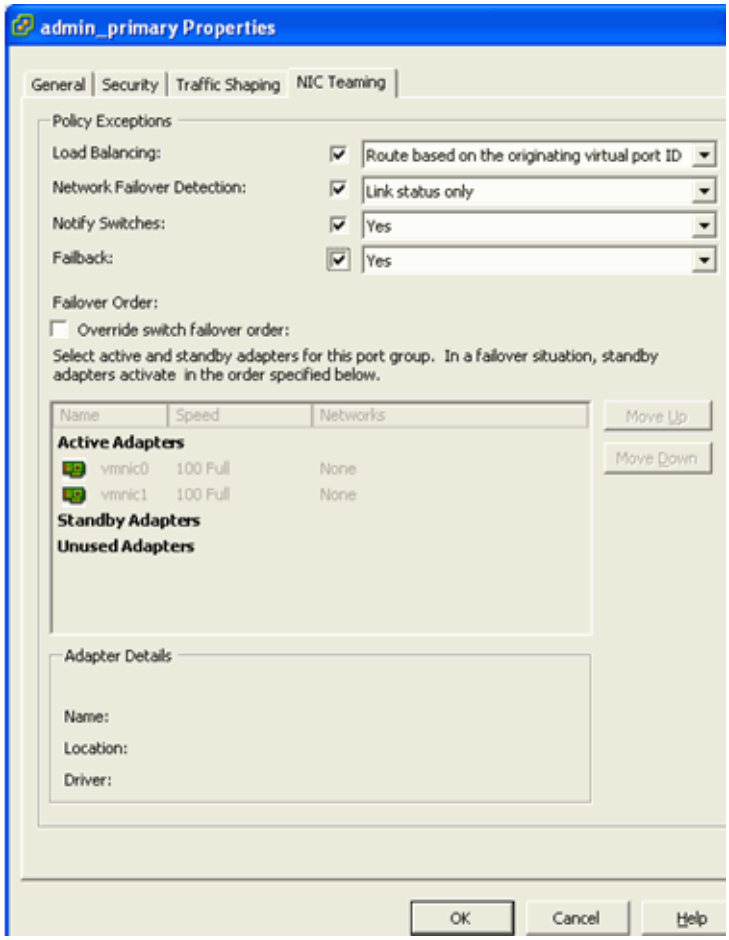
4. In the Port group properties window, select the NIC teaming tab.

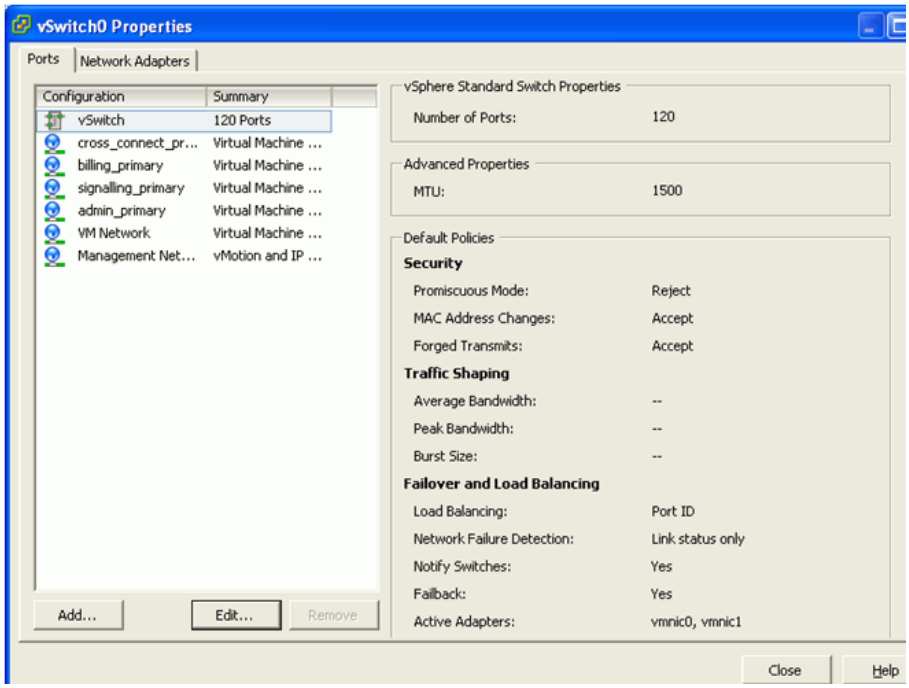


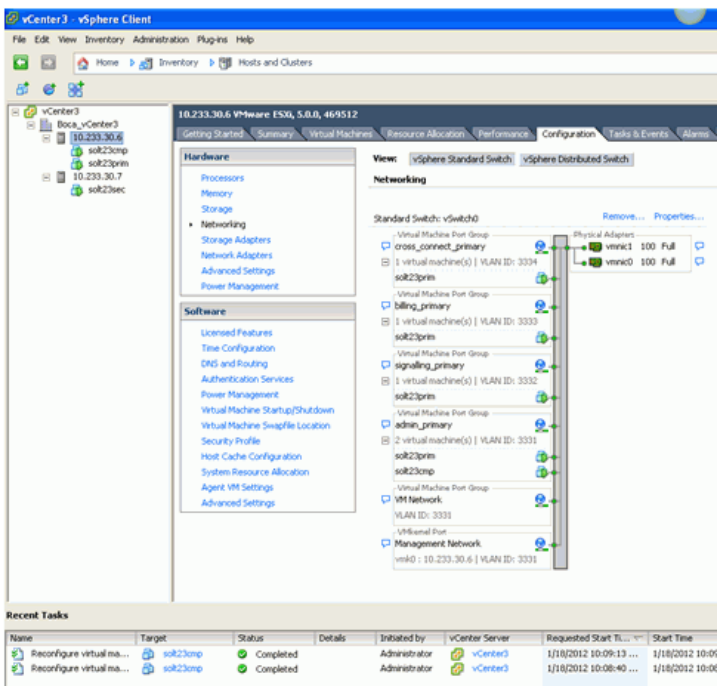
5. Keep the default values for:
   - Load Balancing = Route based on the originating virtual port id
   - Network Failover Detection = Link Status Only
   - Notify Switched = Yes
   - Fallback = Yes




