A MITEL
PRODUCT
GUIDE

Unify OpenScape Voice V9

Service Manual

Service Documentation
08/2024

A31003-H80A0-S100-9-76A9

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.

Contents

1 Introduction

The documentation at hand describes the OpenScape Voice system functionality from a service-oriented point of view.

Scope

The following main functional areas are covered in this documentation:

- Licensing and Packaging
- Backup and Restore
- Software Maintenance (Patching: Online and Remote)
- Diagnostics (Call Tracing, Debugging, Diagnostics)
- Traffic Measurement
- System Monitoring (Alarm Handling, Event Logging, Audits, RapidStat, etc.)
- Remote Operation
- Data Import/Export

1.1 About this Documentation

Audience

Prerequisite Knowledge (Administrators)

Practical Hints on Working with the User Interface

Support of IPv6 in OpenScape Voice Environments

This documentation addresses administrators who configure and manage a communications network with OpenScape products.

Adequate administrator access rights are required to perform administrative tasks within the OpenScape Voice system. Please refer to the corresponding sections about user profiles and access rights for more information.

For making full use of the information provided in this documentation we assume the following knowledge:

- Knowledge of the general working method of communications systems
- Knowledge of terms used in the environment of communications systems
- Practical knowledge of how to configure and manage communications systems
- 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
- **Mandatory fields** are highlighted in **bold** type in the user interface of the OpenScape Voice Assistant.

- Unless explicitly specified otherwise, only valid ASCII characters (a-z, A-Z, 0-9, and underscores) must be used when entering names and other attributes of OpenScape Voice-managed entities. Do **not** use special characters or spaces.
- A powerful, configurable **Search and Filtering** functionality provides for quick, focused search and retrieval of specific information. For details, please refer to the *Search and Filter Functionality* section.
- **Office Codes** can be longer than 9 digits (up to 14 digits).
- The **Destination Code Table** can be provisioned with a range of codes.
- The **Code Restriction Service** accepts the wildcard "x".

OpenScape Voice supports IPv6 on various interfaces.

- IPV6 networks in mixed configurations (IPV4 parts and IPV6 parts) are supported by the OpenScape Voice Assistant. The OpenScape Voice Assistant itself is deploying IPV4 presently. The OpenScape Voice Assistant is able to administer IPV6 addresses (128 bits) in the OpenScape Voice switch and DLS (DlsAPI).

1.2 System Overview

OpenScape Voice is a carrier-class softswitch that is scalable from 300 to 100,000 users per system. When networked, the number of subscribers is virtually limitless. The system runs on highly reliable, fault-tolerant servers using SuSE Linux Enterprise Server Operating System from Novell. The core protocol of OpenScape Voice is the IETF Session Initiation Protocol (SIP).

Components of the OpenScape Voice System Solution

Hardware for OpenScape Voice

Software for OpenScape Voice

Tools for System Administration and Provisioning

Applications

Supported Devices

Hard Phones

Soft Clients

Analog Adapters

SIP Gateways - for Access to the PSTN and other TDM Networks

Gateways

Mediatrix Gateways

Other Gateways

Other Network Devices

In addition to industry-standard SIP, OpenScape Voice supports SIP-Q (QSIG over SIP) for interfacing to legacy PBX systems—for example, HiPath 4000.

The following servers can be used as computing nodes for OpenScape Voice:

- IBM x3250 M2 (upgrades only)
- IBM x3250 M3
- IBM x3550 M3
- IBM x3550 M4
- FTS RX200 S6
- FTS RX200 S7

NOTICE:

The FSC RX330 is available for upgrades and new installations; the xSeries 346 has gone end-of-life and is no longer available for new installations. Upgrades to OpenScape Voice V8 are not supported on the xSeries 346 server; V8 upgrades to x346-based OpenScape Voice requires replacement of the x346 server with either the IBM x3650T or FSC RX330 server.

Among other functions, this software controls call processing, signaling, and cluster operation in redundant systems.

- **Graphical User Interface** for **Common Management Platform** and integrated applications, including:

  OpenScape Voice Assistant
  OpenScape Voice Media Server
  OpenScape UC Application
  OpenScape Branch Assistant
  Deployment and Licensing Service (DLS) for managing SIP endpoints

- **Command Line Interface (CLI)** for system administration and provisioning

Unify applications such as OpenScape Xpressions, OpenScape ComAssistant, OpenScape Contact Center, and OpenScape UC Applicationprovide such functionality as unified messaging, computer-telephony integration, and call center support.

- OpenStage telephones (Models 15, 20, 20E, 40, 60, and 80)
- optiPoint 410/420 SIP
- optiPoint 150 S
- Limited support for SIP-compliant third-party devices
- Cordless IP handset, base station and server software

- optiClient 130 S
- OpenScape Desktop Client Personal Edition
- OpenScape Web Client
- OpenScape Desktop Web Embedded Edition

- HiPath AP 1120 - 2 ports (Does not support SRTP)
- Mediatrix 4102 - 2 ports
- Mediatrix 4104 - 4 ports
- Mediatrix 4108 - 8 ports
- Mediatrix 4116 - 16 ports
- Mediatrix 4124 - 24 ports

- HiPath 3000
- HiPath 4000
- OpenScape Branch 50i (Appliance with integrated Gateways)

- Mediatrix 1204
- Mediatrix 4402
- Mediatrix 4404
- Mediatrix 3600

- Cisco 2621XM, 2650XM, 3725 (PSR required)

- OpenScape Branch solution (50 to 6000 users)

- Comdasys Convergence 1600 branch office proxy/registrar for survivability (50 users)
- Comdasys Convergence 2600 branch office proxy/registrar for survivability (100 users)
- Comdasys 3600 branch office proxy/registrar for survivability (1500 users)
- Session Border Controllers

  Comdasys SIP proxy running in SBC mode

  NOTICE:

  The OpenScape Branch products include integrated SBCs, so they do not require the use of an external SBC.

- OpenScape Media Server

  NOTICE:

  Hardware recommendations for the OpenScape Media Server are specified in the *Media Servers Supported by OpenScape Voice* section of the *OpenScape Voice Configuration, Administrator Documentation*.

- RadiSys Convedia media servers (CMS-1000, CMS-3000, CMS-3000 SEC)

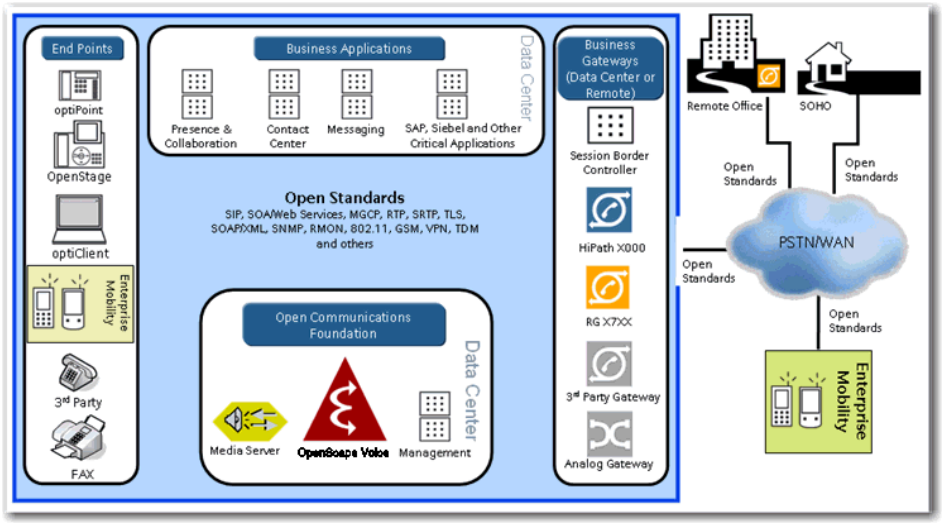

Figure 1: OpenScape Voice Main Components

1.3 Safety Information

Special Notices

Safety

General Safety

Safety with Electricity

High Voltage

Equipment Room

Emergencies

Reporting Accidents

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

Potentially dangerous situations and information of special importance are noted throughout this documentation. The following alert indicators are used:

IMPORTANT:

An important notice calls attention to conditions that, if not avoided, may damage or destroy hardware or software, or may result in unrecoverable data loss.

NOTICE:

A "note" notice calls attention to important additional information.

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

- 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.

- 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.
- 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.

- 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, approved by Unify. 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.

- 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.

- 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 Licensing and Packaging

2.1 Licensing

There are different license types available for **OpenScape Voice** and **OpenScape Unified Communications.**

2.1.1 OpenScape Voice Base License

The OpenScape Voice base license provides full usage of the basic switch software.

The base license also includes 100,000 static licenses at no charge. These licenses are used to provision DNs (Directory Numbers), including primary and phantom lines.

2.1.1.1 How to Activate the OpenScape Voice license

License activation with the license file(s) is necessary. The license file is used to activate the associated licenses and thus the products and their features. The following are examples of license files: 00-50-56-3F-59-8D_OpenScape_Voice_V9_STANDBY-Full.lic, 00-1A-64-21-0B-19_OpenScape_Voice_V9-PF028.lic, 00-50-56-3F-59-8D_OpenScape_Voice_V9-Full.lic

Prerequisites

One license file per node has been acquired

Adequate administrative permissions

Step by Step

1) Determine the appropriate license file for each node of the OSV system.

2) Log in to node1 as srx user in order to execute the following steps.

3) Transfer the node1 license file to path `/opt/unisphere/srx3000/cla_inst/import/` of node1.

4) Execute the following command:

`/unisphere/srx3000/callp/bin/import_license.sh`

In case of failure, escalate to your next level of support. Otherwise, proceed to the next step.

5) For Duplex systems: Repeat steps 2), 3) and 4) for node2.

The license management verifies the signature of the license file against each node's Locking ID. If the verification is successful, the activated licenses are displayed in the Common Management Platform with the associated information.

2.1.1.2 How to Display Bound Licenses

With this task, it is possible to check the bound licenses assigned to a user. Users obtain licenses when they are assigned a profile containing the relevant features.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **User Management > Users & Resources** > **Users**
2) Select a User. Click **Add/Edit** > **Profiles**
3) Select a Profile name and click **Show bound licenses**.

The licenses assigned to a profile / user will be displayed.

NOTICE:

If no licenses are available, the button **Show bound licenses** is inactive.

2.1.2 OpenScape Voice Dynamic User License

Dynamic user licenses control the number of home DNs (Directory Numbers) that can have telephones (and soft clients) simultaneously registered on the system. Often, subscribers (home DNs) have more than one telephone and/or soft client.

One dynamic user license is required for the registration of each unique DN; phantom and secondary lines are not considered unique DNs and are therefore excluded. 100 dynamic user licenses are included as part of some package types. Additional licenses are purchasable.

The number of dynamic user licenses determines the following:

- The number of primary DNs that can be registered concurrently.
- The number of non-keyset DNs that can have one or more telephones/soft clients simultaneously registered on the system.

NOTICE:

Licenses that are purchased or included with a particular package only become available on the OpenScape Voice server when the license file is applied to each node of the OpenScape Voice server. Until then, only the default number of 100 licenses will be available.

The total number of dynamic user licenses form a license pool. Upon SIP registration, the user is granted a single license from the pool of available licenses based on the rules stated above.

OpenScape Voice enforces dynamic user licensing when a registration attempt occurs, as follows:

- If the dynamic user license usage exceeds the warning threshold (default value is 95% of the assigned licenses), a warning is generated to the customer's system administrator. At this point, purchasing additional licenses may be necessary to provide a margin of safety.
- If the dynamic user license usage exceeds 100% of the assigned licenses, a violation alarm is generated to notify the system administrator to immediately purchase more licenses. Licensing enforcement is activated when the number of violations reaches the defined limit of 10, which indicates that usage violations have occurred on ten cumulative days.

After enforcement is initiated and the license pool is completely depleted by the number of incoming SIP registered users, the next endpoint is denied registration and is unable to originate or terminate calls, including emergency calls.

Related concepts

OpenScape UC Server License on page 29

2.1.3 OpenScape Voice Encryption Licenses

Encryption licenses control the number of subscribers in OSV which are configured to allow SRTP and for which at least one contact is registered using the TLS transport type.

Encryption licenses are handled in the same way as dynamic licenses, meaning similar counters, enforcement at registration time, support for subscription based licensing, support for regular license files. This enforcement follows the existing dynamic licensing mechanism (not activated by default; the system allows a predefined number of licensing violations to occur before enforcement is activated).

As long as the Encryption license enforcement is not active, all devices are allowed to register even when exceeding the system's encryption licenses.

NOTICE:

If Dynamic Licensing enforcement or OSMO licensing enforcement is active, the Registration Request may be rejected because of the enforcement for those licenses. OSV keeps track of violations and generates alarms when appropriate to notify the system administrator about the violations.

A registration requiring a new encryption license will be rejected if encryption license enforcement is active and all encryption licenses are used.

NOTICE:

As soon as enforcement becomes active, devices which require but don't possess an encryption license will lose their registration on the next re-registration. This constitutes a complete loss of calling capabilities including the ability to make emergency calls from the device.

2.1.3.1 Reporting of Encryption License usage for Subscription Licensing

Reporting of Encryption License usage to the central subscription licensing service of the CMP is done via a polling mechanism through the OpenScape Voice Assistant and OpenScape Voice SOAP server.

Encryption License usage reporting includes the value of the Encryption High Water Mark counter, the billing period that the counter refers to as well as the product Instance ID, and the number of days until the expiration of the installed Encryption licenses.

All the data needed for Encryption usage reporting is provided by the license manager to the SOAP server.

2.1.3.2 Endpoint Attribute "Disable SRTP"

The "Disable SRTP" endpoint attribute is applicable to subscribers and endpoints, and is unchecked by default.When the new attribute is unchecked SRTP is allowed to and from the endpoint, and If Encryption license checking is enabled in the OSV license file, an Encryption license is checked out when a subscriber registers a contact using TLS.

If a license is unavailable and enforcement is enabled for Encryption licensing due to 10 violations, the registration is rejected with a 402.When the "Disable SRTP" attribute is checked, then SRTP is not offered to the endpoint and removed when offered by the endpoint. An Encryption license is not checked out with this setting.

2.1.4 OpenScape Voice Redundancy License

The OpenScape Voice redundancy license provides full usage of the necessary software required to implement cluster redundancy for co-located or geographically separated nodes.

2.1.5 OpenScape Voice ELA License

The Enterprise License Agreement (ELA) User Suites (Voice Suite, Enhanced Voice Suite and Collaboration Suite) use OSV for voice functionality and differentiate between them through functionality offered from other products. This difference in functionality is enforced through licenses used by other Unify products and so does not concern OSV. On OSV these Suites will consume Dynamic User Licenses (DULs).This differentiation will be enforced on OSV during registration of the device. The lowest end devices (such as analog devices) can register when an Essential or higher type license is used, the mid end devices can register when a Basic or higher end license is used and the high end devices can only register when a DUL license is used as is done now.

NOTICE:

Violation functionality will continue to work as currently implemented for DULs and OpenScape Mobile licenses. So a violation will occur for any license type that is exhausted, but registration will be allowed for that license type in case

enforcement is not activated. Enforcement will be activated as it is done now, after a predefined number of violations occurs. During enforcement, new licenses of an exhausted license type will not be allowed to be consumed. Re-registrations of a device, whose subscriber consumed a license that was already exhausted will not be allowed.

2.1.6 License Information

The legal use of the OpenScape system features requires the corresponding product licenses. You can use the license management to activate these licenses and to view license information. The license management works domain-spanning.

Central License Server (CLS) The Central License Server (CLS) generates and manages the license files. A license file is generated when the License Authorization Code is sent to the CLS by Common Management Platform. The transfer of the license file to Common Management Platform occurs automatically via the internet.

IMPORTANT:

When you connect the Common Management Platform computer system to the internet, make sure that the computer system can only connect to the CLS and other selected, secure target systems.

NOTICE:

In certain circumstances the Common Management Platform may not be able or desired to access the internet. In this case it is possible to manually generate the license file at the CLS and to download it. The associated licenses can then be activated in the Common Management Platform with the license file alone and without internet connection.

Every customer or sales partner has a separate license account on the CLS. The accounts can be maintained at the CLS via a separate web-based user interface. All available and already purchased licenses can be displayed.

Common Management Platform

The licenses are activated with Common Management Platform. The Common Management Platform transfers the License Authorization Code (LAC) to the CLS and receives the associated license file.

The licenses and their related information are displayed in Common Management Platform. You can see the total number of licenses. You can see which licenses are assigned to which applications or features, and when these licenses expire. In addition, you can see how many licenses are still free.

Grace Period

After purchasing or installing the product/feature, the license for it must be activated within a specified time period - called the grace period. Depending on the product involved, this period may be e. g. 30 days.

During this grace period, the product may be restricted or fully functional. If you do not install a license after the grace period, the product becomes severely restricted or stops working entirely.

MAC address (Locking-ID)

During production, hardware is assigned a board-specific number called a MAC address which is unique world-wide. To guarantee unique licensing, the license file is linked to the hardware's MAC address (for example, network card of the system server). Every project/feature license is therefore linked to this locking ID. For the case of virtualized applications, the standard MAC address cannot be used to form a unique ID for locking purposes. So in this case an Advanced Locking ID (ALI) is employed and this involves combining the hostname with certain other key information to form a unique ID which can be used for locking purposes.

The Advanced Locking ID is a 23 byte string comprised of the following information:

GW address

Host name

Host IP Address

Primary DNS

2.1.6.1 How to Display OpenScape License Information

This task is used to retrieve information about license status.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **Maintenance > Licenses > Information**.
2) A list of all features available in the OpenScape system is displayed in the work area. This list contains for each entry the following information:

   Product Name

   Shows the name of the product for which the license information is being displayed.

   Feature Name

   States the feature name.

   Number of used licenses

   Specifies how many licenses are altogether available for the feature and how many of these are already used.

   Validity

   Shows the validity for the feature's licenses. License entries that are invalid or have expired or are about to expire are marked red.

3) You have the option of filtering the list according to specific terms (patterns).
   a) Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).
   b) From the list displayed, select whether the filtering is to be applied to the Product Name or Feature Name column.
   c) Click on **Go** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.
   d) Click on **Clear** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

Related tasks

How to Display and Change Licensing Warning Thresholds on page 31
How to Display the License Usage on page 34

2.1.6.2 How to Enable/Disable Demo Features in OSV

When the user has an OSV switch of version V9(> or equal to V9ps21) and the path `/unisphere/srx3000/callp/bin/` has an alf file of version V8(OSCVoice_V8.alf), then by default all the V9 features are disabled. To enable them, follow the following steps

Prerequisites

Adequate administrative permissions

Step by Step

1) Use the `startCli`
2) Navigate to the menu: **6** > **1** > **1** > **10**
3) The following options appear
   - Selection: 10
   - Software License Management (methods):
   - Display Usage Indicator Info.....1
   - Display Warning Thresholds.....2
   - Modify Warning Thresholds.....3
   - Display VM license locking IDs.....4
   - Display SUSE update Service status.....5
   - Display License File version.....6
   - Enable Feature Field Trial.....7
   - Disable Feature Field Trial.....8
   - Display Feature Field Trial State.....9
4) Choose between options 7 and 8 to Enable/Disable features in V9.
5) After Enable/Disable has been applied, you can select menu option 9 to display the current state of the features.

NOTICE:

For information on how to enable/disable Features via the Assistant, refer to chapter **SLL Features** on *OpenScape Voice, Administrator Documentation*.

2.1.6.3 How to Display License Locking IDs

A locking ID is a unique feature of a computer system - e. g. the MAC address of a network board. The purchased licenses are linked to the Locking ID. You must select the Locking ID to which you want to bind licenses the first time you license the system. All further licensing activities are performed with this Locking ID.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance > Licenses** > **Locking IDs**
2) A list of all computer systems available in the entire system is displayed in the work area. This list contains for each entry the following information:

   NOTICE:

   If a Locking ID was already used for licensing, it is the only Locking ID displayed.

   Locking ID

   Shows the Locking ID (MAC address) of the system to which the licenses are registered.

   Adapter Name

   Shows the name of the adapter that provides the Locking ID.

   Logical Name

   Specifies the logical name of the adapter that provides the Locking ID.

   IP Address

   Specifies the IP address of the adapter that provides the Locking ID. Here there could be several IP addresses displayed - such as in server scenarios. or no IP address (adapter out of service).
3) If you need access to the central license server, click **Link to the Central License Server**.

2.1.7 OpenScape UC Server License

The OpenScape UC (Unified Communications) Server is the software foundation for OpenScape Unified Communications.

This license includes the following:

- SIP Session Control
- Aggregated Presence
- QoS Management
- Session Detail Reports
- Administration and Licensing
- Availability Management

Related concepts

OpenScape Voice Dynamic User License on page 23

2.1.8 OpenScape UC Application License

The OpenScape UC (Unified Communications) Application Enterprise base license is a specific license for the OpenScape UC Application.

The following license type is available:

- Essential

2.1.9 Unify Phone License

The Unify Phone License provides full usage of the necessary software required to register a Unify Phone client.

NOTICE: A Unify Phone client requires a dynamic user license (DUL) and a unify phone license in order to register to the OpenScape Voice server. So, for a user that uses one or multiple Unify Phone clients, a dynamic user license (DUL) and a unify phone license will be consumed. If the user except from Unify Phone clients uses also one or multiple telephones or soft clients, a dynamic user license (DUL) and a unify phone license will be only consumed too.

2.1.10 Symphonia Licenses

Symphonia provides the default user-profiles for the access privileges of the Common Management Platform. If a profile is e.g. assigned to the Symphonia application, it controls the access privileges for the components integrated in the Common Management Platform – for example for the profile or domain administration.

The product names and licenses required for the activated privileges are displayed in the Licenses area.

Functional Sequence

The Symphonia application controls the access privileges for the features of the Common Management Platform.

The user is authorized to do the following if in its profile those features are assigned:

- License Management Admin

  The license **License Management Admin** is required for every regular (user) administrator, e.g. for bind and unbind functions of licenses to the users.

- License Management Extra

  The license **License Management Extra** is required for license-oriented system administration, e.g. for tests and special functions like Synchronization and License Consistency Checks.
- License Management Info

  The license **License Management Info** is required for any administrator who needs to view licenses available/in use information for showing license data like show License Usage.

2.2 Licensing Management

The licensing mechanism includes an OpenScape Mobile license type.

The handling of this license type closely follows the current behavior of dynamic licenses except that its count is managed separately. OpenScape Mobile licenses control the number of concurrent registered clients, each reserving a single license for its DN.

If the license file does not contain an entry for OpenScape Mobile then OpenScape Voice considers OpenScape Mobile licensing as not being activated. License usage will operate as before (i.e., the dynamic license pool will be used to serve OpenScape Mobile users).

NOTICE:

The Trace Manager is able to monitor the key performance indicator *Used OpenScape Mobile Licenses*.

2.2.1 How to Display and Change Licensing Warning Thresholds

This feature allows the administrator to specify the threshold level at which a warning alarm is generated relating to the number of conducted calls.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Configuration > OpenScape Voice** > **Administration** > **Licensing Management** > **Thresholds**.

2) The following items will be displayed

- **Dynamic Licensing Warning Threshold**
- **Basic Licensing Warning Threshold**
- **Essential Licensing Warning Threshold**
- **OpenScape Mobile Licensing Warning Threshold**
- **Encryption Licensing Warning Threshold**
- **Unify Phone Licensing Warning Threshold**

Warning Threshold for Dynamic, Basic, Essential, OpenScape Mobile and Encryption Licensing with the default value being 95%, and the valid range being [0% ...100%].

NOTICE:

Essential , **Basic** and **Unify Phone** licenses are available only when ELA licensing is enabled.

3) Click **Save** to change the threshold values.

Related concepts

OpenScape Voice Client Access License

Related tasks

How to Display OpenScape License Information on page 27

2.2.2 How to Monitor Dynamic Licensing

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP and activate the **OpenScape Voice** tab.
2) Navigate to **Administration** > **Licensing Management** > **Dynamic Licensing Monitoring**.

   The window **Dynamic Licensing** is displayed with the List of Dynamic Licensing statistics.
3) Select a time or a time period to check the license usage.

2.2.3 How to Monitor Basic Licensing

Prerequisites

Adequate administrative permissions

Basic license is available only when ELA licensing is enabled.

Step by Step

1) Log on to the CMP and activate the **OpenScape Voice** tab.

2) Navigate to **Administration** > **Licensing Management** > **Basic Licensing Monitoring**.

   The window **Basic Licensing** is displayed with the List of Basic Licensing statistics.

3) Select a time or a time period to check the license usage.

2.2.4 How to Monitor Essential Licensing

Prerequisites

Adequate administrative permissions

Essential license is available only when ELA licensing is enabled.

Step by Step

1) Log on to the CMP and activate the **OpenScape Voice** tab.
2) Navigate to **Administration** > **Licensing Management** > **Essential Licensing Monitoring**.

   The window **Essential Licensing** is displayed with the List of Essential Licensing statistics.

3) Select a time or a time period to check the license usage.

2.2.5 How to Monitor OpenScape Mobile Licensing

With the statistics logging activated, periods of time can be searched to analyze usage patterns and identify peaks and valleys of license usage.

NOTICE:

If **OpenScape Mobile** licensing is not enabled then the window ‘OSMO Licensing’ shows text indicating that no statistics exist.

Step by Step

1) Navigate to **Configuration** > **OpenScape Voice** > **Administration**.
2) Expand **Licensing Management** and select **OpenScape Mobile Licensing Monitoring**.

   The window OpenScape Mobile Licensing is displayed with the List of OpenScape Mobile Licensing statistics.

3) Select a time or a time period to check the license usage.

2.2.6 How to Monitor Encryption Licensing

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP and activate the **OpenScape Voice** tab.
2) Navigate to **Administration** > **Licensing Management** > **Encryption Licensing Monitoring**.

   The window **Encryption Licensing** is displayed with the List of Encryption Licensing statistics.
3) Select a time or a time period to check the license usage.

2.2.7 How to Monitor Unify Phone Licensing

Prerequisites

Adequate administrative permissions

Unify Phone license is available only when ELA licensing is enabled.

Step by Step

1) Log on to the CMP and activate the **OpenScape Voice** tab.
2) Navigate to **Administration** > **Licensing Management** > **Unify Phone Licensing Monitoring**.

   The window **Unify Phone Licensing** is displayed with the List of Unify Phone Licensing statistics.
3) Select a time or a time period to check the license usage.

2.2.8 How to Display the License Usage

In the Licenses Usage View a summary of the license information will be displayed.

Prerequisites

Adequate administrative permissions

Basic and Essential licenses are available only when ELA licensing is enabled.

Step by Step

1) Navigate to **Configuration > OpenScape Voice** > **Administration** > **Licensing Management** > **Usage**.

2) The following information will be displayed in the window **License Usage**:

a) **Dynamic Licenses Information OpenScape Voice**

- Assigned to the System: Total number of available licenses for the system.

- In Use: Specifies how many licenses for the product are currently in use.

- Total for OpenScape Mobile Devices: Specifies how many licenses are currently being used for the Mobile Devices.

NOTICE:

"Total for OpenScape Mobile Devices" is displayed only if no OpenScape Mobile Licenses are present.

- Maximum Usage of Previous Day: Specifies how many licenses of the product have been used during the last 24 hours.

- Customer Violations / Limit: Displays the number of license violations and the limit set.

NOTICE:

If OpenScape Mobile licensing is not enabled then the counters are not shown and “OpenScape Mobile Licensing is disabled” is displayed instead.

---

b) **Basic Licenses Information OpenScape Voice**

- Assigned to the System: Total number of available licenses for the system.

- In Use: Specifies how many licenses for the product are currently in use.

- Total for OpenScape Mobile Devices: Specifies how many licenses are currently being used for the Mobile Devices.

NOTICE:

"Total for OpenScape Mobile Devices" is displayed only if no OpenScape Mobile Licenses are present.

- Maximum Usage of Previous Day: Specifies how many licenses of the product have been used during the last 24 hours.

- Customer Violations / Limit: Displays the number of license violations and the limit set.

NOTICE:

If OpenScape Mobile licensing is not enabled then the counters are not shown and “OpenScape Mobile Licensing is disabled” is displayed instead.

---

c) **Essential Licenses Information OpenScape Voice**

- Assigned to the System: Total number of available licenses for the system.

- In Use: Specifies how many licenses for the product are currently in use.

- Total for OpenScape Mobile Devices: Specifies how many licenses are currently being used for the Mobile Devices.

NOTICE:

"Total for OpenScape Mobile Devices" is displayed only if no OpenScape Mobile Licenses are present.

- Maximum Usage of Previous Day: Specifies how many licenses of the product have been used during the last 24 hours.
- Customer Violations / Limit: Displays the number of license violations and the limit set.

NOTICE:

If OpenScape Mobile licensing is not enabled then the counters are not shown and “OpenScape Mobile Licensing is disabled” is displayed instead.

d) **OpenScape Mobile Licenses Information for OpenScape Voice**

- Assigned to the System: Specifies how many licenses are available for the system.
- In Use: Specifies how many licenses are assigned to subscribers
- Maximum Usage of Previous Day: Specifies how many licenses of the product have been used during the last 24 hours.
- Customer Violations / Limit: Displays the number of license violations and the limit set.

e) **Encryption Licenses Information for OpenScape Voice**

- Assigned to the System: Specifies how many licenses are available for the system.
- In Use: Specifies how many licenses are assigned to subscribers
- Maximum Usage of Previous Day: Specifies how many licenses of the product have been used during the last 24 hours.
- Customer Violations / Limit: Displays the number of license violations and the limit set.

f) **Unify Phone Licenses Information for OpenScape Voice**

- Assigned to the System: Specifies how many licenses are available for the system.
- In Use: Specifies how many licenses are assigned to subscribers
- Maximum Usage of Previous Day: Specifies how many licenses of the product have been used during the last 24 hours.
- Customer Violations / Limit: Displays the number of license violations and the limit set.

Related concepts

OpenScape Voice Client Access License

Related tasks

How to Display OpenScape License Information on page 27

2.3 Packaging

OpenScape Voice and OpenScape Unified Communications are available with several license types and packaging options which can be combined to fit the needs of the enterprise.

2.3.1 Deployment Models

The available deployment models can be distinguished between redundant and non-redundant configurations with a different maximum number of subscribers.

The following deployment models are available:

- The integrated simplex non-redundant configuration consists of one OpenScape Voice server operating as a standalone system.

  This configuration supports 5000 subscribers if only OpenScape Voice is available and 1000 subscribers in a solution with OpenScape Voice and OpenScape UC (Unified Communications) Application users.

  The OpenScape Voice applications (OpenScape Voice Assistant, Media Server, Customer License Manager, Common Management Platform and Deployment Service), the OpenScape UC Application and the OpenScape SBC reside on the OpenScape Voice server.

- The standard duplex redundant configuration provides redundancy comparable to that of the integrated duplex configuration.

  This configuration supports 100.000 OpenScape Voice subscribers, of which up to 2000 can be OpenScape UC Application subscribers depending on the voice mail system present.

  The OpenScape Voice applications, as well as the OpenScape UC Application and OpenScape SBC, reside on an external server. Geographically separated nodes are supported by OpenScape Voice, not by the OpenScape UC Application.

  NOTICE:

  Supported subscribers depend on hardware and applications configuration. This number can vary widely depending on the features in use at the enterprise.

- The Standard Duplex Large configuration extends the capacity of the Standard Duplex deployment with an added capacity of max 200,000 DNs provisioned in the database. However, the limit of maximum 100,000 registered subscribers and therefore the call model remains the same as the Standard Duplex deployment. The additional provisioned DNs are useful in a large DLS mobility setup, where a virtual device along with a real device need to be provisioned per subscriber, but only one at a time can be registered to the OSV.

  This deployment is available only on systems with at least 12 GB of RAM:

  – IBM x3550 M3
  – IBM x3550 M4
  – Fujitsu RX200 S6

– Fujitsu RX200 S7

3 Serviceability - B&R, Import/Export, SW Maintenance

These features provide mechanisms to improve serviceability.

3.1 Backup & Restore

You can use the backup & restore feature to back up all data and the software of the entire OpenScape Voice system, which includes the operating system and all applications. You can thus restore a complete single- or double-node system after a severe system crash.

OpenScape Voice uses mirrored harddisk drives to minimize the chance of a severe system crash. Owing to these mirrored harddisks, a complete system crash is very unlikely. It is nonetheless necessary to back up the system data in regular intervals for reasons of precaution. The complete failure of a single node or of both systems without any previous backup would lead to a long-lasting failure of the OpenScape Voice system combined with a loss of data.

Use of the backup & restore feature

The backup & restore feature concerns the following data:

- The file system via a backup script, a restore script and the CMP
- The database with the system configuration and the system data via the CMP

IMPORTANT:

Do not rename the backup file as the name contains information used by the restore script.

Methods of backing up or restoring data

Using the backup & restore feature you can back up & restore data in the following manners:

- By means of the fallback partition of the OpenScape Voice server system
- With the aid of an external USB harddisk drive (USB-HDD).
- Using an external backup server.

Scheduling a backup

So that current system data are available in case of a system crash, data of the OpenScape Voice system should be backed up at the following times:

- Immediately after the initial installation
- Immediately before installing patches
- Immediately after installing patches
- Immediately before a software upgrade
- Immediately after a software upgrade
- After comprehensive configuration changes (recommended as addition to regular backups)
- Periodically, at least once per month. We recommend backups in shorter intervals – e. g. once every week.

Typical backup & restore periods

Backing up or restoring an OpenScape Voice system requires approximately the following times:

- Backing up an OpenScape Voice system
  - If you use an external backup server, it takes approximately 75 minutes to back up an unloaded OpenScape Voice node.
  - If you use a fallback partition, it takes approximately 20 minutes to back up an unloaded OpenScape Voice node.
- Restoring a OpenScape Voice system
  - If you use an external backup server, it takes approximately 130 minutes to restore an OpenScape Voice node. (Size of the backup file is approximately 4.2 GB)
  - If you use an external USB harddisk drive, it takes approximately 42 minutes to restore an OpenScape Voice node. (Size of the backup file is approximately 1.6 GB)

The precise time required by the backup and restore process depends on the size of the backup file and on the system environment of the OpenScape Voice system.

Requirements

You must hold the following things ready to restore a system via the backup & restore feature after a crash:

NOTICE: Without these things you can only restore the system by completely reinstalling the OpenScape Voice system, its applications and patches, and executing all individual system adjustments anew. This is a long and error-prone process.

- The OSV installation and restoration DVD image ISO. We recommend to always use the currently available version. In order to restore both nodes simultaneously in a redundant system, two OSV DVD images are required.
- A current backup of each system node

The backup script

The `hiq_backup.sh` backup script is used to back up the file system of an OpenScape Voice system. It is installed with each OpenScape Voice system.

This backup script uses the following default directories for the backup process by default:

- As temporary working directory
  - `/var/backup` in case of a non-imaged system
  - `/software/backup` in case of an imaged system
- As concluding output directory:
  - also `/var/backup` in case of a non-imaged system
  - also `/software/backup` in case of an imaged system

The backup system backs up only the following required partitions of a OpenScape Voice computer system:

- `/`

- /unisphere
- /home
- /opt
- /enterprise
- /var

3.1.1 Backup & Restore with a Backup Server

Backup files can be stored on an external backup server. Such a backup server may be exclusively available to one OpenScape Voice system or be used for several ones, depending on the selected backup strategy.

The backup server must comply with the following requirements:

- The backup server must be able to receive and send backup files that were created via the OpenScape Voice feature Backup & Restore. The transmission occurs via FTP or Secure FTP (OpenSSL).
- The following redundancy requirements must be complied with, by using eg. duplicate hard disk drives:
  - The backup server should have two hard disk partitions on different hard disk drives – primary backup partition and secondary backup partition.
  - The primary backup partition should normally be used for all transmissions from and to the OpenScape Voice system.
  - The backup files can be copied from the primary backup partition to the secondary backup partition by manual operation or scripts.
- Manual or script-based file management is required for the following processes:
  - To synchronize primary and secondary backup partitions.
  - To provide at least two backup files per OpenScape Voice system. After an additional set of backup files has been saved, the oldest set of backup files can be deleted.
  - To archive selected sets of backup files to prevent them from inadvertent deletion.
  - To delete obsolete sets of backup files if no memory is available for current ones.
- Sufficient hard disk capacity for backup files
- Storage of each backup file on two storage media that are physically independent from each other.
- If duplicate hard disk drives are to be used, the backup server should deploy the following additional components:
  - An optional optical or band-based backup system
  - A commercial mechanism to mirror the hard disk drives.

An optimal backup server location must be found, for which the following should be considered:

- Use of an existing backup server that already saves the data of other systems.
- Available bandwidth for the connection between OpenScape Voice system and backup server. Since the backup files are relatively big, a low bandwidth prolongs the system restoration time and thus the OpenScape Voice system downtime.

- Local setup of the backup server at the OpenScape Voice system. In this case the backup files need to be stored at another site also.
  - By means of transmission to a remote server – e. g. via FTP.
  - By means of a streamer the tapes of which are stored at another site.

3.1.1.1 How to Back Up a File System on a Backup Server

To back up the file system of an OpenScape Voice system on a backup server, you need to back up the file system of the single node in case of a single-node system. In case of a redundant system, back up the file system of each single node. Use in both cases the backup script shipped with the OpenScape Voice system.

Prerequisites

root access for the backup script. If access is denied, change as user root in the `sshd_config` file the setting of the **PermitRootLogin** parameter to **yes**. Reboot the sshd-Daemon exclusively with the `/etc/init.d/sshd restart` command.

IMPORTANT:

This change can conflict with the security policy of the customer! How you reduce in that case the SSH ports used by the OpenScape Voice system describes the bulletin INF-09-000766– SSHD Interface Hardening.

No rolling upgrades, patch activities or configuration modifications are performed in the OpenScape Voice system.

The CPU load of the computer system to be backed up amounts to a maximum of 50 %.

The local hard disk drives of the computer system to be backed up offer sufficient memory for the additional backup files. The backup script checks this requirement immediately after the start.

General instructions:

File System Backup can lead for a short period of time (depending on the data) to a high disk I/O causing delays. Thus, file system backup should be planned for times with low or no traffic.

To avoid taking a File System Backup every day, you can perform one after a successful file system backup on both nodes and during the next days you can perform a delta backup by taking a light DB backup.

File System Backup usually is done only on HW systems and should be performed after (you can also perform a backup on VMs, but usually VM snapshots are sufficient):

1. major configuration changes

2. image upgrades (toolkit)

3. HF upgrades (Rolling Upgrade or RU)

NOTICE: File System Backup cares ONLY for the active partition.

IMPORTANT:

The backup script only secures the following required partitions of an OpenScape Voice computer system: `/`, `/unisphere/`, `/home/`, `/opt/`, `/enterprise/` and `/var/`.

NOTICE:

For the backup script and the following commands can be executed, you need to log on to the computer system to be backed up as root user. If you want to back up a computer system remotely, you need to log on as sysad user first, and then switch to the root user with the `su -root` command.

Step by Step

1) On the CE1 computer system of the OpenScape Voice system log on as user `root`.
2) Use the following command to switch to the `var/backup` directory on the computer system: `cd /var/backup`

3) Start the backup script:

- Start the backup script with the following command for using it with its default work and default output directory: `./hiq_backup.sh`
- Start the backup script with the following command for using it with an individual work and / or output directory: `./hiq_backup.sh -d <temporary directory> -w <output directory>`

```
./hiq_backup.sh -d /tmp/backup -w /software/backup
```

NOTICE:

To obtain detailed information about the start options of the backup script, enter the following command: `./hiq_backup.sh -?`

The backup script starts and looks for already available backup files. If the backup script finds available backup files, it displays these. This display is structured like the following example:

```
*** OLD Backups found ***

#ModifiedSize(MB)ActionFile Name

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

1Apr 10 22:056532Save/var/backup/
srx73_Bkup_Apr_10_2004_h22m05s11.tar

2Apr 07 10:116330Replace/var/backup/
srx73_Bkup_Apr_07_2004_h10m11s24.tar

3Mar 31 14:196612Delete/var/backup/
srx73_Bkup_Mar_31_2004_h14m19s13.tar

Choose handling of above backups:

1) Proceed with above actions

2) Keep all backups (don't delete any)

3) Select handling on per-file basis

4) Exit backup

Enter Option:
```

4) If the backup script finds available backup files, you need to define how to handle these:

- To use them for performing the actions suggested by the backup script in the previous output, enter: `1`

NOTICE:

The suggested actions always result from the following: The latest backup file is saved; the second latest backup

file is replaced with the new backup file; all other backup files are marked for deletion.

- To keep all detected backup files unchanged, enter: `2`
- To treat the detected backup files individually, enter: `3`
- To immediately stop the backup script without performing any modifications to the backup files, enter: `4`

If you have selected the individual treatment of the backup files (`Enter Option: 3`), the backup script asks for the treatment of the detected backup files. This display is structured like the following example:

```
Select backups to save, delete or replace:

#ModifiedSize(MB)File Name

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

1Apr 10 22:056532/var/backup/srx73_Bkup_Apr_10_
2004_h22m05s11.tar

Enter ’s’ to save, ’d’ to delete or ’r’ to replace:
```

5) If you have selected the individual treatment for the detected backup files (`Enter Option: 3`), you need to specify the treatment for each detected backup file.

a) Specify for the respectively displayed backup file how it is to be treated.

To keep the displayed backup file unchanged, enter: `s`

To delete the displayed backup file, enter: `d`

To replace the displayed backup file with the new one, enter: `r`

NOTICE:

You can select only one backup file for replacing it.

After you have defined the treatment for all detected backup files, the backup script shows a summary of the selected actions. This display is structured like the following example:

```
All backups have been handled

New backup handling will be:

#ModifiedSize(MB)ActionFile Name

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

1Apr 10 22:056532Save/var/backup/
srx73_Bkup_Apr_10_2004_h22m05s11.tar

2Apr 07 10:116330Save/var/backup/
srx73_Bkup_Apr_07_2004_h10m11s24.tar

3Mar 31 14:196612Save/var/backup/
srx73_Bkup_Mar_31_2004_h14m19s13.tar

Enter 'y' to proceed, 'n' to repeat Selection:
```

b) To execute the displayed actions, enter: `y`

NOTICE:

The backup script checks at this point whether the free disk space is sufficient for the new backup file. If the free disk space is not sufficient, you can use the `clear_backup` script to delete unnecessary patch set backup files.

---

6) The actual backup process starts.

The backup script puts out the following basic information about the current backup process:

```
Starting backup job...

Backup job (12937) has started in the background.

Completion could take from 30 min. to 3 hours,
depending

on whether the switch is busy.

- Monitor the lock file /lock/.backup_ended to
determine when backup completes.

- Check the log file /log/hiq_backup.sh_12826.log for
backup results.- If successful, backup output file
srx73_Bkup_Apr_12_

2004_h08m30s03.tar will be placed in /software/backup.
```

7) If you like to track the progress of the backup job, enter the following command:

```
/var/backup/hiq_backup.sh –s
```

The system shows the current percentage completed. This display is structured like the following example:

```
Checking backup status...

2%: Current size=77886 MBbackup status...

Estimated size=3526456 MBbackup status...
```

When the backup job is complete, the display has the following structure:

```
Checking backup status…

Last successful backup completed on Apr 12 12:20
```

8) Check, if the `.backup_ended` file exist in the `/lock/` directory.

NOTICE:

The backup script generates the `.backup_ended` file after finishing the backup job.

---

9) Switch to the `/log/` directory. In this directory look for the log file that was previously output by the backup script in the information about the current backup job and open it.

10) If no errors were logged in the log file, the new backup file can be archived via the backup concept of the external backup server.

11) If required, follow the described steps for the second computer system of the OpenScape Voice system also.

3.1.1.2 How to Restore the File System of a Single Node in a Redundant OpenScape Voice System

You can restore a single node of a redundant OpenScape Voice system after a severe system crash. In this process you restore the operating system as well

as the file system of the node. Furthermore, you reintegrate the relevant node in the redundancy concept of the OpenScape Voice system. The backup file required for this restoration may be stored on an external backup server.

Prerequisites

The other node of the redundant OpenScape Voice system still works trouble-free.

Access to the computer systems of both nodes of the redundant OpenScape Voice system.

root access to the computer system of the node to be restored

root access to the restoration script. If access is denied, change as user root in the `sshd_config` file the setting of the **PermitRootLogin** parameter to **yes**. Reboot the sshd-Daemon exclusively with the `/etc/init.d/sshd restart` command.

IMPORTANT:

This change can conflict with the security policy of the customer! How you reduce in that case the SSH ports used by the OpenScape Voice system describes the bulletin INF-09-000766– SSHD Interface Hardening.

The hardware of the OpenScape Voice node to be restored is operable and works trouble-free.

New hardware for the OpenScape Voice node to be restored must be identical with the one under which the backup file used in the following has been created. Exceptions are the harddisk drives; they may have a higher storage capacity.

NOTICE:

If you replace a harddisk drive in an OpenScape Voice node, you need to reconfigure the relevant SCSI-RAID controller. If you fail to do so, the operating system may not recognize the new harddisk drive and the file system cannot be restored.

The OSV DVD image ISO. We recommend to always use the currently available version.

A current backup file for the file system of the OpenScape Voice node to be restored.

Network connection to the external backup server on which the current backup file is stored

Name of the physical Ethernet interface via which the node to be restored accesses the network – e. g. eth0

IP address of the physical Ethernet interface via which the node to be restored accesses the network

IP address of the external backup server

If required, the user name under which the external backup server needs to be accessed (with associated password)

IP address of the router via which the external backup server can be reached

Complete path to the directory in which the backup file is stored on the external backup server

Name of the backup file

IMPORTANT:

If you execute the following steps, all data stored on the OpenScape Voice node to be restored will be deleted. Therefore, only perform the following steps if you own a current backup file for the node to be restored.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

Step by Step

1) Connect a keyboard and a monitor with the computer system of the node you want to restore.

2) Start the installation procedure as described in the OpenScape Voice V9, Service Manual: Installation and Upgrades, Installation Guide, section Installation Procedure until you are prompted to choose the service operation to use.

3) Select the `Restore` option.

4) Different backup sources are offered for selection. This display is structured like the following example:

```
Enter backup source:
1...FTP Server (ftp)
2...Secure FTP Server (sftp)
3...External USB hard disk drive
```

5) Depending on the protocol you want to use for accessing the external backup server:

- To access the external backup server via FTP, enter `1`.
- To access the external backup server via SFTP, enter `2`.

You are asked for the name of the backup file to be used for the restoration:

```
Enter Backup File Name []:
```

6) Specify under which complete path and name the backup file is stored on the backup server. Use the slash (/) as path separator.
`/backup/fsc301_Bkup_04_P_Apr_05_2004_h09m26s46_V4000.tar`

NOTICE:

The file system backup file names are standardized such that the hard disk of the OpenScape Voice server can be automatically initialized.

The initialization of the hard disk of the OpenScape Voice server is introduced by the following warning:

```
Result:

Initiating Step: Disk Setup...

*** WARNING ***

This will erase ALL PARTITIONS AND DATA on /dev/sda!

Proceed with create disk label? [y/n]

Enter 'y' to proceed.
```

7) Enter the following:

- `y`, to proceed with the restoration.
- `n`, to cancel the restoration.