vSwitch0 Properties
General
Security
Traffic Shaping
NIC Teaming
Policy Exceptions
Load Balancing:
Route based on the originating virtual port ID
Network Failover Detection:
Link status only
Notify Switches:
Link status only
Beacon probing
Failback:
Yes
Failover Order:
Select active and standby adapters for this port group. In a failover situation, standby adapters activate in the order specified below.
Name
Speed
Networks
Move Up
Move Down
Active Adapters
vmnic0
100 Full
10.233.30.1-10.233.30.31 (VLAN ...
vmnic1
100 Full
10.233.30.1-10.233.30.31 (VLAN ...
Standby Adapters
Unused Adapters
Adapter Details
Name:
Location:
Driver:
OK
Cancel
Help


admin_primary Properties
General
Security
Traffic Shaping
NIC Teaming
Policy Exceptions
Load Balancing:
Route based on the originating virtual port ID
Network Failover Detection:
Link status only
Notify Switches:
Yes
Failback:
Yes
Failover Order:
Override switch failover order:
Select active and standby adapters for this port group. In a failover situation, standby adapters activate in the order specified below.
Name
Speed
Networks
Move Up
Move Down
Active Adapters
vmnic0
100 Full
None
vmnic1
100 Full
None
Standby Adapters
Unused Adapters
Adapter Details
Name:
Location:
Driver:
OK
Cancel
Help


vSwitch0 Properties
Ports
Network Adapters
Configuration
Summary
vSwitch
120 Ports
cross_connect_pr...
Virtual Machine ...
billing_primary
Virtual Machine ...
signalling_primary
Virtual Machine ...
admin_primary
Virtual Machine ...
VM Network
Virtual Machine ...
Management Net...
vMotion and IP ...
Add...
Edit...
Remove
vSphere Standard Switch Properties
Number of Ports: 120
Advanced Properties
MTU: 1500
Default Policies
Security
Promiscuous Mode: Reject
MAC Address Changes: Accept
Forged Transmits: Accept
Traffic Shaping
Average Bandwidth: --
Peak Bandwidth: --
Burst Size: --
Failover and Load Balancing
Load Balancing: Port ID
Network Failure Detection: Link status only
Notify Switches: Yes
Failback: Yes
Active Adapters: vmnic0, vmnic1
Close
Help


vCenter3 - vSphere Client
Recent Tasks

30 Solution Upgrades

30.1 Solution Overview

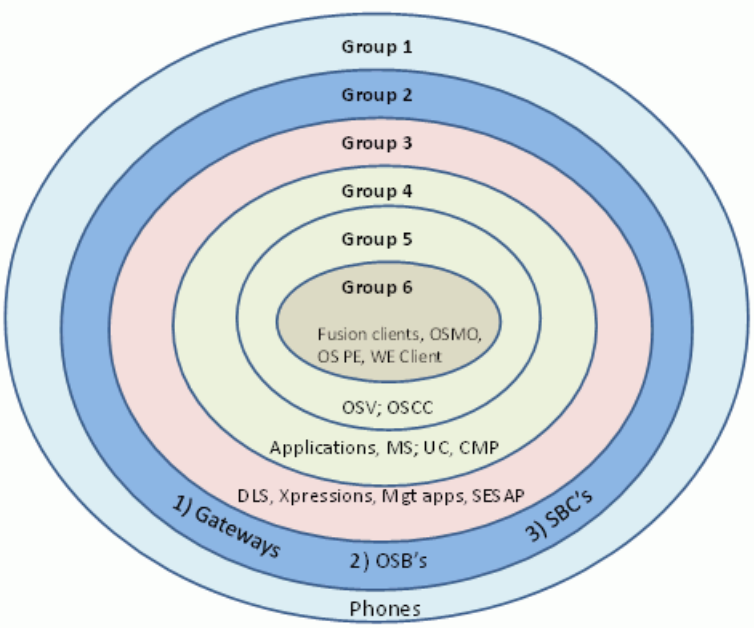
Mitel has defined a standard set of OpenScape products and configurations called the “OpenScape Standard Solution”.

All Mitel products have a Technical Upgrade Concept and an Upgrade Plan. However, when the products are part of a solution, these products use shared interfaces and the upgrades of these products are not independent from each other. The Solution Upgrades Appendix describes how the Upgrade Procedure is to be executed for all components of the Enterprise solution.

There is no longer a strict upgrade sequence of single products required as we support backwards compatibility. However, it is **strongly recommended** to upgrade all solution components to the software versions tested and released with OpenScape V11.

By employing this process, a customer will be able to use the new V11 features without restrictions and ensure the best possible quality of the OpenScape Voice solution due to the highest degree of test coverage.

The solution upgrade sequence will be in accordance to the "edge inwards" upgrade methodology. Solution components are divided into three categories - core products, extended products, and interop products. The upgrade procedure must include all extended and core products, as well as selected interop products.



30.1.1 Upgrade Paths

Note: The OpenScape Voice upgrade concept includes the Applications servers associated with the Voice server(s).

The upgrade of all solution components has to be done according to the documentation provided by the respective products.

This document only contains the upgrade procedures for the following solution elements:

- Multiple Communications Server Admin applications server deployment
- Media Server Standalone applications server deployment
- OpenScape Voice server

During the course of the OpenScape Voice server upgrade, the OpenScape Voice Installation and Upgrades document will direct users to the appropriate documentation for the upgrade of Applications servers. The specific Applications server upgrade will be described in one of the two following documents:

- In this OpenScape Voice Vx Service Manual, Installation and Upgrades (where *x* is the software release version)

- In the OpenScape UC Application Vx Installation and Upgrade, Installation Guide (where *x* is the software release version)

For all other products, please refer to that product's manuals and release notes.

The supported upgrade paths are:

- Upgrade from OpenScape Voice V9/V10 to OpenScape Voice V11

30.1.1.1 Upgrades Addressed in OpenScape Voice Service Manual, Installation and Upgrades

The *OpenScape Voice Service Manual, Installation and Upgrades, Installation Guide* contains the upgrade procedures for the following OpenScape Voice Applications server deployment scenarios;

- Integrated Simplex
- Standard Duplex
- Multiple Communications Server Admin applications server deployment
- Media Server Standalone applications server deployment

Note: The Integrated Simplex Applications upgrade takes place as part of the OpenScape Voice Image installation (unless indicated otherwise by the Release Notes or the OpenScape Voice Installation and Upgrades procedure).