If you proceed with the restoration, the initialization of the hard disk of the OpenScape Voice server will start. The corresponding output is structured like the following example:

```
Total disk space: 70006 MB

Creating partitions. Please wait...

.

.

.

Disk Setup Completed Successfully.
```

After the initialization has ended, the backup file will be retrieved automatically. To this, its file name and storage path are displayed for checking purposes in the following form:

```
Enter Backup File Name:

/backup/fsc301_Bkup_04_P_Apr_05_2004_h09m26s46_V4000.tar
```

8) Perform one of the following:

- Press the `Enter` key to confirm the information displayed.
- Enter the complete path and name under which the backup file is stored on the external backup server. Use the slash (/) as path separator.

You are asked if this is a VLAN configuration:

```
Is this a Vlan Configuration [y/n]?
```

9) Enter the name of the physical Ethernet interface via which the node to be restored accesses the network. The name `eth0` is used by default.

The script asks for the IP address of the physical Ethernet interface:

```
Enter Node's IP Address []:
```

10) Enter the IP address of the physical Ethernet interface.

The script asks for the network mask for the IP address:

```
Enter Node's NetMask []:
```

11) Enter the network mask.

The script asks you for the default gateway via which the external backup server can be reached:

```
Enter Node's Default Gateway []:
```

12) Enter the IP address of the router via which the external backup server can be reached.

The script asks you for the IP address of the external backup server.

13) Enter the IP address of the external backup server.

The script asks you for the user name under which the external backup server must be accessed.

14) Enter the user name under which the external backup server must be accessed.

The script asks you for the password that associates the entered user name.

15) Enter the password for the specified user name.

The restore script connects to the external backup server, copies the specified backup file to the OpenScape Voice node to be restored and

unpacks the files. The duration of this process depends mostly on the performance data of the network.

NOTICE:

The selected backup file is only copied and therefore still kept on the external backup server.

The script indicates in a progress display how it copies the backup file and extract files from there. This display is structured like the following example:

```
Connecting......

Transferring file. May take up to 30 minutes. Please
wait...

Progress.....................................................
.

Transfer finished!
```

The script continues with the progress display and reports how it restores the file system and installs the LILO boot loader. This display is structured like the following example:

```
Restoring file systems...

This may take a long time. Please wait...

Restoring File System "/mnt/home"...

File System "/mnt/home" restored...

Restoring File System "/mnt/opt"...

File System "/mnt/opt" restored...

Restoring File System "/mnt/root"...

File System "/mnt/root" restored...

Restoring File System "/mnt/unisphere"...

File System "/mnt/unisphere" restored...

Restoring File System "/mnt/var"...

File System "/mnt/var" restored...

Disk type and fstab file matched OK...

Restore Completed
```

This process may take up to 30 minutes.

```
Initiating Step: Make Disk Bootable...

Make Disk Bootable Completed Successfully

Exiting...
```

This process takes approximately 30 seconds.

16) Remove the USB stick in the case of a physical server or disconnect the ISO in the case of virtual server.

17) As user root, log on to the computer system to be restored. The node should be in state 4 at this time. Confirm the node state with the `srxqry` command. The “still running” partner node should be at state 4. The example given is truncated to save space

```
# srxqry
-- --- srxqry started on Sat Jul 14 16:42:31 2012 ---
-- OS : Linux-- Platform : x3550M3-- Cluster : bocast4
```

	Node Name	DB State	Op mode	Status
	--------	--------	-------	-------
Local Node	:bocast4a	Secondary active	Normal	Online at state 4
Remote Node	:bocast4b	Primary active	Normal	Online at state 4

18) With the file system restoration the license information of the system is restored, too. The license information is now in the state that was valid at the time when you created the backup file of the file system. If a more recent license file exists, import it in its latest version.

3.1.1.3 How to Restore the File System for all Nodes of an OpenScape Voice System

You can restore all nodes of an OpenScape Voice system after a severe system crash. In this process you restore the operating system as well as the file system of all nodes. The backup files required for this restoration may be stored on an external backup server. In a redundant OpenScape Voice system, both nodes can be restored successively or simultaneously.

Prerequisites

Local access to all computer systems of the OpenScape Voice system. In order to restore both nodes simultaneously in a redundant system, either one monitor and one keyboard per node are required or a KVM switch with one monitor and one keyboard.

root access to the restore script. If access is denied, change as user root in the `sshd_config` file the setting of the **PermitRootLogin** parameter to **yes**. Reboot the sshd-Daemon exclusively with the `/etc/init.d/sshd restart` command.

IMPORTANT:

This change can conflict with the security policy of the customer! How you reduce in that case the SSH ports used by the OpenScape Voice system describes the bulletin INF-09-000766– SSHD Interface Hardening.

The hardware of all OpenScape Voice nodes is operable and works trouble-free.

New hardware for the OpenScape Voice nodes must be identical with the one under which the backup files used here were created. Exceptions are the harddisk drives; they may have a higher storage capacity.

NOTICE:

If you replace a harddisk drive in an OpenScape Voice node, you need to reconfigure the relevant SCSI-RAID controller. If you fail to do so, the operating system may not recognize the new harddisk drive and the file system cannot be restored.

The OSV DVD image ISO. We recommend to always use the currently available version. In the case of a physical server, in order to restore both nodes simultaneously in a redundant system, two restore USBs are required.

A current backup file for each OpenScape Voice node

Network connection to the external backup server on which the current backup file is stored.

Name of the physical Ethernet interface via which the node to be restored accesses the network – e. g. eth0

IP address of the physical Ethernet interface via which the node to be restored accesses the network

IP address of the external backup server

If required, the user name under which the external backup server needs to be accessed (with associated password)

IP address of the router via which the external backup server can be reached

Complete paths of the directories in which the backup files are stored on the external backup server

Names of the backup files

IMPORTANT:

If you execute the following steps, all data stored on all nodes of the OpenScape Voice system will be deleted. Therefore, only perform the following steps if you own current backup files for the affected nodes.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

Step by Step

1) Connect a keyboard and a monitor to the computer system of node CE1.

2) Start the installation procedure as described in the OpenScape Voice V9, Service Manual: Installation and Upgrades, Installation Guide, section Installation Procedure until you are prompted to choose the service operation to use.

3) Select the `Restore` option.

4) Different backup sources are offered for selection. This display is structured like the following example:

```
Enter backup source:

1...FTP Server (ftp)

2...Secure FTP Server (sftp)

3...External USB hard disk drive
```

5) Depending on the protocol you want to use for accessing the external backup server:

- To access the external backup server via FTP, enter `1`.
- To access the external backup server via SFTP, enter `2`.

You are asked for the name of the backup file to be used for the restoration:

```
Enter Backup File Name []:
```

6) Specify under which complete path and name the backup file is stored on the backup server. Use the slash (/) as path separator.
`/backup/fsc301_Bkup_04_P_Apr_05_2004_h09m26s46_V4000.tar`

NOTICE:

The file system backup file names are standardized such that the hard disk of the OpenScape Voice server can be automatically initialized.

The initialization of the hard disk of the OpenScape Voice server is introduced by the following warning:

```
Result:

Initiating Step: Disk Setup...

***Warning***

This will erase ALL PARTITIONS AND DATA on /dev/sda!

Proceed with create disk label? [y/n]

Enter 'y' to proceed.
```

7) Enter the following:

- `y`, to proceed with the restoration.
- `n`, to cancel the restoration.

If you proceed with the restoration, the initialization of the hard disk of the OpenScape Voice server will start. The corresponding output is structured like the following example:

```
Total disk space: 70006 MB

Creating partitions. Please wait...

.

.

.

Disk Setup Completed Successfully.
```

After the initialization has ended, the backup file will be retrieved automatically. To this, its file name and storage path are displayed for checking purposes in the following form:

```
Enter Backup File Name:

/backup/fsc301_Bkup_04_P_Apr_05_2004_
h09m26s46_V4000.tar
```

8) Perform one of the following:

- Press the `Enter` key to confirm the information displayed.
- Enter the complete path and name under which the backup file is stored on the external backup server. Use the slash (/) as path separator.

You are asked if this is a VLAN configuration:

```
Is this a Vlan Configuration [y/n]?
```

9) Enter the name of the physical Ethernet interface via which the node to be restored accesses the network. The name `eth0` is used by default.

The script asks for the IP address of the physical Ethernet interface:

```
Enter Node's IP Address []:
```

10) Enter the IP address of the physical Ethernet interface.

The script asks for the network mask for the IP address:

```
Enter Node's NetMask []:
```

11) Enter the network mask.

The script asks you for the default gateway via which the external backup server can be reached:

```
Enter Node's Default Gateway []:
```

12) Enter the IP address of the router via which the external backup server can be reached.

NOTICE:

If you restore a redundant OpenScape Voice system, the Ethernet interface, the IP address, the network mask and

the gateway address for the redundant node are also queried.

The script asks you for the IP address of the external backup server.

13) Enter the IP address of the external backup server.

The script asks you for the user name under which the external backup server must be accessed.

14) Enter the user name under which the external backup server must be accessed.

The script asks you for the password that associates the entered user name.

15) Enter the password for the specified user name.

The restore script connects to the external backup server, copies the specified backup file to the OpenScape Voice node to be restored and

unpacks the files. The duration of this process depends mostly on the performance data of the network.

NOTICE:

The selected backup file is only copied and therefore still kept on the external backup server.

The script indicates in a progress display how it copies the backup file and extract files from there. This display is structured like the following example:

```
Connecting......

Transferring file. May take up to 30 minutes. Please
wait...

Progress.....................................................

Transfer finished!
```

The script continues with the progress display and reports how it restores the file system and installs the LILO boot loader. This display is structured like the following example:

```
Restoring file systems...

This may take a long time. Please wait...

Restoring File System "/mnt/home"...

File System "/mnt/home" restored...

Restoring File System "/mnt/opt"...

File System "/mnt/opt" restored...

Restoring File System "/mnt/root"...

File System "/mnt/root" restored...

Restoring File System "/mnt/unisphere"...

File System "/mnt/unisphere" restored...

Restoring File System "/mnt/var"...

File System "/mnt/var" restored...

Disk type and fstab file matched OK...

Restore Completed
```

This process may take up to 30 minutes.

```
Initiating Step: Make Disk Bootable...

Make Disk Bootable Completed Successfully

Exiting...
```

This process takes approximately 30 seconds.

16) Remove the USB sticks in the case of a physical servers or disconnect the ISO in the case of virtual servers.

17) Log on to every computer system to be restored as user `root`.

18) With the file system restore the system data of the systems is restored, too. The system data is now in the state that was valid at the time when you created the backup files of the file systems. If a more recent, independent database backup exists, use it to restore the database through the Common Management Platform now.

19) With the file system restore the license information of the systems is restored, too. The license information is now in the state that was valid at the time when you created the backup files of the file systems. If a more recent license file exists, import it in its latest version.

3.1.2 Backup & Restore with a USB Harddisk Drive

Backup files can be stored on an external USB harddisk drive (USB HDD). In this case the backup files need to be additionally stored on an independent second device – e. g. on a second USB harddisk drive, a backup server or a USB flash memory.

The second copy of the backup files should be created from an external computer system, with the system load and time being of no importance. This second copy of the backup files should be stored in a location different from the one that holds the first copy.

NOTICE: Even if USB flash memories appear attractive since they are cheap, please consider that the writing speed of many reasonable flash memories is often only 1 GB/hour. Such flash memories should not be used for the OpenScape Voice system.

3.1.2.1 How to Partition a USB Harddisk Drive

USB harddisk drives use in most cases an FAT32 file system that can manage only files not bigger than 4 GB. This file size is not sufficient for backing up some OpenScape Voice systems. An EXT3 file system must therefore be configured on the USB harddisk drive, if this drive is to be used for backing up an OpenScape Voice system.

Prerequisites

A computer system with a Suse-Linux operating system.

IMPORTANT:

If you use the computer system of an OpenScape Voice system for the following steps, execute them at a time of low system load. This minimizes the effect the partitioning process has on the OpenScape Voice services.

Adequate administrative permissions

IMPORTANT:

Execute the following steps to delete all data stored on the USB harddisk drive.

Step by Step

1) Log on to the computer system as user `root`.

2) Connect the inactive USB harddisk drive to the computer system and switch it on.

The operating system detects the USB harddisk drive after approximately 15 seconds and can access it.

3) Use the following command to have all available drives displayed:`fdisk -1`

The operating system displays information about the available drives. This display is structured like the following example:

```
Device NameStartEndBlocksIdSystem
/dev/sda111024209713682Linux swap
/dev/sda210252048209715282Linux swap
/dev/sda320493584314572883Linux
/dev/sda4358535003643461125Extended
/dev/sda53585563241942883Linux
/dev/sda65633588251198483Linux
/dev/sda758837930419428883Linux
/dev/sda879318954209713683Linux
/dev/sda9895514074104857 4483Linux
/dev/sda10140751663452428 6483Linux
/dev/sda11166351817031457 1283Linux
/dev/sda12181712329010485 74483Linux
/dev/sda13232912533841942 8883Linux
/dev/sda14253392636220971 3683Linux
/dev/sda15263633500317696 75283Linux

Disk/dev/sdb: 160.0 GB, 160041885696 bytes
255 heads, 63 sectors/track, 19457 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device BootStartEndBlocksIdSystem
/dev/sdb11194571562883217FAT3
```

In this example the first drive (`/dev/sda`) is the system drive. The second drive (`/dev/sdb`) is an external USB harddisk drive with 160 GB memory. The operating system is likely to recognize your USB harddisk drive under a different description– e. g. under `/dev/sdc` or `/dev/sdd`. Use the individual desciption of your USB harddisk drive.

4) User the following command to display the information of your USB harddisk drive:`fdisk dev/sdb`

The operating system displays the information of your USB harddisk drive. This display is structured like the following example:

```
The number of cylinders for this disk is set to 19457.
There is nothing wrong with that, but this is larger
than 1024, and could in certain setups cause problems
with:

1) software that runs at boot time (e.g., old versions

of LILO)

2) booting and partitioning software from other OSs

(e.g., DOS FDISK, OS/2 FDISK)
```

5) Use the following command to have the partition table of your USB harddisk drive displayed:`Command (m for help):p`

The operating system displays the partition table of your USB harddisk drive. This display is structured like the following example:

```
Disk/dev/sdb: 160.0 GB, 160041885696 bytes

255 heads, 63 sectors/track, 19457 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes


Device BootStartEndBlocksIdSystem

/dev/sdb111945715628832 17FAT32
```

Up to two partitions can be displayed for your USB harddisk drive. In the example only one partition is available.

6) Check with which file system the partitions have been configured.

- If `Linux` has already been specified under `System`, your USB harddisk drive uses the correct file system. In this case you need not execute the following steps of this chapter.
- If `Linux` is not specified as `System`, continue with the following steps.

7) Use the following command to delete all partitions of your USB harddisk drive:`Command (m for help):d`

8) Use the following command to check whether all partitions of your USB harddisk drive were deleted:`Command (m for help):p`

If all partitions of your USB harddisk drive are deleted, the partition table of your USB harddisk drive is empty. This display is then structured like the following example:

```
Disk/dev/sdb: 160.0 GB, 160041885696 bytes

255 heads, 63 sectors/track, 19457 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes Device


BootStartEndBlocksIdSystem
```

9) Use the following commands to create primary partition on your USB harddisk drive:

a) `Command (m for help):n`
`Command action`

`eextended`

`pprimary partition`

b) `P`

c) `Partition number (1-4): 1`

`First cylinder (1-19457, default 1):`

`Using default value 1`

`Last cylinder or +size or +sizeM or`

`+sizeK (1-19457, default 19457):`

`Using default value 19457`

In the given example a primary partition is created with number 1. The default values are copied for the first and last cylinder.

10) Use the following command to verify that the primary partition was created:`Command (m for help):p`

The operating system shows the primary partition in the partition table for your USB harddisk drive. This display is structured like the following example:

```
Disk/dev/sdb: 160.0 GB, 160041885696 bytes
255 heads, 63 sectors/track, 19457 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device BootStartEndBlocksIdSystem
/dev/sdb11194571562883217Linux
```

11) Use the following command to write the new primary partition on your USB harddisk drive:`Command (m for help):w`

12) User the following command to display the new primary partition of your USB harddisk drive: `fdisk -1`

The operating system displays information about the available drives. This display is structured like the following example:

```
Disk /dev/sda: 73.4 GB, 73406611456 bytes
128 heads, 32 sectors/track, 35003 cylinders
Units = cylinders of 4096 * 512 = 2097152 bytes

Device NameStartEndBlocksIdSystem
/dev/sda111024209713682Linux swap
/dev/sda210252048209715282Linux swap
/dev/sda320493584314572883Linux
/dev/sda4358535003643461125Extended
/dev/sda535855632419428883Linux
/dev/sda65633588251198483Linux
/dev/sda758837930419428883Linux
/dev/sda879318954209713683Linux
/dev/sda9895514074104857 4483Linux
/dev/sda10140751663452428 6483Linux
/dev/sda11166351817031457 1283Linux
/dev/sda12181712329010485 74483Linux
/dev/sda13232912533841942 8883Linux
/dev/sda14253392636220971 3683Linux
/dev/sda15263633500317696 75283Linux

Disk/dev/sdb: 160.0 GB, 160041885696 bytes
255 heads, 63 sectors/track, 19457 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes Device

BootStartEndBlocksIdSystem
/dev/sdb11194571562883217Linux
```

13) Use the following command to format the new primary partition of your USB harddisk drive:`mkfs.ext3 /dev/sdb1`

The operating system shows the formatting information. This display is structured like the following example:

```
mke2fs 1.36 (05-Feb-2009)

Filesystem label= OS type: Linux

Block size=4096 (log=2)

Fragment size=4096 (log=2)

19546112 inodes, 39072080 blocks

1953604 blocks (5.00%) reserved for the super user

First data block=0 1193 block groups

32768 blocks per group,

32768 fragments per group

16384 inodes per group

Superblock backups stored on blocks: 32768, 98304,
163840, 229376, 294912, 819200, 884736, 1605632,
2654208, 4096000, 7962624, 11239424, 20480000, 23887872

Writing inode tables: 0/1193 ...

Creating journal (8192 blocks): done

Writing superblocks and filesystem accounting
information: done

This filesystem will be automatically checked every 23
mounts or 180 days, whichever comes first. Use tune2fs
-c or -i to override.
```

14) Check the new file system of your USB harddisk drive with the following commands:

a) `mkdir -m 777 /usb`
b) `mount /dev/sdb1 /usb`
c) `df -k /dev/sdb1`

The operating system displays the information of the new file system. This display is structured like the following example:

```
Filesystem1K-blocksUsedAvailableUse%Mounted on

/dev/sdb1153834852328281459876081%/usb
```

15) Unmount the USB harddisk drive with the following command:`umount /usb`

16) Separate the USB harddisk drive from the computer system.

3.1.2.2 How to Back Up a File System on a USB Harddisk Drive

To back up the file system of an OpenScape Voice system on a USB harddisk drive, you need to back up the file system of the single node in case of a single-node system. In case of a redundant system, back up the file system of each

single node. Use in both cases the backup script shipped with the OpenScape Voice system.

Prerequisites

Root access for the backup script. If access is denied, as user root, change the setting of the PermitRootLogin parameter to **yes** in file the `sshd_config`. Reboot the sshd-Daemon exclusively with command: `init.d/sshd restart`

IMPORTANT:

This change can conflict with the security policy of the customer! How you reduce in that case the SSH ports used by the OpenScape Voice system describes the bulletin INF-09-000766– SSHD Interface Hardening.

No rolling upgrades, patch activities or configuration modifications are performed in the OpenScape Voice system.

The CPU load of the computer system to be backed up amounts to a maximum of 50 %.

The local harddisk drives of the computer system to be backed up offer sufficient memory for the additional backup files. The backup script checks this requirement immediately after the start.

IMPORTANT:

The backup script only secures the following required partitions of an OpenScape Voice computer system: `/`, `/unisphere/`, `/home/`, `/opt/`, `/enterprise/` and `/var/`.

NOTICE:

So that the backup script and the following commands can be executed, you need to log on to the computer system to be backed up as root user. If you want to back up a computer system remotely, you need to log on as sysad user first, and then switch to the root user with the `su -root` command.

Step by Step

1) On the CE1 computer system of the OpenScape Voice system log on as user `root`.

2) Use the following command to switch to the `var/backup` directory on the computer system: `cd /var/backup`

3) Start the backup script:

- Start the backup script with the following command for using it with its default work and default output directory: `./hiq_backup.sh`
- Start the backup script with the following command for using it with an individual work and / or output directory: `./hiq_backup.sh -d <temporary directory> -w <output directory>`

```
./hiq_backup.sh -d /tmp/backup -w /software/backup
```

NOTICE:

To obtain detailed information about the start options of the backup script, enter the following command: `./hiq_backup.sh -?`

The backup script starts and looks for already available backup files. If the backup script finds available backup files, it displays these. This display is structured like the following example:

```
*** OLD Backups found ***

#ModifiedSize(MB)ActionFile Name

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

1Apr 10 22:056532Save/var/backup/
srx73_Bkup_Apr_10_2004_h22m05s11.tar

2Apr 07 10:116330Replace/var/backup/
srx73_Bkup_Apr_07_2004_h10m11s24.tar

3Mar 31 14:196612Delete/var/backup/
srx73_Bkup_Mar_31_2004_h14m19s13.tar

Choose handling of above backups:

1) Proceed with above actions

2) Keep all backups (don't delete any)

3) Select handling on per-file basis

4) Exit backup

Enter Option:
```

4) If the backup script finds available backup files, you need to define how to handle these:

- To use them for performing the actions suggested by the backup script in the previous output, enter: `1`

NOTICE:

The suggested actions always result from the following: The latest backup file is saved; the second latest backup

file is replaced with the new backup file; all other backup files are marked for deletion.

- To keep all detected backup files unchanged, enter: `2`
- To treat the detected backup files individually, enter: `3`
- To immediately stop the backup script without performing any modifications to the backup files, enter: `4`

If you have selected the individual handling of the backup files (`Enter Option: 3`), the backup script asks for the handling of the detected backup files. This display is structured like the following example:

```
Select backups to save, delete or replace:

#ModifiedSize(MB)File Name

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

1Apr 10 22:056532/var/backup/srx73_Bkup_Apr_10_
2004_h22m05s11.tar

Enter ’s’ to save, ’d’ to delete or ’r’ to replace:
```

5) If you have selected the individual treatment for the detected backup files (`Enter Option: 3`), you need to specify the treatment for each detected backup file.

a) Specify for the respectively displayed backup file how it is to be treated.

To keep the displayed backup file unchanged, enter: `s`

To delete the displayed backup file, enter: `d`

To replace the displayed backup file with the new one, enter: `r`

> **NOTICE:**
>
> You can select the **r** option always for only one of the detected backup files.

After you have defined the treatment for all detected backup files, the backup script shows a summary of the selected actions. This display is structured like the following example:

```
All backups have been handled

New backup handling will be:

#ModifiedSize(MB)ActionFile Name

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

1Apr 10 22:056532Save/var/backup/
srx73_Bkup_Apr_10_2004_h22m05s11.tar

2Apr 07 10:116330Save/var/backup/
srx73_Bkup_Apr_07_2004_h10m11s24.tar

3Mar 31 14:196612Save/var/backup/
srx73_Bkup_Mar_31_2004_h14m19s13.tar

Enter 'y' to proceed, 'n' to repeat Selection:
```

b) To execute the displayed actions, enter: `y`

> **NOTICE:**
>
> The backup script checks at this point whether the free disk space is sufficient for the new backup file. If the free disk space is not sufficient, you can use the `clear_backup` script to delete unnecessary patch set backup files.

6) The actual backup process starts.