30.1.1.2 Upgrades Addressed in OpenScape UC Application Installation and Upgrade, Installation Guide

The *OpenScape UC Application Installation and Upgrade, Installation Guide* describes the upgrade procedures for the following OpenScape Applications server deployment scenarios;

- UC Small deployment
- UC Large deployment
- UC Very Large deployment

30.1.2 General Sequence of the Solution Upgrade

The general sequence of the Solution Upgrade is:

1. Upgrade all components to the latest released version for the corresponding source release (as outlined in the compatibility matrix of the appropriate OpenScape release note). This step is **mandatory** to ensure a smooth upgrade.
2. Upgrade all components which require a new software version to work with OpenScape Voice V11. (These procedures will include the Openscape Applications server upgrades).
3. Upgrade the V9/V10 OpenScape Voice server to V11.

Note: New OpenScape Voice V11 features may not be supported if the source release solution components are not upgraded as required by the Compatibility Matrix.

30.2 Upgrade Sequence for Solution Upgrades

Prior to the Solution upgrade to V11, it is necessary to gather the software versions of the existing customer's solution in order to determine compatibility with OpenScape UC Suite V10 and plan the upgrade. Preparation may include obtaining license files for the target release, confirm the Survival Authority is configured, test IMM, backup Application Response files, backup OSV SNMP files, obtain Screen Shot of Trace Manager Control Config, and update the NOC MIBs. During the upgrade, components are backed up prior to being upgraded.

1. Upgrade phones.

   Note: The existing interface between DLS and phones provides that both the DLS and the phones ignore (read/write) items not understood by DLS or the phones. This provides that a new version of phone software can be managed by an older version of DLS (and vice versa). The phone's menu/web based management is also available for managing the phones individually.

2. Upgrade Gateways, OSBs, SBCs, HP3&4K: These elements are managed with local management tools.
3. Upgrade Management applications, DLS, Xpressions, SESAP.
4. Upgrade Applications, MS, UC, CMP.
5. Upgrade OSV, OSCC.
6. Customer Driven Upgrades: Products in this group are typically rolled out by the customer's IT department or updated by the end user from an Application Store.

Note: Solution upgrade times are very dependent on the complexity of the solution and the expertise of the person performing the upgrade. The following table defines the Solution Upgrade Sequence to be followed for OpenScape UC Suite V10.

Sequence	OpenScape Solution Set Element
Upgrade Group 1 – Phones **Note:** The existing interface between DLS and phones provides that both DLS and the phones ignore (read/write) items not understood by DLS or the phones. This provides that a new version of phone sw can be managed by an older version of DLS (and visa versa). The phone's menu/web based management is also available for managing the phones individually.	
1.	Devices: OpenStage 5, 15, 15 G, 20E, 20, 40, 60, 80, WL3S Desk Phone IP 35G, 55G
2.	OpenScape Cordless IP w/ OpenStage SL4 Professional
Upgrade Group 2 – Gateways, OSBs, SBCs, HP3000 and 4000 **Note:** Elements are managed with local management tools.	
3.	3rd party ATAs and Gateways: Mediatrix AP 1104, AP 1120 SIP, AP 1124, 3631, 3632 (T1 and E1), 4402, 4404 (S0), 1204 (Analog trunk gw), 4102, 4104, 4108, 4116, 4124 (Analog gw/adapter), LP24 (long loop analog adapter)
4.	RG8702, 8708, 8716
5.	OpenScape 4000/RG8350a
6.	OpenScape Branch (50/250, 1000, 6000, 50i, 500i)
7.	OpenScape Business (new name for OS Smart Office) – new in V8 – no upgrade
8.	OpenScape SBC (when used to support a SIP Trunking interface to a carrier SIP service provider) and (when interfacing SIP devices (e.g. Remote OpenStage Phones) and/or OpenScape Branch)
9.	Acme Packet Net-Net 38xx and Net-Net 4500 (SIP trunking only)
10.	Acme Packet Net-Net 4250 (SIP trunking only)
Upgrade Group 3 – Management Apps, DLS, Xpressions, SESAP	
11.	DLS (Windows)
12.	Xpressions (Xpressions V7R1 is used with OS UC Suite V10)
13.	SESAP/Trace Manager

Table 36 Solution Set Component Upgrade Sequence

Sequence	OpenScape Solution Set Element
14.	OpenScape User Management
15.	OpenScape User Management
16.	OpenScape Quality of Service Management
17.	OpenScape Accounting
18.	OpenScape Fault Management/OpenScape Quality of Service Management
Upgrade Group 4 – Applications, MS, UC, CMP	
19.	OpenScape UC Application Enterprise Edition - UC Backend/CMP
20.	OpenScape UC Application Enterprise Edition - Standalone MS
21.	OpenScape UC Application Enterprise Edition - UC FE
22.	OpenScape UC Application Enterprise Edition - Façade Server
23.	OpenScape UC Application Enterprise Edition - Openfire Server for Instant Messaging
24.	OS Fusion for Google
25.	E/A Cockpit
26.	OpenScape Web Collaboration Instant Meeting Pro
Group 5 – OSV, OSCC	
27.	Concierge
28.	OpenScape Contact Center Enterprise
29.	OpenScape Contact Center Campaign Director
30.	OpenScape Contact Center Extensions – Concierge (Integrated with OSCC – can be upgraded independently of OSCC because i/f is stable and is already covered by product testing. If OSCC is upgraded then Integrated Concierge must be upgraded the same time as OSCC)
31.	CSTA Applications
32.	Voice Recording (ASC EVOip, ASC RIA for OpenScape Voice, Verint)
33.	OpenScape Contact Center Voice Portal
34.	OS CC Attendant Console
35.	OSV using outage free toolkit
36.	Genesys
37.	OpenScape Alarm Response Professional + OpenScape Alarm Response Economy (OScAR)
Upgrade Group 6 – Customer Driven Upgrades **Note:** Products in this group are typically rolled out by the customer's IT department.	

Table 36 Solution Set Component Upgrade Sequence

Sequence	OpenScape Solution Set Element
38.	OSMO client (Mobile clients connected to OSV)
39.	OpenScape Personal Edition
40.	ODE WE Client
41.	OS Fusion (Outlook, Lync, Notes)
42.	VMware (to ESXi 5.5)

Table 36 Solution Set Component Upgrade Sequence

Click this link to return to Section 7.2, “Solution Upgrade Considerations”, on page 422.

31 Change E1000 to VMXNET3 network adapters

This procedure only applies to Virtual OSV Deployments.

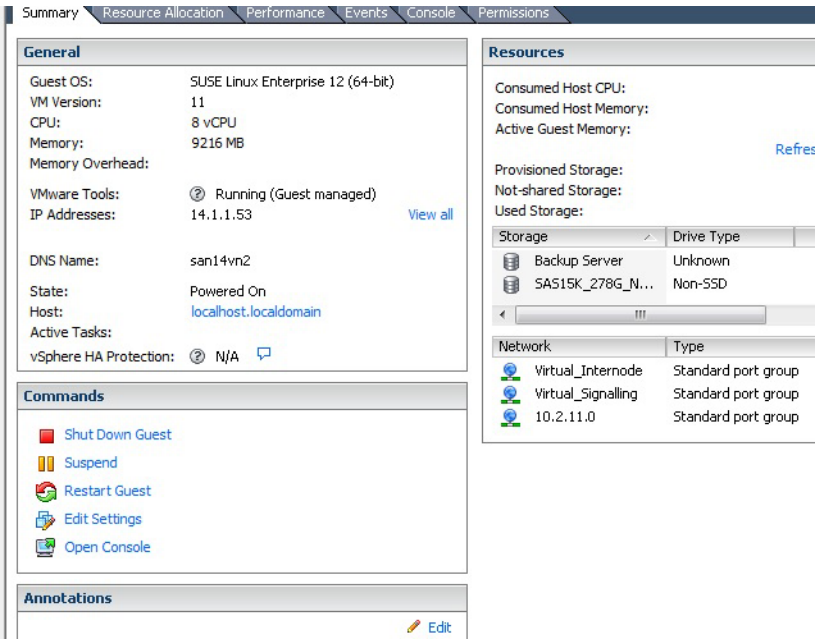
Changing the vNIC type needs to be performed during a maintenance window where no or limited traffic is expected.

Outage needs to be considered on Integrated Simplex deployments. The outage time includes the VM shutdown time, changing VM settings and VM startup time. On the Standard Duplex deployments there is no outage, as the shutdown is done sequentially on each node

Follow the steps below to change from E1000 to VMXNET3 network adapters

1. Check for VMware tools

Login to the Vsphere Client or Vsphere Web Client and verify that VMware tools are installed and running:



2. Verify that the system is running

Login via console or remote shell on the first node and run as root or srx user:

```
# srxqry


Verify the following lines are included in the output

Node name              DB State          Op Mode       Status

---------              --------          -------       ------
```

```
Local Node: <node1_name> Secondary active Normal Online at
state 4

Remote Node: <node2_name> Primary active Normal Online at
state 4

-- UCE and all signaling managers are up and running on
<node1_name>

-- UCE and all signaling managers are up and running on
<node2_name>
```

Run as root:

```
# ~srx/bin/RapidStat -b
```

Only proceed if RapidStat does not report any major error condition.

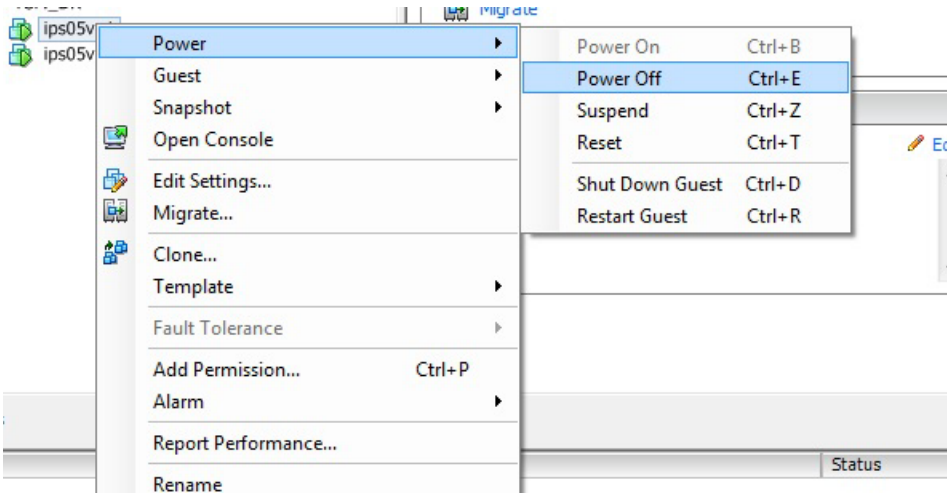
The report summary of this tool will be shown in the screen as well as saved under /log/RapidStat.log.

3. Stop node1

Run as root or srx user

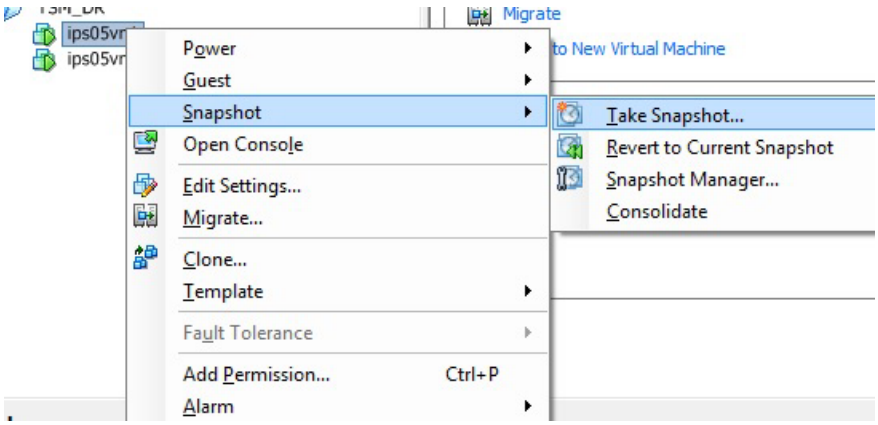
```
# srxctrl 2 0
```

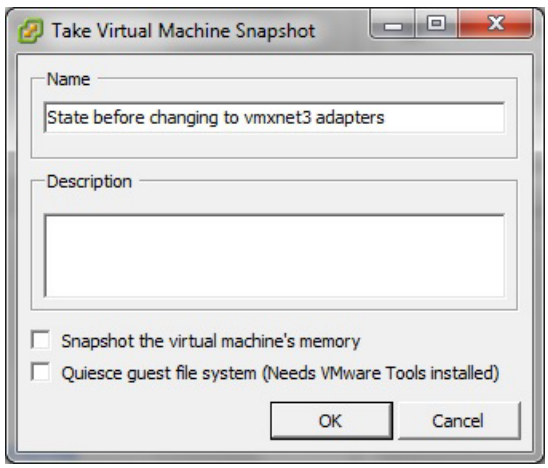
Type "y" to the prompt. When the command returns, login to VSphere Client or VSphere Web Client. The figures below are taken from the VSphere client. Stop the virtual machine; right-click and select Power-> Power Off:



4. Take a VM Snapshot

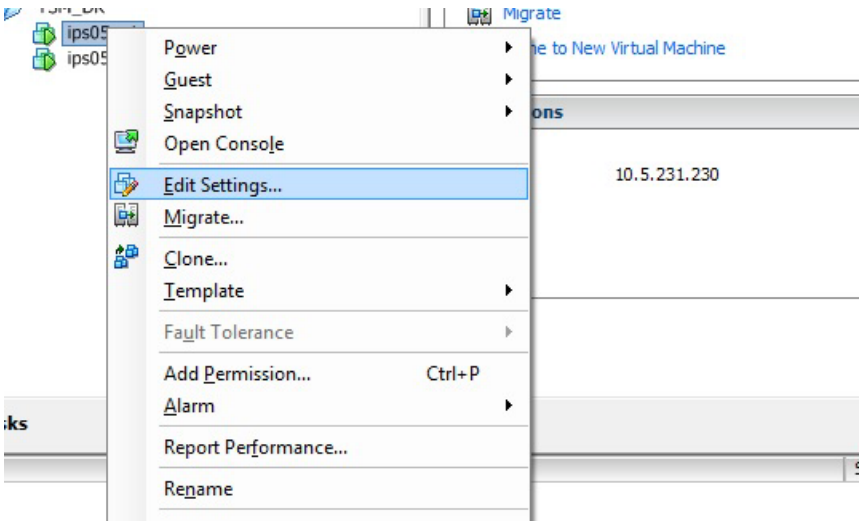
Save a snapshot to roll back to if necessary:



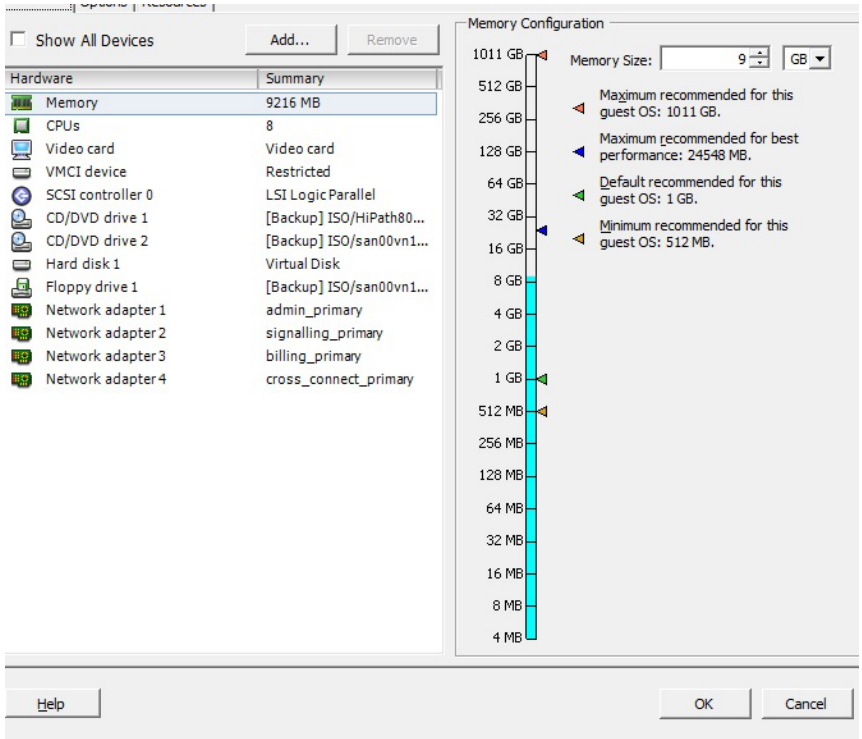


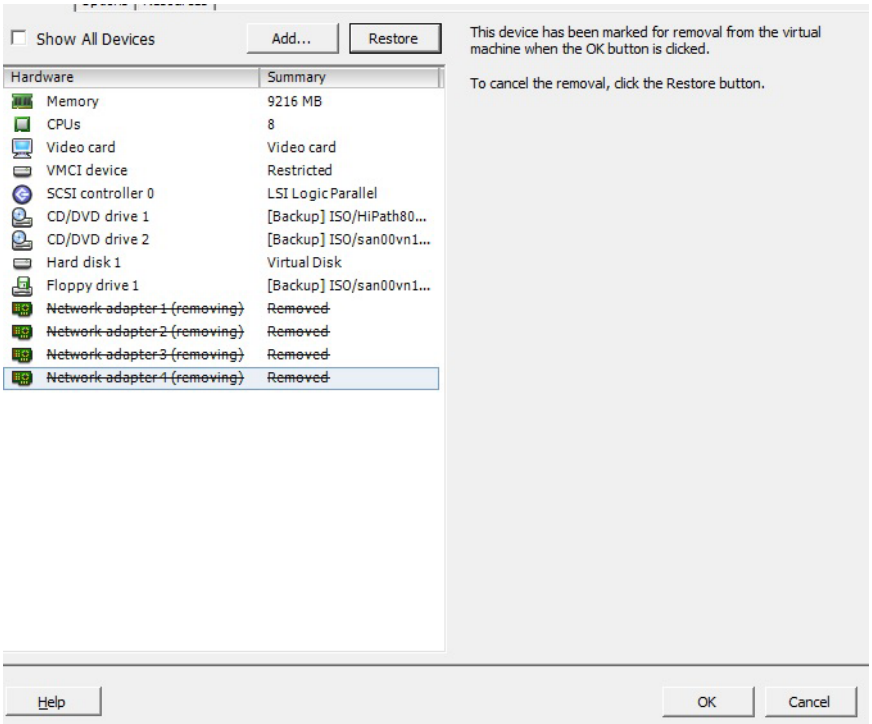
5. Edit the VM Settings

Right click on the VM and select **Edit Settings**:

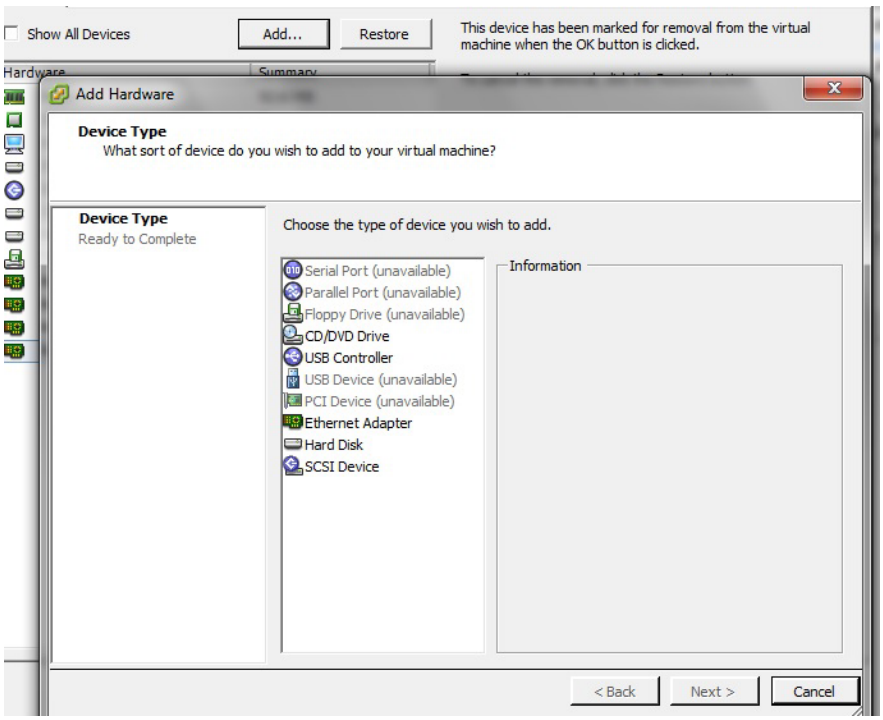


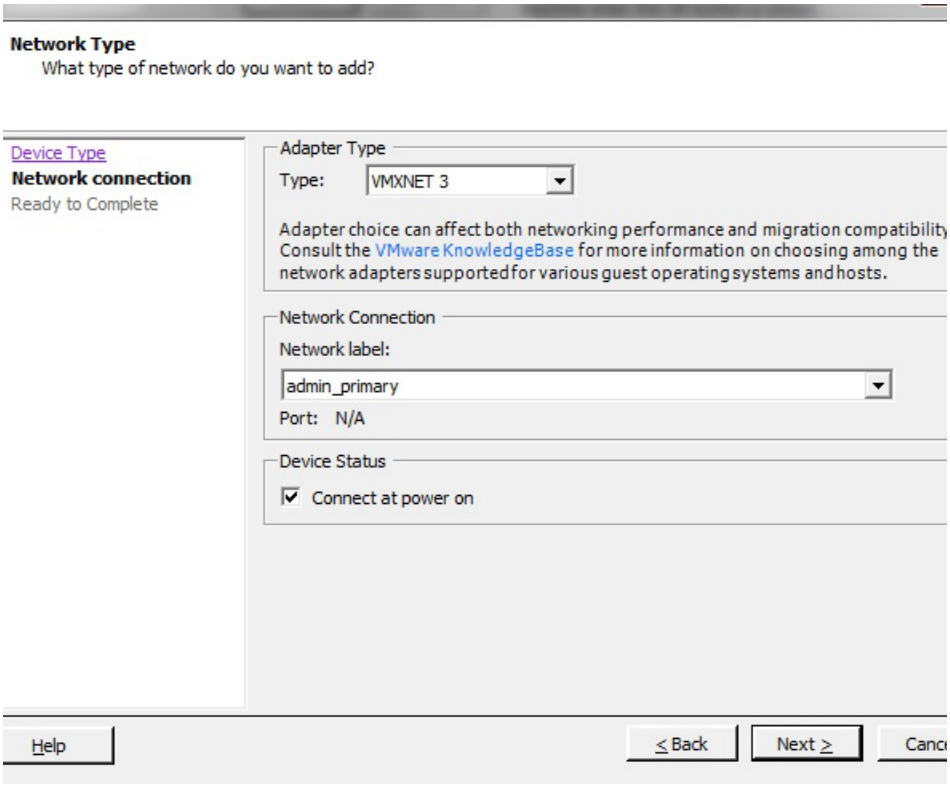
Select all existing **E1000** network adapters and **Remove** one by one. Optionally, note down the MAC address of the old adapters in case you need to use the same on the new adapters.