The backup script puts out the following basic information about the current backup process:

```
Starting backup job...

Backup job (12937) has started in the background.

Completion could take from 30 min. to 3 hours,
depending

on whether the switch is busy.

- Monitor the lock file /lock/.backup_ended to
determine when backup completes.

- Check the log file /log/hiq_backup.sh_12826.log for
backup results.- If successful, backup output file
srx73_Bkup_Apr_12_

2004_h08m30s03.tar will be placed in /software/backup.
```

7) To track the progress of the backup job, enter the following command:

```
/var/backup/hiq_backup.sh –s
```

If the backup job has not been completed yet, the current job progress is displayed. This display is structured like the following example:

```
Backup will complete before Estimated Full Size due to
compression.

Merging dump root.bk to tar file, the estimate will be
inaccurate.

11%: Current Size= 716 MB Estimated Full Size=6486 MB
```

When the backup job is complete, the display has the following structure:

```
Checking backup status…

Last successful backup completed on Apr 12 12:20
```

8) Check, if the `.backup_ended` file exists in the `/lock/` directory.

NOTICE:

The backup script generates the `.backup_ended` file after finishing the backup job.

---

9) Switch to the `/log/` directory. In this directory look for the log file that was previously output by the backup script in the information about the current backup job and open it.

10) If no errors have been logged in the log file, connect the deactivated USB harddisk drive to the computer system and switch it on again.

11) Start the backup script to copy the new backup file with the following command:

```
cd /var/backup./hiq_backup_exthdd.sh -fs
```

The script shows a list of the SCSI partitions available on the computer system. The system partitions `/dev/sda` on which the OpenScape Voice

system is installed is not displayed. This display is structured like the following example:

```
The following ext2/ext3 Linux partitions were found

1) /dev/sdb2 (avail space: 15G) Linux
2) /dev/sdb5 (avail space: 7.0M) Linux
3) /dev/sdb6 (avail space: 6.2M) Linux
4) /dev/sdb7 (avail space: 18G) Linux

Please choose the partition to copy the backup file to
(press q to quit):
```

12) Enter the number of the partition to which you want to copy the new backup file.

The script shows a list of all file system backup files that are stored in the following directories: `/var/backup/`, `/software/backup/`. This display is structured like the following example:

```
The following backup files are available on the system

1) grd15a_Bkup_Jul_11_2005_h09m03s12.tar (1.6G)
2) grd15a_Bkup_Jul_13_2005_h16m43s39.tar (1.6G)
3) grd15a_Bkup_Jul_14_2005_h11m20s28.tar (1.7G)

Please choose backup file to be transferred to external
USB Device(press q to quit):
```

13) Enter the number of the backup file that you want to copy.

The script checks whether the free memory on the selected partition is sufficient for copying the selected backup file. If there is sufficient space, the script copies the selected backup file to the following folder: `/backup/<cluster name>/<node name>/`

NOTICE:

The selected backup file is only copied and therefore still kept on the computer system of OpenScape Voice.

The script indicates in a progress display how it copies the backup file. This display is structured like the following example:

```
Checking for available space on '/dev/ sdb2'...OK

Making directory 'backup/GRD15S/grd15a' on '/mnt/
exthdd12667'...OK

Transferring backup file to external USB Device...OK

Syncing '/mnt/exthdd12667'please wait...OK

Unmounting '/mnt/exthdd12667'...OK

Removing directory '/mnt/ exthdd12667'...OK

Transfer of backup file to external USB Device finished
successfully.
```

14) Separate the USB harddisk drive from the computer system.
15) If required, follow the described steps for the second computer system of the OpenScape Voice system also.

3.1.2.3 How to Restore the File System of a Single Node in a Redundant OpenScape Voice System

You can restore a single node of a redundant OpenScape Voice system after a severe system crash. In this process you restore the operating system as well as the file system of the node. Furthermore, you reintegrate the relevant node in the redundancy concept of the OpenScape Voice system. The backup file required for this restoration may be stored on a USB harddisk drive.

Prerequisites

The other node of the redundant OpenScape Voice system still works trouble-free.

Access to the computer systems of both nodes of the redundant OpenScape Voice system.

root access to the computer system of the node to be restored

root access to the restoration script. If access is denied, change as user root in the `sshd_config` file the setting of the **PermitRootLogin** parameter to **yes**. Reboot the sshd-Daemon exclusively with the `/etc/init.d/sshd restart` command.

IMPORTANT:

This change can conflict with the security policy of the customer! How you reduce in that case the SSH ports used by the OpenScape Voice system describes the bulletin INF-09-000766– SSHD Interface Hardening.

The hardware of the OpenScape Voice node to be restored is operable and works trouble-free.

New hardware for the OpenScape Voice node to be restored must be identical with the one under which the backup file used in the following has been created. Exceptions are the harddisk drives; they may have a higher storage capacity.

NOTICE:

If you replace a harddisk drive in an OpenScape Voice node, you need to reconfigure the relevant SCSI-RAID controller. If you fail to do so, the operating system may not recognize the new harddisk drive and the file system cannot be restored.

The OSV installation and restoration DVD image ISO. We recommend to always use the currently available version.

A current backup file for the file system of the OpenScape Voice node to be restored.

If you use a backup file that was created via the Common Management Platform, rename the backup file as follows: Change `FileSysBackup` in the file name to `Bkup`.

USB harddisk drive on which the current backup file is stored

Name of the partition under which the backup file is stored on the USB harddisk drive

Name of the backup file

Cluster and node name of the OpenScape Voice node to be restored

---

IMPORTANT:

If you execute the following steps, all data stored on the OpenScape Voice node to be restored will be deleted. Therefore, only perform the following steps if you own a current backup file for the node to be restored.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

NOTICE:

The restore scripts used in the following recognize EXT2 / EXT3, NTFS and FAT32 partitions of a USD harddisk drive. For a FAT32 partition, the backup file size is limited to 4 GB less 1 byte. The following description assumes EXT2 / EXT3 partitions.

Step by Step

1) Connect a keyboard and a monitor with the computer system of the node you want to restore.

2) Connect the inactive USB harddisk drive to the computer system and switch it on.

3) Place the OSV DVD in the computer system's drive or run the OSV DVD image ISO from the node.

4) Reboot the computer system.

The following startup options are available:

```
Boot from Hard Disk

Restore Softswitch – Vx.y
```

5) Select the `Restore Softswitch – Vx.y` option.

The computer system starts up in the rescue mode and asks in the following way for the login to be used:

```
Rescue login:
```

6) Enter `root`.

Different backup sources are offered for selection. This display is structured like the following example:

```
Enter backup source:

1...FTP Server (ftp)

2...Secure FTP Server (sftp)

3...External USB hard disk drive
```

7) Enter `3`.

The script shows a list of the SCSI partitions available on the computer system. The system partitions `/dev/sda` on which the OpenScape Voice system is installed is not displayed. This display is structured like the following example:

```
The following ext2/ext3 Linux partitions were found

1) /dev/sdb2 (avail space: 19G) Linux

2) /dev/sdb5 (avail space: 7.4M) Linux

3) /dev/sdb6 (avail space: 7.6M) Linux

4) /dev/sdb7 (avail space: 19G) Linux

Please choose partition containing the backup file
(press q to quit):
```

8) Enter the number of the partition on which the backup file is stored.

The script asks you for the name of the directory in which the backup file is stored on the selected partition: This query is structured like the following example:

```
Provide the path of the directory containing the backup
file(s) on '/dev/sdb2' (i.e. /backup/cluster_name/
node_name)
```

9) Specify the name of the directory in which the backup file of the selected partition is stored. This directory must have the following format: .

```
/backup/<cluster name>/<node name>/
```

NOTICE: You can open an additional shell to determine the directory name on the USB harddisk drive.

NOTICE:

The computer system was booted from the OSV DVD image ISO. Therefore, the restore script can automatically

detect neither the cluster name nor the node name of the node to be restored.

The script shows a list of all file system backup files stored in the indicated directory. This display is structured like the following example:

```
Directory 'backup/GRD15S/grd15a' on '/dev/sdb2'
contains the following backup files

1) grd15a_Bkup_04_P_Jul_11_2005_h12m34s29.tar (1.6G)
2) grd15a_Bkup_04_P_Jul_14_2005_h16m43s39.tar (1.7G)
3) grd15a_Bkup_04_P_Jul_18_2005_h11m20s28.tar (1.6G)

Please choose backup file to be retrieved (press q to
quit):
```

10) Enter the number of the backup file that you want to use for the restoration.

The initialization of the hard disk of the OpenScape Voice server is introduced by the following warning:

```
Result:
Initiating Step: Disk Setup...
***Warning***
This will erase ALL PARTITIONS AND DATA on /dev/sda!
Proceed with create disk label? [y/n]

Enter ’y’ to proceed.
```

11) Enter the following:

- `y`, to proceed with the restoration.
- `n`, to cancel the restoration.

If you proceed with the restoration, the initialization of the hard disk of the OpenScape Voice server will start. The corresponding output is structured like the following example:

```
Total disk space: 70006 MB

Creating partitions. Please wait...

.

.

.

Disk Setup Completed Successfully.
```

The script copies the selected backup file to a temporary memory area of the OpenScape Voice node and unpacks the files from there. This process takes approximately 5 minutes.

NOTICE:

The selected backup file is only copied and therefore still kept on the USB harddisk drive.

The script indicates in a progress display how it copies the backup file and extract files from there. This display is structured like the following example:

```
Retrieving backup file 'grd15a_Bkup_04_P_Jul_11_2005_
h12m34s29.tar' from '/tmp/mnt/exthdd1719/backup/GRD15S/
grd15a', please wait...OK

Unmounting '/tmp/mnt/exthdd1719'...OK

Removing directory '/tmp/mnt/USB/exthdd1719'...OK

Extracting individual backup files...
```

12) As soon as the script starts to extract files from the backup file, separate the USB harddisk drive from the computer system.

After extracting the files, the script displays how it restores the file system and installs the LILO boot loader. This display is structured like the following example:

```
Restoring file systems...
This may take a long time. Please wait...
Restoring File System "/mnt/home"...
File System "/mnt/home" restored...
Restoring File System "/mnt/opt"...
File System "/mnt/opt" restored...
Restoring File System "/mnt/root"...
File System "/mnt/root" restored...
Restoring File System "/mnt/unisphere"...
File System "/mnt/unisphere" restored...
Restoring File System "/mnt/var"...
File System "/mnt/var" restored...
Disk type and fstab file matched OK...
Restore Completed
```

This process may take up to 30 minutes.

```
Initiating Step: Make Disk Bootable...
Make Disk Bootable Completed Successfully
Exiting...
```

This process takes approximately 30 seconds.

13) Restart the computer system with the following command: `reboot`

The computer system reboots. If the OSV DVD had been placed in the computer system's drive, it will be automatically unmounted.

The computer system generally comes up to state 3.

14) When the processing ends, log on to the computer system to be restored as superuser (e.g., user `root`).

15) Remove the OSV DVD from the computer system’s drive, if applicable.

16) Switch to state 3 with the following command (in case the system is not yet in state 3):

```
~srx/startup/srxctrl 3 0
```

17) Replace the `srxBootParams` file with the following commands:

a) `cd /unisphere/srx3000/srx/startup`

b) `rm srxBootParams`

c) `mv srxBootParams.orig srxBootParams`

18) Connect to the database of the node to be restored. To this, execute on the correctly operating node of the redundant OpenScape Voice system the following command: /opt/solid/bin/solsql "tcpip 16760" dba dba

19) Check the status of the node to be restored. To this, execute on the correctly operating node of the redundant OpenScape Voice system the following command:

```
ADMIN COMMAND 'hsb state';
```

20) Depending on the state of the node to be restored, perform one of the following steps:

- Status is `PRIMARY ACTIVE`:

  Leave the database with the following command:

  ```
  exit;
  ```

- Status is `PRIMARY ALONE`:

  Execute the following commands:

  ```
  ADMIN COMMAND `hsb netcopy';
  ```

  ```
  ADMIN COMMAND `hsb connect';
  ```

  ```
  exit;
  ```

21) Switch to the computer system of the node that you want to restore.

22) Switch to the following directory:

```
cd /unisphere/srx3000/srx/startup
```

23) Switch to state 4 with the following command: `./srxctrl 4 0`

24) With the file system restoration the license information of the system is restored, too. The license information is now in the state that was valid at the time when you created the backup file of the file system. If a more recent license file exists, import it in its latest version.

3.1.2.4 How to Restore a File System for all Nodes of an OpenScape Voice System

You can restore all nodes of an OpenScape Voice system after a severe system crash. In this process you restore the operating system as well as the file system of all nodes. The backup files required for this restoration may be stored on a USB harddisk drive. In a redundant OpenScape Voice system, both nodes can be restored successively or simultaneously.

Prerequisites

Local access to all computer systems of the OpenScape Voice system. In order to restore both nodes simultaneously in a redundant system, either one monitor and one keyboard per node are required or a KVM switch with one monitor and one keyboard.

Root access to the restoration script. If access is denied, change as user root in the `sshd_config` file the setting of the **PermitRootLogin** parameter to **yes**. Reboot the sshd-Daemon exclusively with the `/etc/init.d/sshd restart` command.

IMPORTANT:

This change can conflict with the security policy of the customer! How you reduce in that case the SSH ports used by the OpenScape Voice system describes the bulletin INF-09-000766– SSHD Interface Hardening.

The hardware of all OpenScape Voice nodes is operable and works trouble-free.

New hardware for the OpenScape Voice nodes must be identical with the one under which the backup files used here were created. Exceptions are the harddisk drives; they may have a higher storage capacity.

NOTICE:

If you replace a harddisk drive in an OpenScape Voice node, you need to reconfigure the relevant SCSI-RAID controller. If you fail to do so, the operating system may not recognize the new harddisk drive and the file system cannot be restored.

The OSV installation and restoration DVD image ISO. We recommend to always use the currently available version. In order to restore both nodes simultaneously in a redundant system, two OSV DVD images are required.

A current backup file for each OpenScape Voice node

If you use a backup file that was created via the Common Management Platform, rename the backup file as follows: Change `FileSysBackup` in the file name to `Bkup`.

USB harddisk drive on which the current backup files are stored

Name of the partition under which the backup files are stored on the USB harddisk drive

Names of the backup files

Cluster and node name of the OpenScape Voice nodes

IMPORTANT:

If you execute the following steps, all data stored on all nodes of the OpenScape Voice system will be deleted. Therefore, only perform the following steps if you own current backup files for the affected nodes.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

NOTICE:

The restore scripts used in the following recognize EXT2 / EXT3, NTFS and FAT32 partitions of a USD harddisk drive. For a

FAT32 partition, the backup file size is limited to 4 GB less 1 byte. The following description assumes EXT2 / EXT3 partitions.

Step by Step

1) Connect a keyboard and a monitor with the computer system of the node you want to restore.

2) Connect the inactive USB harddisk drive to the computer system and switch it on.

3) Place the OSV DVD in the computer system's drive or run the OSV DVD image ISO from the node.

4) Reboot the computer system.

The following startup options are available:

```
Boot from Hard Disk
```

```
Restore Softswitch – Vx.y
```

5) Select the `Restore Softswitch – Vx.y` option.

The computer system starts up in the rescue mode and asks in the following way for the login to be used:

```
Rescue login:
```

6) Enter `root`.

Different backup sources are offered for selection. This display is structured like the following example:

```
Enter backup source:
```

```
1...FTP Server (ftp)
```

```
2...Secure FTP Server (sftp)
```

```
3...External USB hard disk drive
```

7) Enter `3`.

The script shows a list of the SCSI partitions available on the computer system. The system partitions `/dev/sda` on which the OpenScape Voice system is installed is not displayed. This display is structured like the following example:

```
The following ext2/ext3 Linux partitions were found
```

```
1) /dev/sdb2 (avail space: 19G) Linux
```

```
2) /dev/sdb5 (avail space: 7.4M) Linux
```

```
3) /dev/sdb6 (avail space: 7.6M) Linux
```

```
4) /dev/sdb7 (avail space: 19G) Linux
```

```
Please choose partition containing the backup file
(press q to quit):
```

8) Enter the number of the partition on which the backup file is stored.

The script asks you for the name of the directory in which the backup file is stored on the selected partition: This query is structured like the following example:

```
Provide the path of the directory containing the backup
file(s) on '/dev/sdb2' (i.e. /backup/cluster_name/
node_name)
```

9) Specify the name of the directory in which the backup file of the selected partition is stored. This directory must have the following format:

`/backup/<cluster name>/<node name>/.`

NOTICE: You can open an additional shell to determine the directory name on the USB harddisk drive.

NOTICE:

The computer system was booted from the OSV DVD image ISO. Therefore, the restore script can automatically detect neither the cluster name nor the node name of the node to be restored.

The script shows a list of all file system backup files stored in the indicated directory. This display is structured like the following example:

```
Directory 'backup/GRD15S/grd15a' on '/dev/sdb2'
contains the following backup files

1) grd15a_Bkup_04_P_Jul_11_2005_h12m34s29.tar (1.6G)
2) grd15a_Bkup_04_P_Jul_14_2005_h16m43s39.tar (1.7G)
3) grd15a_Bkup_04_P_Jul_18_2005_h11m20s28.tar (1.6G)

Please choose backup file to be retrieved (press q to
quit):
```

10) Enter the number of the backup file that you want to use for the restoration.

The initialization of the hard disk of the OpenScape Voice server is introduced by the following warning:

```
Result:
Initiating Step: Disk Setup...
***Warning***
This will erase ALL PARTITIONS AND DATA on /dev/sda!
Proceed with create disk label? [y/n]

Enter ’y’ to proceed.
```

11) Enter the following:

- `y`, to proceed with the restoration.
- `n`, to cancel the restoration.

If you proceed with the restoration, the initialization of the hard disk of the OpenScape Voice server will start. The corresponding output is structured like the following example:

```
Total disk space: 70006 MB

Creating partitions. Please wait...

.

.

.

Disk Setup Completed Successfully.
```

The script copies the selected backup file to a temporary memory area of the OpenScape Voice node and unpacks the files from there. This process takes approximately 5 minutes.

NOTICE:

The selected backup file is only copied and therefore still kept on the USB harddisk drive.

The script indicates in a progress display how it copies the backup file and extract files from there. This display is structured like the following example:

```
Retrieving backup file 'grd15a_Bkup_04_P_Jul_11_2005_
h12m34s29.tar' from '/tmp/mnt/exthdd1719//backup/
GRD15S/ grd15a', please wait...OK

Unmounting '/tmp/mnt/USB/exthdd1719'...OK

Removing directory '/tmp/mnt/USB/exthdd1719'...OK

Extracting individual backup files...
```

12) As soon as the script starts to extract files from the backup file, separate the USB harddisk drive from the computer system.

After extracting the files, the script displays how it restores the file system and installs the LILO boot loader. This display is structured like the following example:

```
Restoring file systems...
This may take a long time. Please wait...
Restoring File System "/mnt/home"...
File System "/mnt/home" restored...
Restoring File System "/mnt/opt"...
File System "/mnt/opt" restored...
Restoring File System "/mnt/root"...
File System "/mnt/root" restored...
Restoring File System "/mnt/unisphere"...
File System "/mnt/unisphere" restored...
Restoring File System "/mnt/var"...
File System "/mnt/var" restored...
Disk type and fstab file matched OK...
Restore Completed
```

This process may take up to 30 minutes.

```
Initiating Step: Make Disk Bootable...
Make Disk Bootable Completed Successfully
Exiting...
```

This process takes approximately 30 seconds.

13) Restart the computer system with the following command: `reboot`

The computer system reboots. If the OSV DVD had been placed in the computer system's drive, it will be automatically unmounted.

The computer system generally comes up to state 3.

14) If you are restoring a redundant OpenScape Voice system, wait 30 seconds and then execute the same steps described so far for node CE2.

15) When the processing ends, log on to the computer system to be restored as superuser (e.g., user `root`).

16) Remove the OSV DVD from the computer system’s drive, if applicable.

17) Switch to state 3 with the following command (in case the system is not yet in state 3):

- In a non-redundant OpenScape Voice system:

  `~srx/startup/srxctrl 3 0`
- In a redundant OpenScape Voice system:

  `~srx/startup/srxctrl 3 3`

18) Log on to every computer system to be restored as user `superuser`.

19) On every computer system to be restored replace the `srxBootParams` file with the following commands:

a) `cd /unisphere/srx3000/srx/startup`

b) `rm srxBootParams`

c) `mv srxBootParams.orig srxBootParams`

20) With the file system restoration the system data of the systems is restored, too. The system data is now in the state that was valid at the time when you created the backup files of the file systems. If a more recent, independent database backup exists, use it to restore the database through the Common Management Platform now.

21) Switch to the following directory on one of the computer systems to be restored:

`cd /unisphere/srx3000/srx/startup`

22) Switch to state 4 with one of the following commands:

- In a non-redundant OpenScape Voice system: `./srxctrl 4 0`
- In a redundant OpenScape Voice system: `./srxctrl 4 4`

23) With the file system restoration the license information of the systems is restored, too. The license information is now in the state that was valid at the time when you created the backup files of the file systems. If a more recent license file exists, import it in its latest version.

3.1.3 Backup and Restore Via the CMP

You can use the Common Management Platform manually or automatically back up the database and thus the configuration and data of the OpenScape system. From the information backed up in this way you can restore the database of an OpenScape system. This concerns a single- as well as multi-node installation.

The backup and restore concept by the Common Management Platform is based on the following elements:

- Backup sets
- Archives
- Backup schedules
- Backup & restore jobs

Backup sets

A backup set contains all information that was saved for the OpenScape system during a backup run.

System configurations and system data (backup units) can be backed up in a backup set and we distinguish two types of backup units.

- System

  Backup units that contain entire file systems.
- Data

  Backup units that contain configuration data.

Each backup set may only contain backup units of a single type and is saved in an archive.

The list of offered backup units depends on the type and number of installed applications. The following backup units may be available:

- **OpenScape Voice**
- **OpenScape Branch**
- **Application Server** (OpenScape UC Application)

  The following subordinate backup units are available for this backup unit. You can select them individually by clicking on the name of the **Application Server** backup unit.

- – **Audit Log Files**

  Backs up the log information of the audit log.
  – **Backup & Restore Service**

  Backs up the database for backup & restore.
  – **Cmp Syslog Audit**

  Backs up the configuration file for logging via Syslog. This comprises the host ID, audit status and the actual Syslog configuration.
  – **Conferencing Applets Service**

  Backs up the media-server-related files and the configuration file of the conference portal.
  – **Conferencing Service**

  Backs up the conference database and the configuration file of the conference service.
  – **Container Configuration Files**

  Backs up the configuration entries that concern the single OpenScape services.
  – **Deployment Service**

  Backs up the database information and the configuration file of the deplioyment service.
  – **Domain and License Management Service**

  Backs up the database for the domain management, license management and the contact list.
  – **Groupware Service**

  Backs up the groupware-related files and the associated configuration files.
  – **Installation Files**

  Backs up the answer file of the installation.
  – **lib-logging**

  Backs up the files `log4j.xml` and the `default_log4j.xml`.
  – **lib-snmpdbaccess**

  Backs up the SNMP traps that are sent during operation and stored in the database of the error management.
  – **Logfile Audit Configuration**

  Backs up the configuration file for the audit log.
  – **Media Server**

  Backs up the media-server-related files.
  – **OpenScape Branch Assistant Data**

  Backs up the database and the data of the OpenScape Branch Assistant.
  – **OpenScape Voice Assistant Data**

  Backs up the database and the data of the OpenScape Voice Assistant.
  – **Presence Management Component**

  Backs up the Presence Acl database.
  – **Presence Target Service**

  Backs up the Presence Target database.