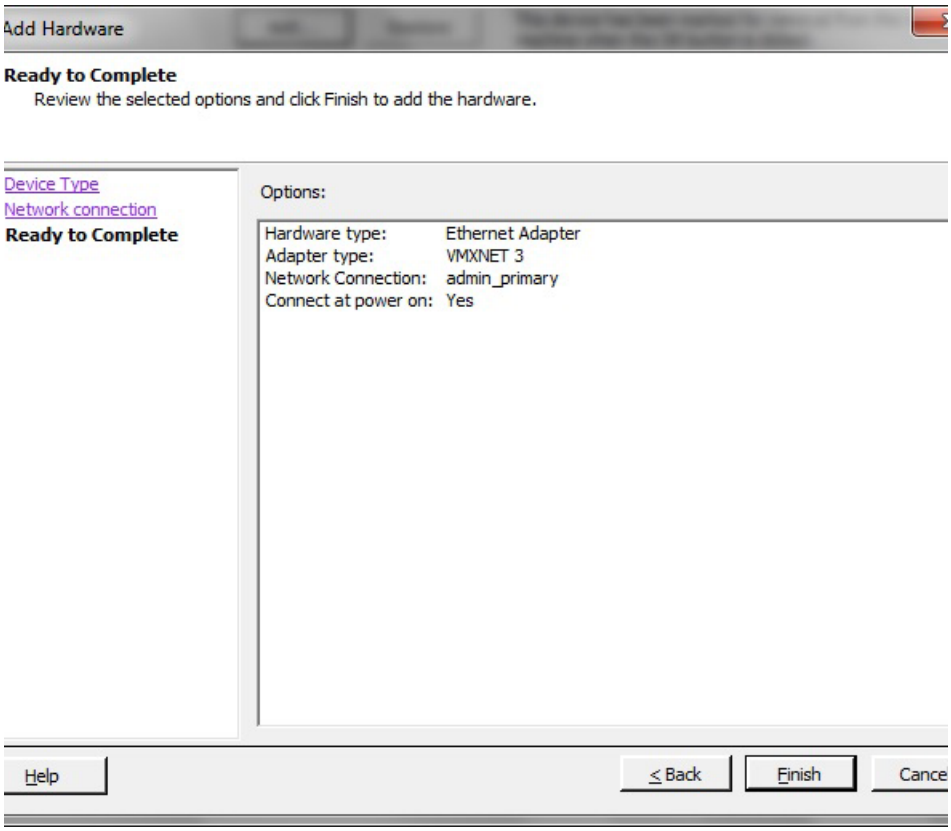




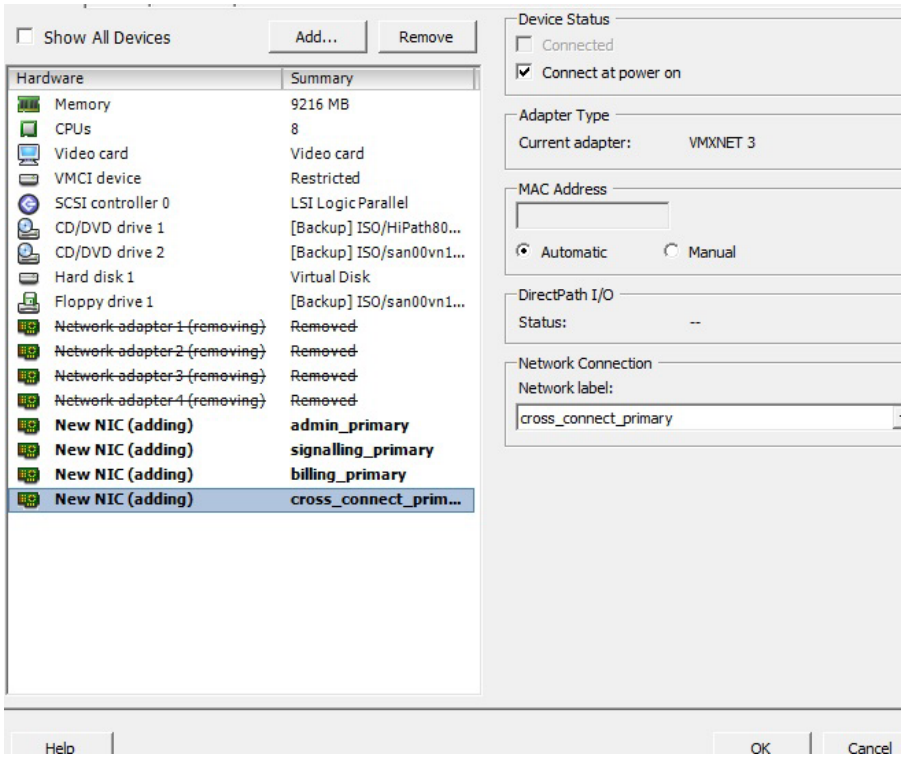
Now add all the necessary network adapters again, this time selecting **VMXNET3** type. Use the same order as the old adapters:




Network Type
What type of network do you want to add?
Device Type
Network connection
Ready to Complete
Adapter Type
Type:
VMXNET 3
Adapter choice can affect both networking performance and migration compatibility
Consult the VMware KnowledgeBase for more information on choosing among the
network adapters supported for various guest operating systems and hosts.
Network Connection
Network label:
admin_primary
Port: N/A
Device Status
Connect at power on
Help
< Back
Next >
Canc

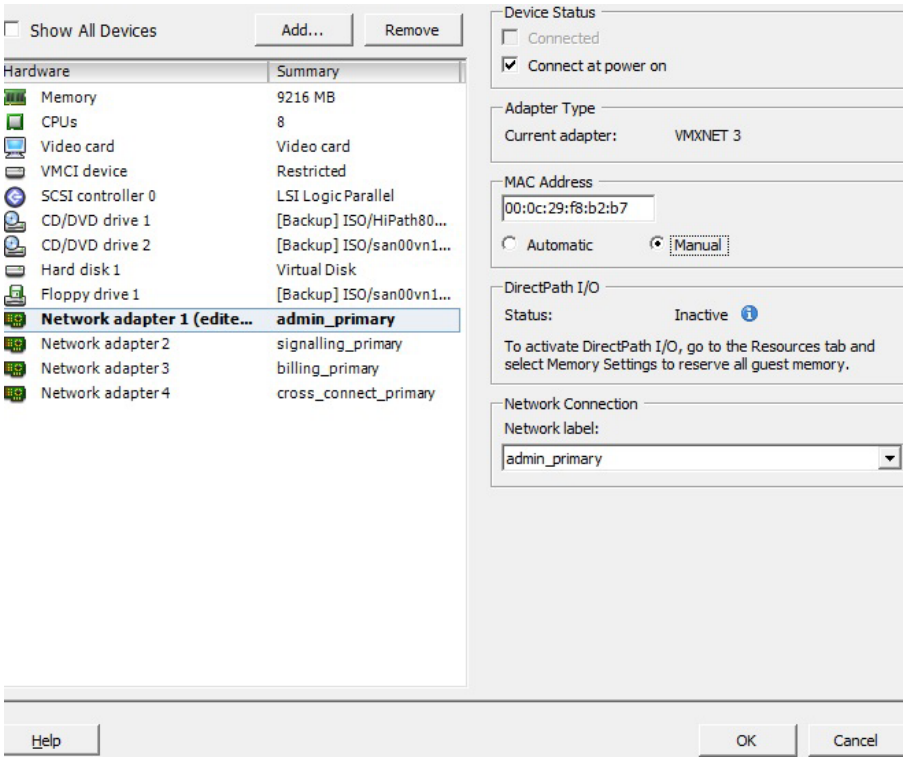


When all network devices have been added, save settings by clicking **OK**:



6. (Optional) Re-use old MAC addresses

If you are going to reuse the old MAC addresses, open the VM Settings again before powering the VM on. Select each one of the new network adapters. From the MAC Address section on the right, select **Manual**. Put the old MAC addresses in the correct order.



7. Start node1

Power on node1. Use the `srxqry` command described above to verify that both nodes are operational again.

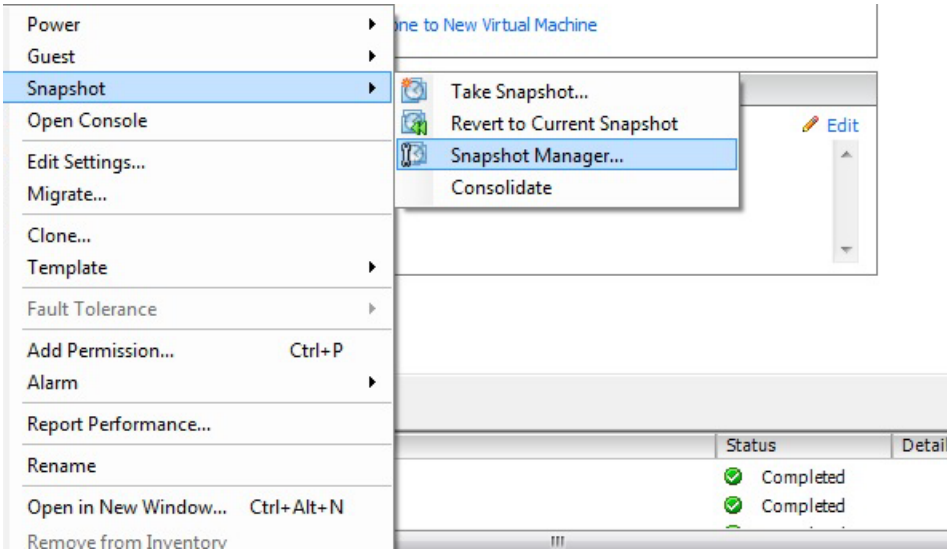
If this is a duplex system repeat the steps above on the second node. If this is a simplex, proceed to the Verification steps and Cleanup.

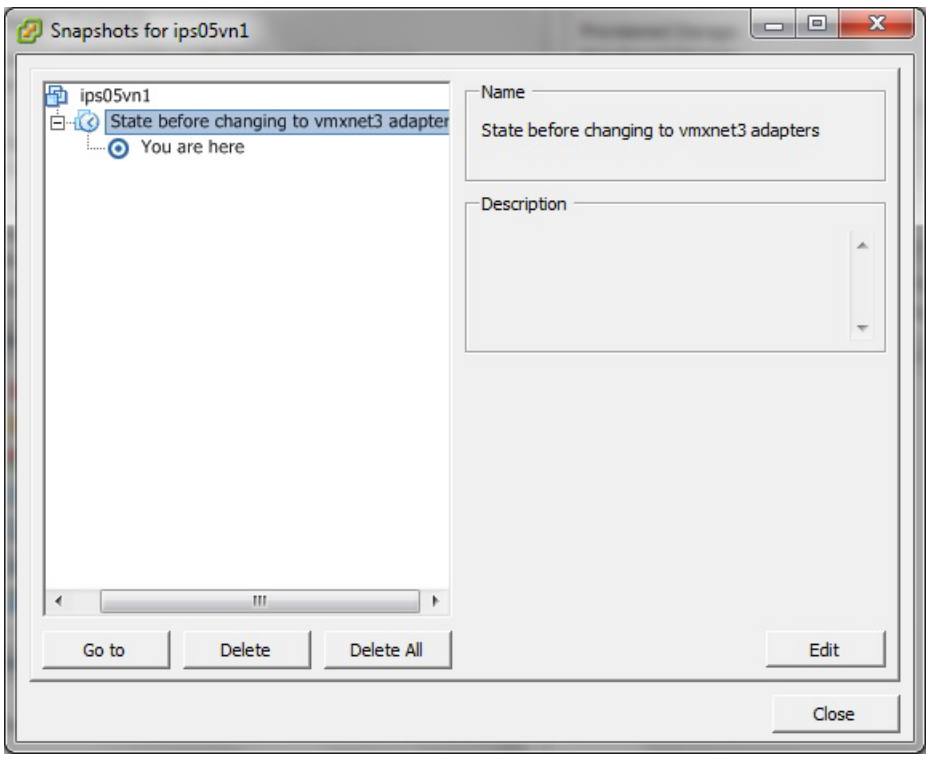
8. Verification steps

When finished, repeat the "Verify system is running" steps above. Verify that no new errors or warnings are shown in the RapidStat summary.

9. Cleanup

After finishing, remove the snapshot you got before:


Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Clone...
Template
Fault Tolerance
Add Permission... Ctrl+P
Alarm
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Take Snapshot...
Revert to Current Snapshot
Snapshot Manager...
Consolidate
Edit
Status
Completed
Completed


Snapshots for ips05vn1
ips05vn1
State before changing to vmxnet3 adapter
You are here
Name
State before changing to vmxnet3 adapters
Description
Go to
Delete
Delete All
Edit
Close

Index

A
accidents, reporting 23
Adobe Reader 20
Applications 295
Applications Servers 299

B
Backups 439
BasicTraffic Tool (BTT) 387, 573
Boot-Up speed 229

C
checking
  port assignments 290
Checklist 172
CLI Users 437
configuring Ethernet NICs 288

D
Datastore 189
disabling auto-negotiation 288

E
editing
  the node.cfg file 50
electrical safety information 21
emergency information 23
emergency safety 23
equipment room safety 22
Ethernet card
  configuring for fixed operation 288
Ethernet switch 77
Executive Assistant with Cockpit 469
EZIP 581

F
Fallback 382, 507

G
general safety 21
graphical and numerical data screens 574
Guest machine 207
Guidelines 174

I
installation
  assumptions 29
  checklist 30
  media 28
  prerequisites 29, 115
Installation prerequisites 297
Installation Wizard 51
installing
  OpenScape Voice hardware platform 73
  the client 573
install_time.log 577
IPSec configuration 671

K
KVM/Mouse combination 291

L
Linux Accounts 437
Login credentials 188

M
menu structure of BTT 574
Migration 521
Migration Toolkit Software 548
Migrations 417
Multiple Communications Server 331

N
Node.cfg file 181
node.cfg file 115

O
OpenScape Applications 295, 370
OpenScape Voice
  basic traffic tool 573
  installation 29
  signaling stream security 651
  software installation 115
OpenScape Voice Reference Image 115
Overview 171

P
prerequisite knowledge 19

R
Remote SW Upgrade 491
reporting accidents 23

S
safety information 21
setting Ethernet NICs 288
signaling

stream security
OpenScape Voice 651
Standalone Survival Authority 395
Survival Authority Configuration 409

T

testing
KVM/mouse combination 291
Toolkit Method 471
Trace File Information 373
transport layer security (TLS) 651

U

Uninstall Integrated Simplex 313
upgrade
paths 424
Upgrades 417, 443
User ID and Password 276
using the basic traffic tool 573

V

Virtual floppy disk 185
Virtual switch 191
Virtualization 170
VM Configuration Parameters 175
VM CPU requirements 180
VM Disk requirements 180
VM Memory requirements 180
VM Network requirements 177
VM Solutions 177
VMware vSphere client 188
vSphere client 186

© 2026 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.