- **Presence Configuration File**

  Backs up the configuration file of the Presence service.
- **Presence Service**

  Backs up the Presence database.
- **Presence XMPP Connector**

  Backs up the Presence XMPP connector database.
- **Rules Service**

  Backs up the Rule database.
- **Scheduler Service**

  Backs up the database for the time-controlled jobs of the Scheduler service.
- **svc-alarmhandler**

  Backs up alarms received during operation and stored in the database of the error management.
- **svc-faulthandler**

  Backs up error messages received during operation and stored in the database of the error management.
- **svc-loggingconfigmanager**

  Backs up the file `loggermanager_<guid>_localhost.xml` that contains the configuration for Trace-on-Resource and Online-Trace.
- **svc-onlinetrace**

  Backs up the configuration file for Online Trace.
- **Voice Portal**

  Backs up the voice-portal-related files.
- **Web Client Configuration Backup**

  Backs up the files for configuring the Web Client.
- **Web Client Database Backup**

  Backs up the database of the Web Client.
- **Workflow Engine**

  Backs up the database of the Workflow Engine.

Archives

Each archive defines a memory location under which created backup sets are stored. It also defines how this memory location can be accessed.

You can specify archives on local or remote computer systems. A remote computer system can be accessed via the following protocols:

- FTP
- SFTP

NOTICE:

You ideally store archives always in parallel on a remote SFTP / FTP server and on the local computer system. In this way you prevent the backup information from getting irretrievably lost in

case of a system crash. The backup information is in the ideal case then also locally available.

An archive may contain a configurable number of backup sets. If the number of backup sets you store in an archive is greater than has been configured, the respectively oldest backup sets are overwritten.

You can assign a password to protect an archive from unauthorized access.

Backup Schedules

You can use a backup schedule to automatically back up the configuration and data of the OpenScape system.

Jobs

The OpenScape system executes different administration processes in so-called jobs, which you control and monitor in the Common Management Platform. Each job comprises selected backup units that are successively processed by the job.

The following administration processes are executed in the OpenScape system as jobs:

- Backup of system units
- Restore of system units
- Export of configuration data
- Import of configuration data

3.1.3.1 How to Display/Edit the Settings of a Backup Set

How to display all backup sets available in the system:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **General** > **Backup Sets**.

   A list of all backup sets configured in the selected domain appears in the work area with following attributes:

   Archive name

   Name of the archive in which the backup set is saved.
   Creation date

   Date on which the backup set was created.
   Status

   Shows whether or not there are any faults in the backup set.
   Comment

   Comment, entered when the backup set was created (optional).
   Type

   Type of the backup units to be saved in the backup set.
   Service Release

   Version of the application
   Action by

   User that performed the backup action
3) To display the content of a backup set, select the checkbox that associates the relevant backup set and click on **Show content**.
4) To display or change the comment of a backup set, select the checkbox that associates the relevant backup set and click on **Edit comment**.
5) To display the information that was created during the generation of the backup set, select the checkbox that associates the relevant backup set and click on **Show reply**.
6) Click on **Close** to close the window.

3.1.3.2 How to Delete a Backup Set

How to remove a backup set from an archive:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Backup Sets**.

   A list of all backup sets configured in the selected domain appears in the work area.
3) Select the checkboxes of the backup sets that you want to delete.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected backup sets.

The selected backup sets are removed from the system's database and from the list of all backup sets.

3.1.3.3 How to Add an Archive

Prerequisites

Adequate administrative permissions

IMPORTANT:

You ideally store OpenScape system archives on an external SFTP / FTP server and the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash and it also locally available.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **General** > **Archives**.

A list of all archives that are configured in the selected domain appears in the work area.

3) Click on **Add**.

The dialog with the archive settings opens.

4) Under **Name** enter a short, unique name for the new archive.

Under this name the archive is administered in the Common Management Platform.

5) In case you have a Large deployment system and you are adding a Data backup archive you must select the Acting node.

NOTICE:

The acting node is defined as the node the final backup set will be stored in, not on which node the backup will start initially.

---

6) From the Protocol drop-down list select the protocol via which the archive is to be saved.

- **HD**, to locally store the archive on the server computer.
- **FTP**, to store the archive via FTP on a computer system in the network.

NOTICE:

For the deployment scenario Integrated Simplex of OpenScape UC Application applies: To save an

archive via FTP, a corresponding packet filter must be configured in OpenScape Voice.

- **SFTP**, to store the archive via Secure FTP on a computer system in the network.

  NOTICE:

  For the deployment scenario Integrated Simplex of OpenScape UC Application applies: To save an archive via SFTP, a corresponding packet filter must be configured in OpenScape Voice.

7) If you have selected the **HD** protocol, enter in the **Path on file system** field an absolute path in which the archive is to be saved.

`/var/siemens/backup`

NOTICE:

Special characters in the path are not supported.

NOTICE:

For the base directory of the entered path the read / write attributes must have been set. You can set these attributes with the following command: `chmod 777 <Base directory>`

8) When you have selected the **FTP** or **SFTP** protocol, proceed as follows:

a) In the **Path to server** field enter an absolute path in which the archive is to be stored.

`/ftp/siemens/backup`

NOTICE:

Special characters in the path are not supported.

b) Enter under **Server address** the server address of the computer system on which the archive is to be stored.

c) Under **Login name** and **Password**, enter the user name and the password to be used for access to the server computer.

IMPORTANT:

The special characters double quotes (") and comma (,) are not supported in the Password field.

9) In the **Maximum number of backup sets** section use the **Data** and **System** fields to specify the maximum number of backup sets of type Data or System to be stored in the archive.

10) If you want to save the archive data encrypted, enter the encryption password under **Encryption password** and **Confirm encryption password**.

11) Click on **Save** to copy the entries to the system's database.

The new archive is saved and displayed in the archives list.

Related tasks

How to Add a Backup Schedule on page 93
How to Back Up a Backup Set Manually (Immediate Backup) on page 98

3.1.3.4 How to Edit an Archive's Settings

How to edit an archive’s setting:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Click on the name of the archive the settings of which you want to edit.

   The dialog with the settings of the relevant archive opens.
4) Perform the desired setting modifications for the relevant archive.
5) Click on **Save** to copy the entries to the system's database.

3.1.3.5 How to Delete an Archive

How to delete an archive:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Select the checkboxes of the archives that you want to delete.

   NOTICE:

   The DEFAULT archive cannot be deleted.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected archives.

The selected archives are removed from the system's database and from the list of all archives.

3.1.3.6 How to Test an Archive

Here you can test whether you are able to access an archive. A check is made as to whether the computer system can be accessed and whether files can be created and deleted in the desired directory.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Select the checkbox of the archive you want to test.
4) Click on **Test archive**.

   You will be informed about the test results in a separate window.
5) Click on **Close** to close this informational window.

3.1.3.7 How to Display/Edit an archive's Backup Sets

How to Display an archive’s backup sets

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Select the checkbox that associates the archive the backup set of which you want to edit.
4) Click on **View backup sets**.

   A window opens that displays the backup sets of the selected archive.
5) To display the content of a backup set, select the checkbox that associates the relevant backup set and click on **Show content**.
6) To display or change the comment of a backup set, select the checkbox that associates the relevant backup set and click on **Edit comment**.

7) To display the information that was created during the generation of the backup set, select the checkbox that associates the relevant backup set and click on **Show reply**.
8) Click on **Close** to close the window.

3.1.3.8 How to Delete an Archive's Backup Sets

How to delete an archive’s backup sets:

Prerequisites

Adequate administrative permissions

Step by Step

1) Select in the **Domain** drop-down list of the toolbar the domain in which you want to delete an archive.
2) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
3) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
4) Select the checkbox that associates the archive from which you want to remove the backup sets.

   NOTICE:

   The DEFAULT archive cannot be deleted.
5) Click on **View backup sets**.

   A window opens that displays the backup sets of the selected archive.
6) Select the checkboxes of the backup sets that you want to delete.
7) Click on **Delete**.
8) Click on **OK** to confirm the deletion of the selected backup sets.

The selected backup sets are removed from the system's database and from the list of all backup sets.

3.1.3.9 How to Add a Backup Schedule

How to add a backup schedule:

Prerequisites

Adequate administrative permissions

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the installation of the dump RPM packet on the corresponding computer system.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires for the hard disk drives of the corresponding computer system the use of the ext3 file system on LVM2.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the following lines at the end of the file `etc/sudoers`:

```
sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
lvBackupManagentUtility.sh

sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
fsBackup.sh
```

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

   A list of all backup schedules configured in the selected domain appears in the work area.
3) Click on **Add**.
   The backup wizard dialog opens.
4) Select the archive to which the backup schedule is to be added.

   NOTICE:

   Backing up the file systems of the OpenScape UC Application computer systems for a Duplex deployment scenario, you must select the DEFAULT archive.

   - Use the **…** button to select an existing archive.
   - Click on the **Add** button to create a new archive.
5) Click on **Next**.
6) Select the **backup type** of the backup units which are to be backed up.
7) How to back up only selected backup units for OpenScape UC Application:
   a) Click on the name of the Application Server backup unit.

      A dialog box opens displaying the individual OpenScape UC Application backup units.
   b) Select the checkbox of the backup units you want to back up for OpenScape UC Application
   c) Click on **Save**
8) Select the backup units to be saved.
9) Click on **Next**.
10) Enter a short, unique name for the new schedule under **Name**.

    Under this name the schedule is administered in the Common Management Platform.
11) In the **Reoccurs** drop-down list, select the frequency with which the backup is to be repeated.
12) Specify in the **Backup on** field at which time the backup is to start.

13) In the **Occurrences** drop-down list select the frequency with which the backup is to be repeated.
14) Click on **Save** to copy the entries to the system's database.

The new backup schedule is saved and displayed in the list of backup schedules.

Related tasks

How to Add an Archive on page 89
How to Back Up a Backup Set Manually (Immediate Backup) on page 98

3.1.3.10 How to Edit Backup Schedules

How to edit a backup schedule:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

   A list of all backup schedules configured in the selected domain appears in the work area.
3) Select the checkbox that associates the backup schedule the settings of which you want to edit.
4) Click on **Edit**

   The dialog with the settings of the relevant backup schedule opens.
5) In the Reoccurs drop-down list, select the frequency with which the backup is to be repeated.
6) Specify in the Backup on field at which time the backup is to start.
7) In the Occurrences drop-down list select the frequency with which the backup is to be repeated.
8) Click on **Save** to copy the entries to the system's database.

3.1.3.11 How to Delete a Backup Schedule

How to delete a backup schedule:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

   A list of all backup schedules configured in the selected domain appears in the work area.
3) Select the checkboxes of the backup schedules that you want to delete.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected backup schedules.

The selected backup schedules are removed from the system's database and from the list of all backup schedules.

3.1.3.12 How to Display Backup Schedules

How to display a backup schedule:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

   A list of all backup schedules configured in the selected domain appears in the work area.
3) Select the checkbox that associates the backup schedule the settings of which you want to edit.
   - Name

     Name of the schedule.
   - Archive name

     Name of the archive in which the backup set is saved
   - Reoccurs

     Setting showing when and how often the schedule is repeated
   - Day (for weekly backup only)

     Day of backup.
   - Time

     Time of backup
   - Remaining occurences

     Shows how the schedule is repeated

3.1.3.13 How to Display the Job Status

Status information about the last executed or currently active job is stored and displayed in the Common Management Platform. Such jobs can involve backup, restore or an import or export of data.

Prerequisites

Adequate administrative permissions

Step by Step

1) Select in the **Domain** drop-down list of the toolbar the domain in which you want to display the status of a job.
2) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
3) In the navigation tree, click on **General** > **Latest Job**.

   The work area displays status information that concerns the last executed or currently active job and its backup units.
4) The job display refreshes automatically. You can update the display at any time by clicking on **Refresh**.
5) If you want to display further details of the last performed job, click on **Details**.

   NOTICE: The **Details** button is not available until the job has been fully processed.

Related tasks

How to Back Up a Backup Set Manually (Immediate Backup) on page 98
How to Restore System Elements by Backup Set on page 99

3.1.3.14 How to Terminate a Job

A job can be a backup, a restoration or an import or export of data.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Latest Job**.

   The work area displays status information that concerns the last executed or currently active job and its backup units.

3) While a job is being executed you can:

- You can use the **Cancel Running** button to cancel the processing of the backup unit being edited.

  The job will then start processing the next backup unit.

  NOTICE: This button is not available until a job is being processed.

- You can use the **Cancel All** button to cancel the processing of all backup units.

  The job is then immediately terminated.

  NOTICE: This button is not available until a job is being processed.

NOTICE:

Canceling a backup unit processing will take some time. If processing of a backup unit can be completed within this period, this processing will actually not be canceled.

3.1.3.15 How to Back Up a Backup Set Manually (Immediate Backup)

Besides the automatic backup by backup schedules you can start the backup also manually.

Prerequisites

Adequate administrative permissions

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the installation of the dump RPM packet on the corresponding computer system.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires for the hard disk drives of the corresponding computer system the use of the ext3 file system on LVM2.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the following lines at the end of the file `etc/sudoers`:

```
sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
lvBackupManagentUtility.sh

sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
fsBackup.sh
```

Enough empty disk space for the directory `/tmp` on the computer system.

NOTICE:

If there is not enough empty disk space for the directory `/tmp`, the backup process will aboard with an error message.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Backup**.

   The backup wizard dialog opens.
3) Select the archive to which the backup set is to be added.

   NOTICE:

   Backing up the file systems of the OpenScape UC Application computer systems for a Duplex deployment scenario, you must select the DEFAULT archive.

   - Use the **...** button to select an existing archive.
   - Click on the **Add** button to create a new archive.
4) Click on **Next**.
5) Select the **backup type** the backup units of which are to be backed up.
6) Select the **backup units** to be backed up.
7) Click on **Start backup**. The backup starts according to the settings made.

NOTICE: The backup percentage completion rate is displayed when backing up a file system as this function takes a long time particularly when backing up the file system to external SFTP/ FTP server.

NOTICE: The percentage completion rate is displayed as "N/A" when backing up the data since this function takes a short time to complete when compared to backing up a file system.

Related tasks

How to Add an Archive on page 89
How to Add a Backup Schedule on page 93
How to Display the Job Status on page 97

3.1.3.16 How to Restore System Elements by Backup Set

You can manually restore a file system or a database from a backup set.

Prerequisites

Adequate administrative permissions

You have previously saved the data to be restored in an archive.

The data of the archive are not damaged.

IMPORTANT:

You ideally store OpenScape system archives on an external SFTP / FTP server and the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash. The backup information is in the ideal case then also locally available.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **Backup& Restore** > **Restore**.

The restore wizard dialog opens.

3) Select with **…** the archive in which the desired backup set is stored.

In some cases the restore wizard do not display an archive for restoring the system elements – e. g. after a severe system crash. In this case, execute the following steps to restore the reference to an existing archive:

NOTICE:

When you restore an archive from the local file system, the restoration process operates under the Unix user account sym. Verify that all files of the relevant archive can be accessed with sym. If the system cannot access the files, you will be notified by a corresponding error message.

a) Click on **Add**.

The dialog with the archive settings opens.

b) Enter any archive name in the **Archive name** field.

c) In the **path on file system** field specify the path under which you previously stored the archive that you now want to use for restoring the system elements.

d) Click on **Save**.

The archive can now be selected in the restore wizard provided that the archive data are not damaged.

4) Click on **Next**.

5) Select the backup set that you want to use to restore the system elements.

6) Click on **Next**.

   The backup units of the selected backup set are displayed.

7) Select the backup units that you wish to restore.

8) Click on **Start Restore**.

The restore starts according to the settings made. The restore progress is then usually graphically displayed. If not, you can show the restore progress manually by displaying the job status.

IMPORTANT:

If you are restoring the database of a Simplex OpenScape Voice system, the symphoniad must be stopped and started after the successful database restore. After the successful database restore, as the root user, use the following commands to stop and start the symphoniad:

/etc/init.d/symphoniad stop

/etc/init.d/symphoniad start

Related tasks

How to Display the Job Status on page 97

3.1.3.17 How to Restore the Entire System After a Crash

How to restore the entire system after a crash:

Prerequisites

Adequate administrative permissions

You backed up the configuration and data of the OpenScape system in an archive before the crash.

The archive's data have not been damaged by the crash.

You have restored the file system of the computer systems concerned.

IMPORTANT:

You ideally store OpenScape system archives on an external SFTP / FTP server and the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash. The backup information is in the ideal case then also locally available.

A system crash of the OpenScape system may damage system files. If this happens, you need to reinstall the OpenScape system before you can restore the configuration and the data of the OpenScape system.

When reinstalling, definitely use the answer file you have created for the initial installation for the following reasons:

- The Symphonia community name must be the same for the initial and reinstallation.
- The administrator password for the system database must be the same for the initial and reinstallation. The import feature is otherwise unable to restore the database.
- The IP addresses and host names must be the same for the initial and reinstallation, since they are referenced in the data that will later restore them.

NOTICE:

If you restore the OpenScape system on another computer system, you disconnect the original computer system from the network. When you reconnect the original computer system to the network under a different IP address, verify that all components of the OpenScape system are deactivated on this computer system.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **Backup& Restore** > **Restore**.

The restore wizard dialog opens.

3) Select with **…** the archive in which the desired backup set is stored.

In some cases the restore wizard do not display an archive for restoring the system elements – e. g. after a severe system crash. In this case, execute the following steps to restore the reference to an existing archive:

NOTICE:

When you restore an archive from the local file system, the restoration process operates under the Unix user account sym. Verify that all files of the relevant archive can be

accessed with sym. If the system cannot access the files, you will be notified by a corresponding error message.

a) Click on **Add**.

The dialog with the archive settings opens.

b) Enter any archive name in the **Archive name** field.

c) In the **path on file system** field specify the path under which you previously stored the archive that you now want to use for restoring the system elements.

d) Click on **Save**.

The archive can now be selected in the restore wizard provided that the archive data are not damaged.

4) Click on **Next**.

5) Select the backup set that you want to use to restore the OpenScape system.

6) Click on **Next**.

The backup units of the selected backup set are displayed.

7) Select besides the **HiPath8000** backup unit all units for restoration.

In doing so be sure to select the units of all representable pages.

NOTICE:

If you do not want to restore specific units, exclude them from your selection.

NOTICE:

If you want to restore the configuration of OpenScape Voice, too, select the **HiPath8000** backup unit also.

8) Click on **Start Restore**.

The restore starts according to the settings made. The restore progress is then graphically displayed.

9) If you use OpenScape UC Application, restart OpenScape UC Application with the following commands.

a) `/etc/init.d/symphoniad stop`

b) `/etc/init.d/symphoniad start`

10) The password for the administrator account `administrator@system` is after the data restoration reset to the value that was valid when the backup files were stored. If you want to allocate a new password for the administrator account `administrator@system`, execute the following command.

- <Osc#Install [1]>`/servicetools/security/resetUserAccount.sh administrator@system` <new password >

[1] <Osc-Install > is the setup file of the OpenScape system: /opt/siemens/ or /enterprise/

3.1.4 Update & Restore System Configuration via Easy IP (EZ-IP)

Easy IP (EZ-IP) is a component responsible for changing configuration of the cluster node(s). It is used to update current configuration or restore previous system configuration(s) and is delivered in windows through NCPE package.

The Administrator can update and restore the following parameters without system outage and call processing outage, while the system stays at state 4.

General Tab parameter	Description
Default router IP	The machine that will route packets not currently addressed by the configured interfaces. **NOTICE:** In Node seperation scenarios, Default Router Node 2 IP address field will also be displayed.
Survival Authority IP	IP address of Survival Authority
Superuser IP	IP Address of the Element Manager. Default value : 0.0.0.0
NTP Server 1	Name (IP address) of network NTP Server
NTP Server 2	Name (IP address) of secondary network NTP Server
Stand Alone service enabled	Checkbox for enabling Stand Alone Service
Timeout	Timeout value for accessing DNS servers
Attempts	Maximum attempts for accessing DNS servers
IP 1	IP address of DNS name server
IP 2	IP address of secondary DNS name server
IP 3	IP address of third DNS name server
Domain 1	Name of primary search domain for DNS
Domain 2	Name of secondary search domain for DNS
Domain 3	Name of third search domain for DNS
Domain 4	Name of fourth search domain for DNS
Domain 5	Name of fifth search domain for DNS

General Tab parameter	Description
Domain 6	Name of sixth search domain for DNS

Remote Admin Tab parameter	Description
IP	Default value :0.0.0.0
Netmask	Netmask for this interface
MTC Controller URL	URL for the Remote Administration of Node 1/2
Gateway	Default Gateway for this interface

Routes Tab parameter	Description
Destination IP	Destination IP for this interface
Netmask	Netmask for this interface
Gateway	Default Gateway for this interface
Nafo ID	Failover Possible values : **1)** nafo0 (Administration network) **1)** nafo1 (Signaling network) **1)** nafo2 (Billing network) **1)** nafo3 (Installation network)

Servers Tab parameter	Description
Destination IP	By default the value is normally the NMC IP Address
Port	Trap destination port. Default value : 162
License Server 1	FQDN or IP
License Agent Port	License Agent Port on HiQ. **NOTICE:** It must match port specified during installation.

IMPORTANT:

In the case of Virtual configuration the fields are not editable nor visible by the user.

3.1.4.1 How to Configure the General EZIP Settings (`node.cfg` Parameters)

Security Administrator has the capability to create individual Packet Filter Rules (PFR) through the Packet Filter Rules management menu. It is assumed that he is an experienced user familiar with the system's aliases.

Prerequisites

The administrator profile must have the "Node.cfg Parameters" permission which is part of the access group Global Settings of OSV profiles. Default OSV profiles *Security Administrator* and *Super Administrator* have this access right by default.

Step by Step

1) Log on to the CMP and navigate to **Configuration** > **OpenScape Voice** tab.
2) Select the switch from the **Switches** dropdown list.
3) Navigate to the **Administration** > **General Settings** menu.
4) Click on the **EZIP**.

   The **EZIP Settings** dialog opens.
5) Navigate to the **General** area in order to add/edit the following basic information for the EZ-IP configuration.

General Tab parameter	Description
Default router IP	The machine that will route packets not currently addressed by the configured interfaces. **NOTICE:** In Node separation scenarios, Default Router Node 2 IP address field will also be displayed.
Survival Authority IP	IP address of Survival Authority
Superuser IP	IP Address of the Element Manager. Default value : 0.0.0.0
NTP Server 1	Name (IP address) of network NTP Server
NTP Server 2	Name (IP address) of secondary network NTP Server
Stand Alone service enabled	Checkbox for enabling Stand Alone Service
Timeout	Timeout value for accessing DNS servers
Attempts	Maximum attempts for accessing DNS servers

General Tab parameter	Description
IP 1	IP address of DNS name server
IP 2	IP address of secondary DNS name server
IP 3	IP address of third DNS name server
Domain 1	Name of primary search domain for DNS
Domain 2	Name of secondary search domain for DNS
Domain 3	Name of third search domain for DNS
Domain 4	Name of fourth search domain for DNS
Domain 5	Name of fifth search domain for DNS
Domain 6	Name of sixth search domain for DNS

6) Click **Save**.

3.1.4.2 How to Configure the Remote Admin EZIP Settings (`node.cfg` Parameters)

Prerequisites

The administrator profile must have the “Node.cfg Parameters” permission which is part of the access group Global Settings of OSV profiles. Default OSV profiles *Security Administrator* and *Super Administrator* have this access right by default.

Step by Step

1) Log on to the CMP and navigate to **Configuration** > **OpenScape Voice** tab.

2) Select the switch from the **Switches** dropdown list.

3) Navigate to the **Administration** > **General Settings** menu.

4) Click on the **EZIP**.

The **EZIP Settings** dialog opens.

5) Navigate to the **Remote Admin** area in order to add/edit the following basic information for the EZ-IP configuration.

Remote Admin Tab parameter	Description
IP	Default value :0.0.0.0
Netmask	Netmask for this interface
MTC Controller URL	URL for the Remote Administration of Node 1/2
Gateway	Default Gateway for this interface

6) Click **Save**.

3.1.4.3 How to Configure the Route EZIP Settings (`node.cfg` Parameters)

Prerequisites

The administrator profile must have the “Node.cfg Parameters” permission which is part of the access group Global Settings of OSV profiles. Default OSV profiles *Security Administrator* and *Super Administrator* have this access right by default.

Step by Step

1) Log on to the CMP and navigate to **Configuration** > **OpenScape Voice** tab.
2) Select the switch from the **Switches** dropdown list.
3) Navigate to the **Administration** > **General Settings** menu.
4) Click on the **EZIP**.

   The **EZIP Settings** dialog opens.
5) Select the **Routes** tab in order to Add/Edit basic information for the EZ-IP configuration.

Routes Tab parameter	Description
Destination IP	Destination IP for this interface
Netmask	Netmask for this interface
Gateway	Default Gateway for this interface
Nafo ID	Failover Possible values : **a)** nafo0 (Administration network) **a)** nafo1 (Signaling network) **a)** nafo2 (Billing network) **a)** nafo3 (Installation network)

   For information on the Add/Edit Route fields refer to Section Route Settings
6) Click **Save**.

3.1.4.4 Route Settings

In the **Routes** Add/Edit window you will find the following parameters:

Add/Edit Route parameter	Description
Destination IP	Destination IP for this interface
Netmask	Netmask for this interface
Gateway	Default Gateway for this interface

Add/Edit Route parameter	Description
Nafo ID	Failover Possible values: **1)** nafo0 (Administration network) **1)** nafo1 (Signaling network) **1)** nafo2 (Billing network) **1)** nafo3 (Installation network)

3.1.4.5 How to Configure the Server EZIP Settings (`node.cfg` Parameters)

Prerequisites

The administrator profile must have the “Node.cfg Parameters” permission which is part of the access group Global Settings of OSV profiles. Default OSV profiles *Security Administrator* and *Super Administrator* have this access right by default.

Step by Step

1) Log on to the CMP and navigate to **Configuration** > **OpenScape Voice** tab.

2) Select the switch from the **Switches** dropdown list.

3) Navigate to the **Administration** > **General Settings** menu.

4) Click on the **EZIP**.

The **EZIP Settings** dialog opens.

5) Navigate to the **Servers** area in order to add/edit basic information for the EZ-IP configuration.

Servers Tab parameter	Description
Destination IP	By default the value is normally the NMC IP Address
Port	Trap destination port. Default value : 162
License Server 1	FQDN or IP
License Agent Port	License Agent Port on HiQ. **NOTICE:** It must match port specified during installation.

For information on the Add/Edit SNMP Destination Server fields refer to Section SNMP Settings.

6) Click **Save**.

3.1.4.6 SNMP Settings

In the **SNMP** Add/Edit window you will find the following parameters:

Add/Edit SNMP 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: **1)** v2c **2)** 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: **1)** v2c, Security Name = public **2)** 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: **1)** MD5 **2)** SHA
Auth Password	Authentication password. Only enabled if Version is set to v3 and Auth/Security Level is set to authPriv or authNoPriv.

Add/Edit SNMP parameter	Description
Privacy Type	Encryption standard. If Version is set to v3 and Auth/ Security Level is set to authPriv the following options are available: **1)** AES (Advanced Encryption Standard) **2)** DES (Data Encryption Standard)
Privacy Password	User password. Only enabled if Version is set to v3 and Auth/Security Level is set to authPriv.
Trap Engine ID	Identifier for the given SNMP.

3.1.5 A Non-Service Affecting Tool to Add and Delete OSV Static Routes

The OpenScape Voice (OSV) now provides a tool to add and delete OSV static routes without impacting service. This tool is invoked via the OSV node command line with the ManageRoutes.pl script. This script allows the root user to update (Add or Delete) static routes in the OSV while the system is in state 2, 3 or 4. Previously this activity was only possible with EZIP, which required a node outage.

3.1.5.1 Description

The script is node specific, meaning only updates to the OSV file configuration data and Operating System (O/S) routing data on the current node will take place. On a cluster system the command should be repeated on the other node. Two main tasks are performed by the script:

- Add Route
- Delete Route

Additionally the user can display:

- The route data of the OSV node O/S and configuration files (option -**view**)
- The ManageRoutes.pl script version (option -**version**)
- The syntax of the script (option -**help**)
- The info presented here (option -**info**)

Three types of static routes are supported:

- Multicast / Broadcast
- IPv4
- IPv6

All IPv4 routes are automatically added as source base routes provided there is an associated gateway (admin/billing/signaling) on the same subnet.

The script performs 10 main functions:

1) validate user parameters

2) read route data from node.cfg, routes.cfg and O/S tables
3) run the GenRoutesChecker script
4) validate user input parameters with respect to O/S route data
5) update O/S global routes
6) update O/S source base routes
7) update node.cfg file and generate new checksum
8) update source base route configuration file
9) re-run the GenRoutesChecker script
10) display results

The user parameters are validated for basic consistency to ensure all mandatory parameters are specified and that IP addresses are formatted correctly. The following checks are performed:

- All mandatory parameters are specified
- IPv6 and IPv4 destination and gateway addresses are valid
- CIDR is valid for destination IP address

The OSV configuration data and O/S data is read and validated. The following data is read:

- node.cfg gateways, routes and subnets
- Routes.cfg source base route data
- O/S global routes
- O/S source base routes

The script will call the GenRoutesChecker script to validate routes are correctly configured on the system. If this script fails then the user will have to resolve these issues before the route updates can be performed to the system. This behavior can be over-ridden using the -**nogenrouteschecker** option. The **nogenrouteschecker** skips the initial GenRoutesChecker script validation.

IMPORTANT:

Caution needs to be exercised when using the nogenrouteschecker option because a route that can negatively affect the OSV routing can be entered into the O/S (and node.cfg file).

Further validation is performed to ensure the user parameters match the current OSV configuration and O/S data.

- device is present in O/S
- gateway address in on a valid subnet
- if action is add check if the route does not already exists
- if action is delete check if the route does exists

The O/S routes and source base routes are then updated. Only routes that are added by the script can be deleted by the script.

NOTICE:

This behavior can be circumvented using the -**forcedelete** option. This **ManageRoutes.pl** script option should be used with care as it directly impacts the installed routing of the OSV node(s).

Routes in the node.cfg are defined as first node (node1) or second node (node2). In a cluster configuration the route will only be applied to the O/S if the node matches the node identity. The route will always be added to the node.cfg file even if not added to the O/S (because node.cfg files must be identical in a cluster configuration). In a co-located OSV the routes will typically be added to the O/S and node.cfg files of both nodes. In a network separated OSV configuration the O/S routes will be different between the nodes but the node.cfg files will be identical.

Routes which are updated in the O/S will also be updated in the node.cfg file unless the **-nonodecfgupdate** option is specified.

IMPORTANT:

This option should only be used by IFgui Update tool (EZIP). It is NOT considered a good practice to use this option from the command line because the route is not updated to the node.cfg. If this route data is not updated to the node.cfg a subsequent reboot will clear the route from the O/S. It is important to keep the node.cfg consistent with the O/S routes

---

Any changes to the node.cfg will result in a new checksum being recalculated for the node.cfg file.

If it is determined that no action is to be performed then the script will exit.

Note the GenRoutesChecker script will always be re-run at the end of the script independent of the **-nogenrouteschecker** option value. This ensures any action performed did not cause any issues.

Finally the script will display if any updates were made and if any errors where found.

```
O/s global route:   Updated:            YES (or NO)
O/S source routes:  Updated:            YES (or NO)
Node.cfg:           Updated:            YES (or NO)
Routes.cfg:         Updated:            YES (or NO)
GenRoutesCfg:       Errors:             YES (or NO)
GenRoutesChecker:   Errors:             YES (or NO)
```

For a cluster system the ManageRoutes.pl script output always includes the syntax necessary to update the route data to the partner node.

Each execution of the ManageRoutes.pl script generates a backup node.cfg file. Up to 5 backups of the node.cfg file will be maintained. These files will be named node.cfg.bak1 through node.cfg.bak5, with node.cfg.bak1 being the most recent node.cfg backup. When the OSV node has five node.cfg backup files the next ManageRoutes.pl script activity will overwrite the already existing files. The original node.cfg will be copied to node.cfg.orig. These files are written to /etc/hiq8000.

3.1.5.2 Restrictions/Cautions

- The default behavior of the -delete option is to only delete routes that have been added by the **ManageRoutes.pl** script. Installed node.cfg routes cannot be deleted unless the **-forcedelete** option is used.

  IMPORTANT:

  The **-forcedelete** option should be used with caution as it directly impacts the installed routing of the OSV node(s).

- The script only changes the routes and node.cfg file on the local OSV node.

  IMPORTANT:

  To keep the node.cfg and routes consistent the same action must be applied to both nodes of a cluster. It is the responsibility of the craft to run the tool on both OSV nodes. Failure to do so will result in RapidStat reporting a routing mismatch.

- Routes which are updated in the O/S will also be updated in the node.cfg file unless the **-nonodecfgupdate** option is specified.

  IMPORTANT:

  This option should only be used by IFgui Update tool (EZIP). It is NOT considered a good practice to use this option from the command line because the route is not updated to the node.cfg. If this route data is not updated to the node.cfg a subsequent reboot will clear the route from the O/S.It is important to keep the node.cfg consistent with the O/S routes. The node.cfg files must be identical in a cluster configuration. In a co-located OSV the routes will typically be added to the O/S and node.cfg files of both nodes. In a network separated OSV configuration the O/S routes will be different between the nodes but the node.cfg files will be identical.

- The **nogenrouteschecker** skips the initial **GenRoutesChecker** script validation.

  IMPORTANT:

  Caution needs to be exercised when using the **-nogenrouteschecker** option because a route that can negatively affect the OSV routing can be entered into the O/S (and node.cfg file).

3.1.5.3 Syntax

```
ManageRoutes.pl -action add|delete -type M -ipdest
IPAddress[/CIDR] -device [ethX|bondX] [OPTS]
```

```
ManageRoutes.pl -action add|delete -type 4 -ipdest
IPAddress[/CIDR] [ -gw [IPAddress] | -device [ethX|
bondX|] ] [OPTS]

ManageRoutes.pl -action add|delete -type 6 -ipdest
IPAddress[/CIDR] -gw [IPAddress] [OPTS]

ManageRoutes.pl -action viewO/S global route: Updated: YES
(or NO)

ManageRoutes.pl -version

ManageRoutes.pl -info

OPTS: [ -nonodecfgupdate | -nogenrouteschecker | -
forcedelete | -node first|second|both | -test_only]
```

Parameters:

-action: Mandatory, action to perform

- add - Add a route to the O/S and update node.cfg file
- delete- Delete a route to the O/S and update node.cfg file
- view- Display OSV config data and O/S route data

-device: the Device which the route is associated with.It is mandatory for MultiCast routes

- For IPv4 routes required if no gateway specified
- See ifconfig -a for list of valid devices

-gw: Gateway the route is associated with. Mandatory for IPv6 routes.

- Required for IPv4 routes if no device is specified
- IPAddress (IPv4 or IPv6) input in dotted decimal format.
- This parameter is not valid for Multicast routes.

-ipdest: Mandatory, IP Destination Address: IP address (IPv4 or IPv6) in dotted/colon decimal format. An optional CIDR netmask can be added. If the CIDR is not supplied the IP address will be treated as a host address; in this use case an IPV6 address CIDR will be 128. For an IPV4 address the CIDR will be 32. A CIDR to IPv4 Netmask Table is listed at the end of this section.

-node: Optional, Describes the nodeID the request is associated with. One of first, second or both. If the node parameter is not used the nodeID is determined using the solution, test_bed and node_separation parameters in the node.cfg.

- solution 25 (assume low cost), node set to first.
- test_bed simplex, node set to both.
- test_bed cluster and node_separation none, node set to both.
- test_bed cluster and node_separation separated and nodeid=1, node set to first.
- test_bed cluster and node_separation separated and nodeid=2, node set to second.

Since the node.cfg file should be identical on both nodes, the **ManageRoutes.pl** script must be run on both nodes. The route is always updated in the node.cfg (unless the **-nonodecfgupdate** option is used) but is only applied to the O/S on the node that matches the node parameter.

-nonodecfgupdate: Optional, Do not update the node.cfg file. In general this option should only be used by EZIP. It is NOT considered a good practice to

use this option from the command line because the route is not updated to the node.cfg. If this route data is not updated to the node.cfg a subsequent reboot will clear the route from the O/S. Care must be taken when using this option since an inconsistency between the node.cfg and O/S may result. The node.cfg files must be identical in a cluster configuration.

-forcedelete: Optional, Normally users can only delete routes which have been added by the script. Deleting a pre-installed route will be rejected unless the **-forcedelete** option is used. This avoids issues where routes could be deleted that would impair the OSV operation in a negative manner.

-test_only: Optional. Runs the script in test only mode. No updates are made to the O/S or configuration files. The script will validate the OSV node O/S routes, config files and the user input data and report any issues to the console. The best practice is to always execute the **ManageRoutes.pl** with the **-test_only** option before attempting any routing updates to the OSV node. All issues should be resolved before attempting an update without the **-test_only** option. A summary of the changes that would have been made is reported. This includes:

- global O/S route command
- source base O/S route command.
- changes to be made to the node.cfg file.
- GenRoutesCfg and GenRoutesChecker results

-type: Mandatory, Route Type. Three types of routes can be added to the OSV:

- M - Multicast Routes
- 4 - IPv4 Static Routes
- 6 - IPv6 Static Routes

-version: Display script version

-view: Display the routing data of the OSV node O/S and configuration files

-help: The syntax of the **ManageRoutes.pl** script

-info: The info presented here

3.1.5.4 Best Practice for ManageRoutes.pl Script Execution

It is a good practice to follow this convention when adding static routes to the OSV node(s):

1) In case an invalid configuration can not be resolved, have a current file system backup available before the **ManageRoutes.pl** activity takes place. If a current file system backup for the OSV system is not available one should be made. Refer to the “Backup & Restore” section of OpenScape Voice Service Manual, Service Documentation. At the very least the Active and Fallback partitions of the OSV node(s) should be synchronized before the ManageRoutes.pl activity takes place.

2) It’s important to understand the existing route configuration before executing the ManageRoutes.pl script. Run the ManageRoutes.pl script with the **-action view** option to list the current configuration. This output can be used to help resolve any warnings or errors that may be reported by a ManageRoutes.pl test_only check (step 3).

3) Execute the ManageRoutes.pl script with the -test_only option before actually executing any routing updates to the OSV node. All errors reported

during the –test_only run must be resolved before attempting the actual OSV routing update. A summary of the changes that would have been made is reported. This includes:

- results of the global O/S route command
- results of the source base O/S route command
- any changes to be made to the node.cfg file
- results of the **GenRoutesCfg** and **GenRoutesChecker** commands

4) After resolving any warnings or errors that may be reported by step 3, execute the **ManageRoutes.pl** script to add or delete the routes from the OSV nodes. Execute the command on both nodes of a duplex system. For a cluster system the **ManageRoutes.pl** script output always includes the syntax necessary to update the route data to the partner node.

3.1.5.5 ManageRoutes.pl Script Examples

It is a good practice to execute the ManageRoutes.pl script with the **test_only** option before executing any routing updates to the OSV node.

1) View the OSV route data

```
ManageRoutes.pl - action view
```

2) Add IPv4 host gateway route

```
ManageRoutes.pl -action add -type 4 -ipdest
200.20.20.20/32 -gw 10.48.250.1
```

3) Add IPv4 subnet device route

```
ManageRoutes.pl -action add -type 4 -ipdest
200.20.0.0/16 -device bond0
```

4) Add IPv6 host gateway route

```
ManageRoutes.pl -action add -type 6 -ipdest
fd00:4:5:6:10:48:250:118/128 -gw fd00:4:5:6::1
```

5) Add IPv6 subnet gateway route

```
ManageRoutes.pl -action add -type 6 -ipdest
fd00:4:5:6:10:48:250:118/128 -gw fd00:4:5:6::1
```

6) Add Multicast host device route

```
ManageRoutes.pl -action add -type M -ipdest
239.255.2.3/32 -device bond0
```

7) Delete IPv4 host gateway route

```
ManageRoutes.pl -action delete -type 4 -ipdest
200.20.20.20/32 -gw 10.48.250.1
```

8) Delete IPv4 subnet device route

```
ManageRoutes.pl -action delete -type 4 -ipdest
200.20.0.0/16 -device bond0
```

9) Delete IPv6 host gateway route

```
ManageRoutes.pl -action delete -type 6 -ipdest
fd00:4:5:6:10:48:250:118/128 -gw fd00:4:5:6::1
```

10) Delete IPv6 subnet gateway route

```
ManageRoutes.pl -action delete -type 6 -ipdest
fd00:4:5:6::/64 -gw fd00:4:5:6::1
```

11) Delete Multicast host device route

```
ManageRoutes.pl -action delete -type M -ipdest
239.255.2.3/32 -device bond0
```

12) Add IPv4 host bi-pass GenRoutesChecker test

```
ManageRoutes.pl -action add -node both -type 4 -ipdest
239.255.2.3/32 -device bond0 -nogenrouteschecker
```

13) Add IPv4 host route on Geo-Separated first node (node1) - repeat command on both nodes

```
ManageRoutes.pl -action add -node first -type 4 -ipdest
200.20.20.20/32 -gw 10.48.250.1
```

14) Add IPv4 host route on Geo-Separated second node (node2) - repeat command on both nodes

```
ManageRoutes.pl -action add -node second -type 4 -
ipdest 200.20.20.20/32 -gw 10.50.250.1
```

15) Add IPv4 host gateway route in test only mode

```
ManageRoutes.pl -action add -type 4 -ipdest
200.20.20.20/32 -gw 10.48.250.1 -test_only
```

3.1.5.6 ManageRoutes.pl Script Log files and Data Collection

Log files generated by the **ManageRoutes.pl** script:

- /log/ManageRoutes.log contain trace statements from this script.
- /var/log/messages contains an entry when any route is added/deleted
- up to 5 backup versions of the latest node.cfg file will be maintained.
- the original node.cfg will be copied to /etc/hiq8000/node.cfg.orig.

If this script fails then the following information should be collected:
Files (from each node of a duplex system)

- /etc/sysconfig/network/ifroute-*
- /etc/hiq8000/node.cfg.*
- /etc/hiq8000/routes.cfg
- /log/ManageRoutes.log
- /log/GenRoutesCfg.log
- /log/GenRoutesChecker.log
- /log/route_table.log
- /log/static_route.log
- /etc/init.d/route_table status

Displays (from each node of a duplex system)

- ip route show table all
- ip -6 route show
- /etc/hiq8000/ManageRoutes.pl -view

3.1.5.7 CIDR to IPv4 Netmask Table

The ip destination netmask should be entered in CIDR format. Here is the dotted to CIDR translation:

```
cidr == 32 => 255.255.255.255;
cidr == 31 => 255.255.255.254;
cidr == 30 => 255.255.255.252;
cidr == 29=> 255.255.255.248;
cidr == 28=> 255.255.255.240;
cidr == 27=> 255.255.255.224;
cidr == 26=> 255.255.255.192;
cidr == 25=> 255.255.255.128;
cidr == 24=> 255.255.255.0;
cidr == 23=> 255.255.254.0;
cidr == 22=> 255.255.252.0;
cidr == 21=> 255.255.248.0;
cidr == 20=> 255.255.240.0;
cidr == 19=> 255.255.224.0;
cidr == 18=> 255.255.192.0;
cidr == 17=> 255.255.128.0;
cidr == 16=> 255.255.0.0;
cidr == 15=> 255.254.0.0;
cidr == 14=> 255.252.0.0;
cidr == 13=> 255.248.0.0;
cidr == 12=> 255.240.0.0;
cidr == 11=> 255.224.0.0;
cidr == 10=> 255.192.0.0;
cidr == 9=> 255.128.0.0;
cidr == 8=> 255.0.0.0;
cidr == 7=> 254.0.0.0;
cidr == 6=> 252.0.0.0;
cidr == 5=> 248.0.0.0;
cidr == 4=> 240.0.0.0;
cidr == 3=> 224.0.0.0;
cidr == 2 => 192.0.0.0;
cidr == 1=> 128.0.0.0;
cidr == 0=> 0.0.0.0;
```

3.2 Import and Export of System Data

Data for the **Common Management Platform** (Domain Management, System Management), **OpenScape Voice** (Assistant data, all Configuration data,

Subscriber / Endpoint data) and **OpenScape Branch** can be imported or exported easily via csv or zip files.

The following data can be imported and exported:

- Data for **Common Management Platform**
  - Domain Management

    Comprises user- and resource-related data. You can use predefined lists (*.csv or *.zip) to import multiple users or multiple resources or export these to a list. This is an advantage if you need to work with large amounts of data.

    For Import/Export, please be aware of the following exceptions:

    Pins and passwords are not exported.

    Domains are exported but can not be imported.

    Profiles as profile objects can not be imported. A user can be assigned profiles if they have already been specified, e.g. by the **Common Management Platform**.

    NOTICE:

    You can obtain more structure information by experimentally exporting the relevant data.

  - Domain Management for **Xpressions**

    Comprises user- and resource-related data in a format that can be used for an import into a **OpenScape Xpressions** system.
  - System Management

    Comprises the **Common Management Platform** and **OpenScape UC** Application configuration data with all nodes and applications.
- Data for **OpenScape Voice**
  - Assistant data (switch-independent)

    Comprises the **OpenScape Voice** data: URL of the DLS, DLS job information, List of all job IDs.
  - Assistant data (switch-specific)

    Comprises the **OpenScape Voice** data: Endpoint templates, Subscriber templates used for the **OpenScape Voice** user management, Business group specific default values, Customer-specific notes for the **OpenScape Voice** main entities (business groups, subscribers, feature profiles etc.), Gateway URLs.
  - Assistant data (switch-specific with DLS)

    Comprises the **OpenScape Voice** data: URL of the DLS, DLS job information, Endpoint templates, Subscriber templates used for the **OpenScape Voice** user management, Business group specific default values, Customer-specific notes for the **OpenScape Voice** main entities (business groups, subscribers, feature profiles etc.), Gateway URLs.
  - All configuration data

    Comprises the **OpenScape Voice** data: Business Group, Subscribers, Endpoints, Endpoint Profile, Feature Profile, Numbering Plan, Office Code, Directory Number, Routing Area, Class of Service, Calling

Location, Destinations, E911 Subnets, Authorization Codes, Executive/ Assistant, Speed Calling Lists, Departments, Routes, Alias, Time, Destination, Day Schedule, Period Schedule, Weekly Schedule, Media Gateway, Media Gateway Circuits, Code Processing, Origin Destinations, Origin Route, Carrier Destinations, Carrier Route, CAC Groups, CAC Policies, MLHG, Prefix Access Codes, Destination Codes, Location Codes, ENUM Operators, ENUM Servers, Intercepts, Treatment, RTP Parameter, Display Number Modification.

– Subscriber/endpoint data (ENUM format)

  Comprises the **OpenScape Voice** data: Directory Number and SIP.

- Data for **OpenScape Branch**

  Comprises the **OpenScape Branch** configuration file.

3.2.1 How to Import Data

How to import Data:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Import**.

The dialog for importing a file opens.

2) In the **Import file** field specify the name of the import file (*.csv or *.zip).

- Enter the name and path or
- use the **Browse** button to select the file.

The dialog with the associated information opens.

3) Select the **Type of file to be imported**.

4) Select the **Included type of data** to be imported.

5) Select the **Target Node** for the file to be imported. Enter the name or use the search function **...**.

6) Click **Import**.

The import of data is started. A message will show the success or the error reason of the import procedure.

3.2.1.1 How to Import OpenScape Voice Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Import**.

The wizard for importing data opens.

2) Enter the name and path or use the **Browse** button to select the file. Click **Next**.

3) Select the type of data.
4) Select **All configuration data** under tab **OpenScape Voice**.
5) Select a target system under **Target** for import.
6) Click **Import**.

   The Latest Job Status window opens.

3.2.1.2 Assistant Data

The OpenScape Voice Assistant is the application to administer and configure the OpenScape Voice communications system. OpenScape Voice Assistant provides the element management interfaces.

The administrator is allowed to export files containing the assistant relevant data as well as the schema definition files for a successful recreation of that data.

Assistant relevant data to be exported:

- CheSe Group Identification (Members and their secondary lines)
- URL of Deployment Service (DLS)
- Gateway URLs
- URLs to external applications
- Business Groups (BGs) related defaults
- Subscriber Templates used for OpenScape Voice User Management
- Customer specific remarks for the main OpenScape Voice entities (BGs, Subscribers, Feature Profiles, etc.)
- Endpoint (EP) Templates

System Specific Information

The exported Assistant data consists of three file types:

- SQL files, representing each schema in the Assistant's database
- CTR files, containing information about each table's structure in every schema
- DAT files, containing the actual table data.

Other Characteristics

The export file can later be used as a base for DB-Offline generation or to configure an 'empty' newly installed Assistant. The newly installed Assistant has to administer the same OpenScape Voice as the original Assistant had (same BGs, Feature Profiles, etc.). In that case, the export file can be transferred between different Assistants.

3.2.1.3 How to Import Assistant Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Import**
   The dialog for importing a configuration is opened.
2) Enter the name and path or use the **Browse** button to select the file. Click **Next**.
3) Select **Assistant Data** under tab **OpenScape Voice Data**.
4) Click **Import**.
   The Assistant database is populated with the data from the import file.

3.2.1.4 How to Create a DB Import File for Offline DB Generation

Prerequisites

Adequate administrative permissions

Step by Step

1) Retrieve an exported file:
   - OSV configuration data
   - Assistant data
2) Import the export file into the Excel template for Offline DB Generation provided by the system.
3) Configure the parameters by editing the content as required.
4) Generate a DB Import file (`*.txt`) from the configured data.
5) Use the import file on the target system for Offline DB Generation.

3.2.2 How to Export Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Select your domain from drop-down list of menu **Domain:**.
2) Navigate to **Operation & Maintenance** > **Recovery** > **Import & Export** > **Export**.
   The wizard for exporting data opens.
3) Select in the field Common Management Platform one or more options:
   - Domain Management
   - Domain Management Export for Xpressions
   - System Management
4) Select the desired export units:
   - Select the desired export options for the Common Management Platform.
   - Select the desired export options for the OpenScape Voice.
   - Select the desired export options for the OpenScape Branch.

5) In drop-down list under **Select switches / appliances**, select the systems from which you want to export data.

NOTICE:

Erroneous selection of units can be corrected (overwritten) by a new selection.

---

6) Click **Next**.

The **Confirm export configuration** window opens. For your control, all configuration settings for the export are displayed.

7) Click **Export**.

The selected export data are exported and provided for downloading on the Common Management Platform computer system. The duration of this procedure depends on the extent of the exported data.

If export procedure failed a message window will show the error reason.

8) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

3.2.2.1 How to Export All OpenScape Voice Configuration Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**

The wizard for exporting data opens.

2) Select the desired export options for the OpenScape Voice.
3) Mark the checkbox **All Configuration Data**.
4) In drop-down list under **Select switches**, select the OpenScape Voice systems the data of which you want to export.

NOTICE:

Erroneous selection of switches can be corrected (overwritten) by a new selection.

---

5) Click **Export**.

The configuration data is exported to a text file.

The Latest Job Status window opens. A Backup is started. Use the link in the area **Result of export job** to download the configuration data.

3.2.2.2 How to Export Assistant Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**

   The dialog for exporting a configuration is opened.
2) Select in the **OpenScape Voice** field the checkbox **Assistant Data**..
3) From the right pop-up window select one option:
   - switch independent
   - switch specific
   - switch specific with DLS.
4) Define the switch in the field **Select switches**, if you selected a switch specific data file.
5) Click **Export**.

   The assistant data is exported to a zip file.

   The default file name is `ExportFile.zip`.
6) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

   A file download browser dialog opens, allowing you to save the zip file to a drive/device on the local system, to a drive/device located on a remote system, or to a network drive.

   The ZIP file exported from the OpenScape Voice Assistant must be decompressed to a local folder - preferably to the folder named `Exported Data/ name_of_zip_file`. This folder will be used as input source for the Offline DB Regeneration Template.

3.2.2.3 How to Export OpenScape Voice ENUM (Electronic Number Mapping) Data

How to export ENUM data:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

   The wizard for exporting data opens.
2) Mark checkbox **Subscriber Numbers in ENUM format**
3) Enter a switch in the **Select switches** field or click **Edit...** and select a switch from the list.
4) Click **OK**
5) Click **Next**.

   The **Confirm export configuration** window opens. For your check, all configuration settings for the export are displayed.
6) Click **Export**.

   The selected export data are exported and provided for downloading on the Common Management Platform computer system. The ENUM data is

exported to a text file. The duration of this procedure depends on the extent of the exported data.

If export procedure failed a message window will show the error reason.

7) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

3.2.3 How to Export Data Scheduled

How to Export Data Scheduled:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Schedules**.

   The **List of export schedules** window opens.

2) Definition of export schedules:

   - To create a new export schedule: Continue with step 3.
   - To change an existing export schedule: Mark the checkbox of the schedule. Click **Edit**. Continue with step 8.
   - To delete an existing export schedule: Mark the checkbox of the schedule. Click **Delete**.

3) Click **Add**.

   The **Schedule Export** wizard opens.

4) In **Select archive** select an existing archive or create a new one:

   - Type in the name of an archive.
   - Select an archive via Search function **...**.
   - Click **Add...** to add a new archive. Make your settings in the **Add new archive** window. Finish with **Save**.

5) Click **Next**.

   The **Component** window opens.

6) Select a component to export. Click **Next**.

7) Enter a name for the export schedule.

8) Define the fields **Reoccurs** and **Backup on** (date and time when you want to export).

9) Click **Save**.

   An export schedule was defined or changed.

3.2.4 How to Create User Accounts by Import

How to create user accounts by import:

Prerequisites

Adequate administrative permissions

Step by Step

1) Export the **Domain Management** component from the Common Management Platform to your local computer.
2) Open the downloaded Zip file.
3) Open the file `Package_domainmanagement_domainmanagement001.zip`.
4) Open the following file with a text editor: `domain_configuration.csv`.

   The exported OpenScape UC Application domain information is displayed.
5) Insert the information of the users that you want to add to the CMP in the exported file `domain_configuration.csv` under **##User**.

NOTICE: If the data is to contain special characters, you need to use a text editor that supports the UTF-8 file format. Microsoft Windows Wordpad and Microsoft Word do not support the UTF-8 file format. Notepad does.

NOTICE:

Separate the fields of an entry from each other with semicolon.

---

a) Enter the reserved name **User** in the user entry under **##User**. This name defines the entry as user entry.
b) Specify the ID (Login name from CMP) for the new user in the user entry under **id**.
c) Enter the domain to which the new user shall belong in the user entry under **domain**.
d) Specify the display name for the new user in the user entry under **displayName**.

Example:

##User	id	domain	displayName	...
User	tBrown	system	Tony Brown	...

6) Insert the information of the users that you want to add to the CMP in the exported file `domain_configuration.csv` under **##Contact**.

NOTICE:

Separate the fields of an entry from each other with semicolon.

---

a) Enter the reserved name **Contact** in the contact entry under **##Contact**.
b) Enter the user ID from step 5b in the contact entry under **externalId** in the following format: <User ID>@<domain>.
c) Go to field named **assignedSymUserIdentity** in the data structure for ##Contact. This field is used by the OpenScape system when importing data to assign the correct user entry to the contact entry.
d) Specify under **assignedSymUserIdentity** the information from the **externalId** contact field.

Example:

##Contact	externalID	...	assignedSymUserIdentity
Contact	tBrown@system	...	tBrown@system

7) Save the supplemented file `domain_configuration.csv` in the CSV format.
8) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
9) Import the Zip file in the Common Management Platform.

You have created user accounts via the Common Management Platform import feature.

3.2.5 How to Configure the IM Address by Import

How to configure the IM address by import:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

   The wizard for exporting data opens.
2) Export the **Domain Management** component from the Common Management Platform to your local computer.
3) Open the downloaded Zip file.
4) Open the file `Package_domainmanagement_domainmanagement001.zip`.
5) Open the following file with a text editor: `domain_configuration.csv`

   The exported OpenScape UC Application domain information is displayed.

6) Enter the respectively desired voicemail number in the exported file `domain_configuration.csv` in the **imAddress** field of the relevant subscriber entries.

   Example:

##Contact	externalID	...	imAddress	...
Contact	tBrown@system	...	tBrown@imdomain	...

7) Save the supplemented file `domain_configuration.csv` in the CSV format.
8) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
9) Import the Zip file in the Common Management Platform.

   You have now created user accounts via the Common Management Platform import feature.

You have configured the Instant Messaging address in the relevant subscriber accounts via the Common Management Platform import feature.

3.3 Configuration of Voicemail Numbers

Configuration of user settings are done by the Common Management Platform import feature in OpenScape UC Application, e.g. the voicemail number. This method is particularly useful to configure a setting for a large number of user accounts.

To configure a new voicemail number in user accounts by the Common Management Platform import feature the following steps must be performed:

1) Creation of a new Voicemail Number by Import
2) Configuration of a Voicemail number for User Accounts

3.3.1 How to Create a New Voicemail Number by Import

Prerequisites

Adequate administrative permissions

Step by Step

1) Export the **Domain Management** component from the Common Management Platform to your local computer.
2) Open the downloaded Zip file.
3) Open the file `Package_domainmanagement_domainmanagement001.zip`.
4) Open the following file with a text editor: `domain_configuration.csv`.

   The exported OpenScape UC Application domain information is displayed.

5) Add all voicemail numbers you want to configure in the user accounts in the next section to the exported file `domain_configuration.csv` under **##Voicemail**.

NOTICE:

Always specify phone numbers fully qualified in the GNF format. Example: 492404901100.

---

6) Specify the data for a new voicemail number:

NOTICE:

Separate the fields of an entry from each other with semicolon.

---

a) Enter the reserved name **Voicemails** under **##VoiceMail**. This name defines the entry as entry for a voicemail number.
b) Enter the new voicemail number fully qualified in the GNF format under **id**.
c) Enter the domain to which the new voicemail number shall belong under **domain**.
d) Specify the display name for the new voicemail number under **displayName**.

Example:

##VoiceMail	id	domain	displayName
Voicemails	492404901101	system	492404901101

7) Save the supplemented file `domain_configuration.csv` in the CSV format.
8) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
9) Import the Zip file in the Common Management Platform.

You have created voicemail numbers via the Common Management Platform import feature.

3.3.2 How to Configure a Voicemail Number for User Accounts

How to configure a voicemail number for user accounts:

Prerequisites

Adequate administrative permissions

Voicemail number is created.

Step by Step

1) Export the **Domain Management** component from the Common Management Platform to your local computer.
2) Open the downloaded Zip file.

3) Open the file `Package_domainmanagement_domainmanagement001.zip`.
4) Open the following file `domain_configuration.csv` with a text editor:

   The exported OpenScape UC Application domain information is displayed.
5) Enter the respectively desired voicemail number in the exported file `domain_configuration.csv` in the **assignedVoicemail** field of the relevant user entries.
   a) Go to **##User**
   b) Select the wanted user below **##User** from one of the fields **id** or **displayName**.
   c) Go to field **assignedVoicemail** of this user.
   d) Enter the Voicemail number.

   NOTICE:

   Always specify phone numbers fully qualified in the GNF format. Example: 492404901100.

   Example:

##User	id	domain	displayName	assignedVoicemail
User	tBrown	system	Tony Brown	4924049011001

6) Save the supplemented file `domain_configuration.csv` in the CSV format.
7) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
8) Import the Zip file in the Common Management Platform.

You have configured the created voicemail number in the relevant subscriber accounts via the Common Management Platform import feature.

3.4 Software Maintenance

Software Maintenance is performed to display the current release and revision levels of application software, to install patches and SMR (Software Maintenance Releases) on the OpenScape Voice software.

Software Maintenance activities can be performed on the OpenScape Voice server without affecting existing call processing service. However, calls in a setup phase may be dropped.

The Software Maintenance features provided via the OpenScape CMP (Common Management Platform) allow administrators to maintain the OpenScape Voice Servers by:

- Online Patching
- Remote Patching
- Interrogation and Display of the OpenScape Voice Server System Software and Patch Levels

3.4.1 Remote SW Upgrade

The general concept of upgrading performs major SW release upgrades remotely and splitting SW transfer from SW activation, which can reduce service cost related to sending service personnel to a site to perform the upgrade.

The remote upgrade procedure use the following features and properties:

- Creation of a place on the OSV node to store the image ISO, node.cfg, response file (for integrated systems), migration toolkit, license file, and OSV patchsets.
- Transferring the image, node.cfg, response file, license file, migration toolkit and OpenScape Voice patchsets to the nodes via SFTP.
- Execution of SW activation as a separate task instead of automatically activating the SW when it is transferred to the node.
- Elimination of the need for a real DVDs and USB sticks during major release upgrade.
- Utilization of the RSA functionality for remote access. Utilization of the Remote console for Virtual deployment.
- New boot option to execute the Upgrade Manager Functionality based on the Migration toolkit.

IMPORTANT:

For remote upgrades you need to have a fully functional system as a prerequisite.

3.4.1.1 SW Upgrade for Configuration Standard Duplex

SW activation is realized via the boot option which starts the on-board upgrade manager, based on the existing Migration toolkit SW.

IMPORTANT:

The continuous tracing is not active after an upgrade with the Migration toolkit. Migration toolkit will not save/import any tracing configuration.

There will be an outage of ~1 hour. If the outage is not acceptable on a Standard Duplex system, Live Upgrade can be performed.

Functional Sequence

Steps of the Upgrade

1) Install migration toolkit

- Install latest migration toolkit on both OSV nodes. This will also automatically create `/repository/upload` directory if it does not exist.

> **NOTICE:**
>
> All OpenScape Voice licenses which have the keyword OpenScape_Voice in the license file name are imported.
>
> All OpenScapeUC licenses which have the keyword OpenScape in the license file are imported.

2) SW Transfer

- Upload the image, `node.cfg`, license file, toolkit rpm, and OpenScape Voice patchsets (optional) to the `/repository/upload` on both nodes using SFTP.

> **NOTICE:**
>
> Use node.cfg.primary for Node 1 and node.cfg.secondary for Node 2.

- The user could also choose to transfer a single zip file containing the above files instead.

3) Upgrade Setup and Data Export phase via RSA.

- Using a single command (upgrade8k), the upgrade environment is setup and the configuration and DB data (this starts the provisioning freeze) into the new directory used to store.

4) Activation new SW via RSA

- You will use RSA for remote access (must log in to each node).
- You will reboot both nodes and boot of a new boot option to begin the SW activation.
- The on-board upgrade manager SW will look in a predefined directory for SW and files necessary to perform the upgrade.
- If the on-board upgrade manager SW finds all the SW and files necessary to perform the upgrade, the new SW will be installed on the backup partition including importing the data (via toolkit functionality).
- After the upgrade is completed the new software will be active.
- If for any reason the upgrade fails, the service person will be able to fallback to the source partition.

3.4.1.2 SW Upgrade for Configuration Simplex

The steps follow the process as Standard Duplex.

The OpenScape Applications will be automatically installed during image installation.

> **NOTICE:**
>
> Response files no longer need to be generated for integrated systems in `/repository/upload`.

If a response file is found in `/repository/upload` that file will take precedence over the file that is automatically generated via the Image installation.

3.4.1.3 How to Upgrade Version using OpenScape Voice Assistant

The Upgrade Version feature offers the capability to initiate and monitor an Upgrade Version of the System using CMP/OpenScape Voice Assistant. This procedure eliminates the use of DVDs and USB sticks or any Cli commands, so as the Service Administrator can execute the Upgrade remotely.

Prerequisites

Adequate administrative permissions

Step by Step

1) Logon to the CMP and navigate to **Maintenance** > **Inventory** tab.
2) Navigate to the **Applications** tab.
3) In the right menu of the Application view click on the **Upgrade Version** button.

   The **Upgrade Version** dialog opens.
4) In the **Upgrade Version** window the Service Administrator can view the required files for the Upgrade that are uploaded to the directory `/repository/upload` of the OpenScape Voice.

   NOTICE:

   In case of an Integrated Simplex system the **Upgrade Version** window contains only one textbox with the current content of the `/repository/upload` directory of the Node. In case of a cluster system there are two textboxes, one for the content of the directory for Node 1 and one for Node 2. In this case, the content must be the same for both Nodes.
5) Click **Start Upgrade** button.

   In case of a cluster system, once the Upgrade is initiated successfully the administrator will be informed about the status of the procedure. During this time the administrator may monitor the upgrade until the end or close the window and revisit it at a later time. A new dialog opens which displays the **Upgrade Status** of the system. The status is updated every 30 seconds informing the administrator about the progress of the Upgrade. If the procedure finishes successfully, the **Upgrade Status** value turns to **Completed**. When the Administrator presses the **Close** button, the OpenScape Voice Assistant "unlocks" for provisioning and administration.

   If any error occurs during the Upgrade an automatic fallback is initiated. In this case the administrator is informed and an option to **Download Logs** is offered. By clicking the **Download Logs** button a new pop up window is displayed and the user is asked to download the log files .tar.tgz for troubleshooting and further analysis. By clicking the **Finish Upgrade**

button, the OpenScape Voice Assistant "unlocks" the provisioning and the administration of OpenScape Voice system.

In the case of a OpenScape Voice simplex system, the OpenScape Voice Assistant is not available during installation so the administrator cannot monitor the upgrade status. An **Upgrade Version** dialog opens informing the administrator that the OpenScape Voice Assistant is not available and that the screen will not be updated. In case monitoring is needed, the Service Administrator can perform it remotely using the RSA. In case of error the Administrator shall collect manually the upgrade log files and contact the next level of support.

An upgrade of an OpenScape Voice cluster system takes approximately 2 hours (the time may differ and depends on the Database size of the number/ size of the additional patchsets).

When the procedure starts, the **Applications** list indicates that the specific OpenScape Voice is currently updated (under the **Active version** column the value **Upgrade version in progress..** is displayed). An error message will appear then the Administrator tries to **Upgrade version** while **Software Application** takes place. Moreover, in the **Nodes** list, the specific node under upgrade is not editable for maintenance (the dashboard of the node is not accessible). Finally, the corresponding switch is not available for provisioning, under the **Configuration** > **OpenScape Voice** > **General** > **Switches** menu. Under the **Version** column the value **Upgrade version in progress..** is displayed and under the **Connectivity** column the value **---** exists.

NOTICE:

In the case of an IntegratedSimplex deployment, when the upgrade of the menus finishes successfully, the upgrade status is not retrieved and appears to still be in progress. Follow the path **Maintenance> Inventory> Applications**, right click on the link and select **UpgradeVersion**. Refresh OpenScape Voice switch data from **Configuration > OpenScape Voice > General > Switches**, select the switch name link and click on the **Refresh Switch Data** button. When you apply these steps, OpenScapeVoice Assistant retrieves the status from OpenScape Voice, sees the completed status of the upgrade, unlocks the switch from CMP and updates the CMP screens with the correct OSV information status.

3.4.2 Recovery Escalation

The Recovery Escalation feature performs a stop and restart of the OpenScape Voice application when a rolling process restart is detected.

Simplex System

The Recovery Escalation detects if processes are restarting by detecting events with event number 107-47 with ’restart=no’.

If a number of these events is detected in a certain time period (more than 5 process starts or exits of the same process within 15 minutes) the node will be taken down to level 3 and back to level 4.

In case of a shared memory corruption this will solve the problem.

If no more restarts will be detected for 2 hours, the node is marked as "Fully Recovered".

If the rolling process start still persists the system requires probably a file system restore.

NOTICE:

A node restart of a simplex system is limited to one restart in 8 hours.

Duplex System

In a duplex system further actions will be performed. The following situations can occur.

Process restarts in one node only

- If the node restart did not fix the problem and rolling restarts persist, the offending node is taken down to level 3 and stay in this state for 24 hours.
- After 24 hours in state level 3 the node will be configured back to state 4.
- If no more restarts are detected for 2 hours, the node is marked as "Fully Recovered".

Rolling restarts in both nodes

- One node is restarted, the other node is restarted later. In case of a shared memory corruption these will be the only actions.
- If the problem is not cleared by node restart, the following steps will be performed.
  - Node 1 restarts once and is then deactivated.
  - Node 2 restarts more than 60 minutes later and stays active for 8 hours.
  - Once Node 2 is active again, Node 1 is re-activated.
  - More than 60 minutes later, Node 1 is deactivated and stays down until node 2 activates it either after 24 hours or when it restarts after 8 hours.

If the rolling process start still persists the system requires probably a file system restore.

Additional Information

The node restart function can also be triggered by the internal test call generator. The OpenScape Voice periodically generates a test call to itself. If the test calls fails repeatedly the involved call processing software processes are restarted. If this does not help a hiQTestCallGEnNotOkProcRestart alarm is generated and regenerated every 30 minutes for as long as test calls fail.

A node restart is not triggered in following situations:

- During an upgrade
- Within 60 (default) minutes after a node activation no caused by a node restart trigger.
- Within 60 (default) minutes after partner node activation or deactivation (simplex <-> duplex transition)
- While a node is leaving or entering standalone operation
- While the partner node is going to restart itself

NOTICE:

The given timers and counters are default values, they can be modified by Unify customer service.

Alarms

For this feature two critical alarms (’Node Recovery by Restart’ and ’Node Down’) will be produced.

- If the alarms clear normally, the system has been recovered from rolling process restarts.
- If the alarms clear and then recur, further actions are required (e.g. file system restore).

3.4.2.1 Rolling Process Restart Detection

Each OSV node monitors process restarts of its own node by watching the RTP dump log. When the same SW process starts more than 4 (default) times within 15 minutes (default) the node generates a major alarm event "Rolling Process Restarts".

The alarm is cleared after a node restart or when there are no more restarts of this process for 30 minutes (default). The alarm is re-generated every 30 minutes (default), if the alarm condition still exists.

NOTICE:

Currently the CDR Handler process is excluded from the node restart detection. The process may restart periodically on purpose when all billing servers are unavailable.

3.4.2.2 Callprocessing Failure Detection via Test Call Generator

The OSV periodically generates a test call to itself. If the test call fails repeatedly the involved callprocessing SW processes are restarted. If this does not help an alarm `hiQTestCallGenNotOkProcRestart` is generated and regenerated every 30 minutes for as long as test calls fail.

3.4.2.3 Node Restart Function

A node restart means stopping and restarting RTP middleware and all OSV processes. During a node restart the Linux operation system, cluster software (PrimeCluster or HA-Linux) and database (SolidTech) stay active.

Functional Sequence

The OSV process PSR monitors the RTP dump log for node restart trigger events. The reaction to such an event depends on redundancy status and history.

A node restart is triggered by the following event requirements:

- The event is logged in the RTP dump log
- The event reports a problem of the node on which it is logged.
- The event is re-generated at node startup and periodically with the period less than the **Node Restart Alarm Clearance Time** as long as the fault condition exits.

A node restart is not triggered:

- During upgrade
- Within 60 (default) minutes after a node activation not caused by a node restart trigger.
- Within 60 (default) minutes after partner node activation or deactivation (simplex <-> duplex transition).
- While a node is leaving or entering standalone operation.
- While the partner node is going to restart itself.

3.4.2.4 Node Restart: Simplex Operation

There is only one active node in the OSV cluster (Simplex OSV or partner node unavailable). Upon a node restart trigger event: OSV node restarts itself only if there have been no node restarts due to a node restart trigger event within the last 8 hours (default) and no node restarts within the last 60 minutes (default).

A critical **Node Recovery By Restart** alarm is reported. The alarm is cleared after 120 minutes (default) of no node-restart-triggers. If the node has to be restarted again because of a node-restart-trigger while a previous **Node Recovery By Restart** alarm is still active the alarm is re-generated (a clear event **Node Recovery Failed** followed by a new **Node Recovery By Restart** alarm).

Functional Sequence

- An OSV SW process crashes and is restarted automatically, but crashes again multiple times within a certain time period (more than 4 times in 15 minutes).
- An alarm **Rolling process restart event** is reported.
- The node is restarted and the alarm **Node Recovery By Restart** is reported.
- Once the node is active again the rolling process alarm is cleared with **Rolling Process Restart Alarm Reset**, and potentially reported again.
- If there are no restarts of the process for 30 minutes the alarm is cleared with **No More Rolling Process Restarts**.

If there are still restarts the alarm is cleared with **Rolling Process Restart Alarm Reset** and re-generated.

- If there are no more **Rolling process restart event** alarms within 120 minutes the node alarm is cleared with **Node Recovered**.
- **Rolling process restart event** is ignored for 8 hours after the node restart, i.e. the node is not restarted a second time.
- If the alarm **Rolling process restart event** appears again after 8 hours the node is restarted.

If the alarm **Node Recovery By Restart** is still active at this time it is cleared with **Node Recovery Failed** and re-generated as part of the node restart.

3.4.2.5 Node Restart: Duplex Operation

Both nodes of the cluster are active. Upon a node restart trigger event: If there have been no node restarts within the last 120 minutes (default) a critical **Node Recovery By Restart** alarm is generated. The node is restarted. If there has been a node restart due to a node restart trigger within the last 120 (default) minutes.

The event **Node Recovery Failed** is reported, which clears the current alarm. A critical **Node Down** alarm is reported. The node is deactivated. The node is restarted after 24 hours (default). Alarms are cleared with a **Node Recovered** event after 120 minutes (default) of no new node restart trigger events.

Functional Sequence

Before a node restarts itself it requests confirmation from the partner node:

- If node 2 has requested a confirmation and receives a confirmation request from node 1 it cancels its own restart activity and confirms.
- If node 1 has requested a confirmation and receives a confirmation request from node 2 it discards the request from node 2.

The result is that only node 1 restarts if both nodes see node restart triggers.

- An OSV SW process crashes and is restarted automatically, but crashes again multiple times within a certain time period (more than 4 times in 15 minutes).
- An alarm "Rolling process restart event" is reported.
- The node is restarted and the alarm "Node Recovery By Restart" is reported.
- Once the node is active again the rolling process alarm is cleared with "Rolling Process Restart Alarm Reset". If there are no more process restarts within 120 minutes the node alarm is cleared with "Node Recovered".
- If the alarm "Rolling process restart event" appears again within 120 minutes the node recovery alarm is cleared with "Node Recovery Failed" and a new alarm "Node Down" is generated and the node is deactivated.
- After 24 hours the node is re-activated (and the sequence continues starting three bullets above).

Other Characteristics

Rolling process restart in duplex that cannot be fixed because:

- Node1 has a rolling process restart
- Node1 is restarted
- Process restarts continues and the node is deactivated
- After a while (default 24 hours) node is re-activated
- Process restarts continue and node is deactivated again.

3.4.3 Online Patching

IMPORTANT:

If the patchset(s) are stored on the OpenScape Voice server the zip patch files downloaded from SWS must have srx read and write permissions on the target OpenScape Voice Server node. The unzip command must only be run as user srx on the

OpenScape Voice Server node. Address any questions to your next level of support.

Software Maintenance is performed to display the current release and revision levels of application software, to install patches and SMR (Software Maintenance Releases) on the OpenScape Voice software.

Online patching is used to implement patches and SMR (Software Maintenance Releases) on the OpenScape Voice software. It performs a software update without affecting service

In a cluster, online patching of the OpenScape Voice software can be performed as long as the new software is compatible with the old software.

Functional Sequence

During online patching with compatible new software, one node is stopped and updated with new software. After this process is complete, the same process takes place on the partner node.

Patching procedures always apply to the active partition only. Its software can be backed up prior to patching by copying its entire contents to the fallback partition.

Other Characteristics

Online patching is known as a rolling upgrade.

3.4.3.1 How to Upload Patches in the Common Repository

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes& Applications** > **Repository**.
2) Click **Add**.

   The dialog **Add to software repository** for uploading files opens.
3) Choose the files:
   - `.tar` and the corresponding `.spa` patchset files
   - Single ZIP archive containing all the necessary files.
4) Click **Save**.

   From the internal/external DVD the files are uploaded at `/repository`

NOTICE:

If it is needed to upload an OpenScape Voice emergency patchset , its .spa file needs to be edited in order to be saved successfully on CMP, since it contains information for all the base patchsets in addition to information for the emergency patchsets. It is necessary to edit it, remove the entries/info for the base OpenScape Voice patchsets

and save it. Under sections: Files and Checksums there must only be only entries/info for the OpenScape Voice emergency patchsets. Then it should be saved properly to CMP - Common Repository location. "

3.4.3.2 How to Check Node Health

Prerequisites

Adequate administrative permissions

Step by Step

1) Logon to the CMP and navigate to **Maintenance** > **Inventory** tab.
2) Navigate to the **Applications** tab.
3) Choose an application of type "OpenScape Voice" from the list. Click on the arrow at the right margin of the screen to open the context menu.
4) In the context menu click **Software Activation**.

   Window **Software activation** opens.
5) Click **Check Node Health** in the area **Software Updates**.

   This may take several minutes. You will get an information window with the following data about the node health:

   - CE IP, CE Name, Patch Version; OS Type, OS Version, RTP Version, Node DB Role, DB Version, Third Party Version and a sequence with all RapidStat Message Types (Error, Warning) and corresponding RapidStat Messages (Error, Warning).

3.4.3.3 How to Install Patch Sets

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes& Applications** > **Applications**.
2) Choose an application of type "OpenScape Voice" from the list. Click on the arrow at the right margin of the screen to open the context menu.
3) In the context menu, click **Software Activation**.

   Window **Software activation** opens.

NOTICE:

Upon using Location=CommonRepository, verify that there are no files with root:root permissions on your OpenScape Voice patchsets directory /software/patch/<release name dir> or the file transfer will fail with error: "sFTP error - Permissions denied Please delete the existing files", since

the OpenScape Voice Assistant can only transfer files with srx:rtpgrp permissions from the CMP local repository.

4) Choose the location and the corresponding OpenScape Voice patchset.
   - Select **node1** > **OpenScape Voice** if the patches are copied to the directory: `/software/patch/<release_level`.
   - Select **node1** > **DVD** if the patchsets are to be found on a DVD.
   - Select **Common Repository** if the patches are uploaded in the Common Repository
5) Select the **Synchronize two versions before Software Activation** checkbox if you want to synchronize the Active version to the Backup version.
6) Click **Activate**.

NOTICE:

You have to check whether the system really needs to be updated and is ready for the update.

To do so, click **Check Node Health**.

This may take several minutes and is mandatory.

NOTICE:

NOTICE:

If there is more than one node to update, select the **Auto continue to 2nd node** check box to automatically continue and update the second node.

Auto continue to 2nd node will not take place unless the Software Activation window remains open. If you close the Software Activation window, the **Auto continue to 2nd node** will not be applied.

The installing procedure on OpenScape Voice will start.

3.4.3.4 Upgrade Progress Screen

Upgrade Progress Screen opens after starting of upgrade process for new software to the connected nodes. During process you can follow the actual ongoing of the upgrading process at which node working and result.

Functional Sequence

The following information is given on the screen:

- CE IP:

  The IP address of the node being updated.

- CE Name:

  The name of the node being updated
- Upgrade State:

  The current state of the process being executed.

  E.g. UpgradeStateFallbackInProgress
- Percentage completion:

  The completion status of the currently running process as a percentage value
- Start Time:

  The date and time when the upgrade started.
- Originator IP:

  The IP address of the system on which the upgrade process was started.
- From Patchset:

  The version and number of the patchset that was installed before the current upgrade started.
- To Patchset:

  The version and number of the patchset that is currently being installed.
- Upgrade Method:

  The upgrade method used for the current upgrade.

  E.g. UpgradeMethodRolling
- Upgrade Message:

  The current status of the running upgrade.

  E.g. "Update started: 'adsa11n1: Installing units'"

3.4.3.5 How to Remove Patch Sets

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes& Applications** > **Applications**.
2) Choose an application of type "OpenScape Voice" from the list. Click on the arrow at the right margin of the screen to open the context menu.
3) In the context menu, click **Software Activation**.

   Window **Software activation** opens.
4) Choose the location and the corresponding OpenScape Voice patchset.
   - Select **node1** > **OpenScape Voice** if the patches are copied to the directory: `/software/patch/<release_level`.
   - Select **node1** > **DVD** if the patchsets are to be found on a DVD.
   - Select **Common Repository** if the patches are uploaded in the Common Repository.

5) Select the **Synchronize two versions before Software Activation** checkbox if you want to synchronize the Active version to the Backup version.
6) Click **Activate**.

NOTICE:

You have to check whether the system really needs to be updated and is ready for the update.

To do so, click **Check Node Health**.

This may take several minutes and is mandatory.

NOTICE:

NOTICE:

If there is more than one node to update, select the **Auto continue to 2nd node** check box to automatically continue and update the second node.

Auto continue to 2nd node will not take place unless the Software Activation window remains open. If you close the Software Activation window, the **Auto continue to 2nd node** will not be applied.

The rolling downgrade procedure on OpenScape Voice will start.

3.4.3.6 How to repair OpenScape Voice system after Rolling Upgrade failure

During a Rolling Upgrade, a pop-up window **Upgrade Progress** is displayed. This popup provides the status of the Rolling Upgrade. If the Rolling Upgrade is completed successfully the administrator can close the **Upgrade Progress** window. If the Rolling Upgrade fails, the **Upgrade Progress** window is updated to provide information related to the Rolling Upgrade failure. Follow these steps to repair an OSV system in case of a Rolling Upgrade failure :

Prerequisites

Adequate administrative permissions

Step by Step

1) Click **Download Logs** to download the log files. These logs will provide details to help locate the source of the Rolling Upgrade failure. A pop-up window for downloading the log files is displayed.

2) Click **Save** to save the log files locally and proceed with the fix of Rolling Upgrade Failure.

INFO: There are two options for completing the repair of the OpenScape Voice system after a Rolling Upgrade Failure:
- The first option is to escalate the problem directly to the next level of technical support. This option is applicable if no downtime is allowed and the administrator has enough time to debug the issue. The logs downloaded in step 1 should be made available for analysis when the Rolling Upgrade failure is reported. If you choose to follow this option, escalate the problem to the next level of support now. DO NOT proceed to steps 3 through 5 unless instructed to do so by the next level of support. -The second option is **Quick Repair**.This option will activate the Backup version of OpenScape Voice system and the system will be rebooted.This is applicable if downtime is possible, the administrator has no time to debug the issue and it is very important to have a system back to the level 4,as soon as possible.The Quick Repair steps are detailed in steps 3 through 5 of this section.

---

3) On the Upgrade Progress window, click **Quick Repair** button. A confirmation pop-up window **Quick Repair** is displayed.
4) Click **OK** to start the reparation process.The activation of Backup version starts and system is rebooted.
5) Click **Close** to close the **Quick Repair** window and wait for a few minutes.

NOTICE: Once the OpenScape Voice System is at level 4, the administrator may perform a manual version synchronization from the OpenScape Voice Dashboard in order to completely remove the problem from the system. The logs downloaded in step 1) should be available for analysis when the Rolling Upgrade failure is reported.

3.4.4 Remote Patching

IMPORTANT:

If the patchset(s) are stored on the OpenScape Voice server the zip patch files downloaded from SWS must have srx read and write permissions on the target OpenScape Voice Server node. The unzip command must only be run as user srx on the OpenScape Voice Server node. Address any questions to your next level of support.

The remote patching feature reduces maintenance costs by providing a method to access patching mechanisms and orchestrating related third-party software updating and upgrading mechanisms via a simple point-and-click user interface.

Functions of this capability:

- Semi-automates the patching procedure via a GUI

- Improves the success rate of patch installation
- Reduces frequency of patch back-outs and escalations to resolve patch installation failures.

Functional Sequence

The user interface is supported as follows:

- GUI via patch application for rolling upgrade
- CLI (Command Line Interface) and script for rolling upgrade and split-mode upgrade applications

Other Characteristics

Authorized service personnel can determine which method is best for the installation and customer. Patch sets can be stored in an OpenScape Voice local directory or on a DVD.

OpenScape Voice also provides an interface to the Serviceability Platform for Applications, which is a network that allows Enterprise Services to install patches on the OpenScape Voice family of products in accordance with service contract agreements.

3.4.5 Common SW Update User Interface

This feature provides a common user interface and a common patch repository, via the CMP (Common Management Platform), to apply software updates to the OpenScape Voice /OpenScape Voice, and OpenScape Branch from the remote services infrastructure.

The OpenScape Voice and OpenScape Branch Assistants providing a user interface to facilitate software update on OpenScape Voice, OpenScape SBC and OpenScape Branch nodes respectively with the following functions:

- Shows Active version of a selected node
- Select a repository from a list of repositories. This list shall include node specific repositories (if there are any) as well as the new common Software Updates Repository.
- Lists software versions available in the selected repository. In case the common repository is selected, only the ones that are applicable for the given product shall be listed.
- Activates Software:

  Depending on the location of the repository, this action may include transfer of software to the node. In this case, activation shall follow transfer without user intervention.
- Shows the activation progress (including transfer, if applicable)
- Provides the connecting function to the CMP.

Functional Sequence

The following functions are possible via the Software Repository GUI:

- View a list of all Software Updates available in the Repository (Product name, Version, File Size)
- Filter / sort the list on product name / version / size (sorting only)

- Delete Software updates:

  This is used to free disk space after updates are activated.
- Upload files:

  This will make possible to upload software updates, from administrator's laptop to the repository.

The repository manager supports CMP/Assistant and other openSOA (Service Oriented Architecture) services providing the following functions:

- Store uploaded software updates in the repository
- Delete software updates
- List software updates using certain filter/sorting criteria

  Filtering/sorting on:

  – Product name (i.e installable unit name)
  – Version
  – Size (sorting only) = sum of size of all files that make up the update)
- Provide the location of a given software update to facilitate transfer of it to the nodes by the Assistants

System Specific Information

The size of the Software Update Repository will be limited to at minimum 2.5 GB. This is to allow versions of OpenScape Branch as well as three patches per version for OpenScape Voice co-exist in the repository. The limit shall be enforced by the repository manager.

All installed units of nodes administered via the Common Management Platform are listed in the Common Management Platform UI to facilitate the launching of upgrade managers that are responsible to the given installed units. The current software versions executing on each installed unit is also shown.

Other Characteristics

Meta data in the format of a `.spa` file will be utilized for proper storage of uploaded software updates. Only software updates accompanied by a `.spa` file can be uploaded to the repository. The `spa` file specifies the description of a software update such as the product name, version, files and checksum.

A software update may constitute of one or more files. The format of a software update that can be uploaded to the common repository is specified in the `.spa` file that accompanies the software update.

For all the files that make up a software update the checksum are in the `.spa` file. A checksum check shall take place before the software update is accepted in the repository as a valid one.

All the files of a software update shall be discarded if at least one of them fails the checksum. At the UI level, the user is informed that upload failed due to checksum verification failure.

3.4.5.1 How to Update a Node via CMP (Common Management Platform)

Prerequisites

Adequate administrative permissions

Step by Step

1) Logon to the CMP and navigate to **Maintenance** > **Inventory** tab.
2) Navigate to the **Applications** tab.
3) Choose an application from the list. Click on the arrow at the right margin of the screen to open the context menu.
4) In the context menu click **Software Activation**.

   Window **Software activation** opens.
5) You get the information about the system to be updated.
6) Select **Location** of the software updates in the area **Software Updates**.
7) Select a **Version** of the software update.
8) Click **Activate**.

3.4.6 System Software and Patch Level

The System Software and Patch Level feature provides the administrators the ability to display and automatically update a billboard-type area with the current release and revision of the application software.

At the time of the initial loading of the application and every time thereafter, a product reflects exactly what application software version, inclusive of base release and patch set level, it is running. Furthermore, if a patch has been somehow removed, the billboard reflects that information easily and clearly.

The updating and downgrading of this area is an automated part of the patchset loading instructions or file. This information can be displayed locally or remotely, and can be printed.

3.4.7 SW Safety During Patching due to HDD Partitions

Two partitions of equal size for each node guarantee the security during patching procedures.

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).

The patching procedures apply to the ‘Active’ partition only.

The software on the Active partition can be backed up prior to patching by copying the entire contents of the Active partition over the Fallback partition.

Should an unrecoverable error happen while patching, one option is to recover by booting off of the Fallback partition that contains the backup.

4 Serviceability - Alarms and Fault Messages

These features provide mechanisms to improve serviceability.

4.1 System Monitoring

System monitoring features deliver information on the system, especially alarms and fault messages automatically from the system components as base for maintenance actions. System processes are written to logging files find out different reasons about erroneous behavior. Audit log logs all important activities performed by the Common Management Platform users.

4.1.1 Concept of the Alarms and Fault Messages

All alarms and faults created by the installed OpenScape systems and OpenScape applications can be centrally monitored in the Common Management Platform. Administrators receive in the Common Management Platform an overview of all alarms and faults, can sort and filter them according to various criteria, and can also acknowledge alarms. In addition, the alarms are optionally forwarded to the OpenScape Voice Fault Management via SNMP traps.

Related concepts

Alarm Destination on page 266
Alarm Logging and Reporting on page 149
Active Alarms and Alarm Logs on page 156
Alarm List on page 164
Fault Logs on page 263

4.1.2 Alarm Logging and Reporting

The alarm reporting feature provides for the reporting of faults detected by the application software executing on OpenScape Voice using the common interface provided by the RTP (Resilient Telco Platform) event manager. Detected faults are identified by RTP events with a priority of 1, 2, or 3 which corresponds to critical, major, and minor alarm levels, respectively.

With an alarm the system generates a notification to an administrator. Alarms could be the result of:

- at least one fault was detected in the system
- exceeding of configured thresholds like number of licenses used, CPU usage, etc.
- a system overload

Each alarm has a status of *Confirmed* or *Unacknowledged*. An alarm with a status of *Unacknowledged* is called an active alarm. If the status of an alarm is changed from *Unacknowledged* to *Confirmed*, the alarm is labeled as *Reset*. If the status of an alarm is changed from *Confirmed* to *Unacknowledged*, the alarm is labeled as *Raised*.

When an alarm is created the status is set to *Unacknowledged* by default. The status is changed to *Confirmed* when a raise condition is detected to be valid. The status can then be changed back to *Unacknowledged* when a reset condition is detected to be valid (automatically reset) or when the alarm is manually reset by the administrator or another external FM system.

Framework alarms raised in the system are sent to alarm destinations. These alarm destinations can be displayed in an alarm destination list. An alarm destination consists of an IP address and a TCP/IP port.

Every 10 minutes, the OpenScape Voice assistant synchronizes with all OSV alarms. If the synchronization fails a relative alarm is raised and appears in the Alarm Log screen. If the synchronization is successful there is no entry in the Alarm Log screen, although an internal error alarm message is registered in the symphonia log.

Related concepts

Concept of the Alarms and Fault Messages on page 149
Active Alarms and Alarm Logs on page 156

4.1.2.1 Alarm Information

All alarms and faults can be centrally monitored in the Common Management Platform (CMP). Administrators receive in the Common Management Platform an overview of all alarms and faults. Alarms are delivered with a list of various criteria. They can be sorted and filtered according to criteria. Administrators can also acknowledge alarms. In addition, the alarms are optionally forwarded to the OpenScape Voice Fault Management via SNMP (Simple Network Management Protocol) traps.

Alarms contain for each entry the following information:

- **Alarm ID**: ID that uniquely identifies an alarm. If you click the alarm ID the settings of the relevant alarm are displayed.
- **Severity:** The severity level shows how critical an alarm is. The following severity levels can be displayed:
  - Critical (red)
  - Major (orange)
  - Minor (yellow)
  - Warning (cyan)
  - Information (blue)
  - Normal (green)
- **Origin**: Specifies which application or which system has raised the alarm (e.g. OpenScape Voice).
- **Managed Resource (alarm source ID**): Describes the entity that has generated the alarm. This is either a Fault Handler or an SNMP Trap Receiver (which makes the connection to the OpenScape Voice system and the OpenScape SBC-Gateway). The entity is referenced by a GUID (Global Unique Identifier). This GUID can be used to identify the alarm source in the system management.
- **Source Name:** Alarms source name
- **Alarm Type**: Designates the type of alarm.

- **Event Type**:specifies the following information about the progress of the alarm:
  - **New**: New Alarm
  - **Reoccurred**: An already existing alarm has reoccurred. The time stamp of the existing alarm is refreshed and the alarm hit count is increased by one.
  - **Confirmed**: An administrator has confirmed the alarm. The alarm is still active.
  - **Unacknowledged**: An administrator has not yet confirmed the alarm. The alarm is still active.
  - **Cleared**: The alarm has been cleared, either by an administrator, by the system, or# by a cyclic cleanup feature.
  - **Unknown**: The type of alarm could not be recognized by the system.
- **Last Occurred**: Date and time when this alarm last occurred.
- **User**: Name or ID of the user associated with the alarm. If the alarm is unconfirmed, the display remains empty.

Other Characteristics

To get more information about the reasons of the alarm, click the **Alarm ID**:

- General tab: This displays additional notes that have been entered for the selected alarm
- Description tab: This shows you a more detailed description of the selected alarm.

4.1.2.2 Alarm Types

Each alarm is mapped to an alarm type by RTP configuration files. The RTP keeps all alarm summary information per category, which can be queried via CLI and SNMP.

The alarm categories used and supported by the OpenScape Voice system are:

- Communication
- Processing
- Service
- Equipment
- Database
- Security
- Indication

4.1.2.3 Alarm Type: Communication

A failed communication link with another network element is reported as a communication alarm, such as:

- Authentication Server
- Media Gateway (SIP)
- Billing Server (CDR FTP site)
- Threshold crossing alert of communication failures with single endpoints (SIP phone).

System Specific Information

Generally, communication alarms are automatically cleared.

4.1.2.4 Alarm Type: Processing

Processing error alarms are mainly software alarms, such as:

- Process did not start, could not initialize or could not change, or crashed
- Software errors
- Call processing/signaling errors
- Corrupted, missing or unknown messages or parameters
- Provisioning, downloading problems
- Timer expiration
- Resource problems (files, disk partition, timers)
- Billing errors
- Overload

System Specific Information

Many of these alarms are reported as threshold crossing alarms. Processing alarms can either be cleared manually or automatically by the system after an extended period of non-occurrence.

4.1.2.5 Alarm Type: Service

Service alarms report problems related to:

- Plug-In Card
  - Ethernet
  - SCSI
- Power Supply
- Disk
- Fan
- Complete Node
- Ethernet Link
- Ethernet LinkGroup (Bonding Driver)

System Specific Information

Generally, equipment alarms are automatically cleared.

The OpenScape Voice system detects hardware troubles using the Intelligent Platform Management Interface (IPMI) supported by the hardware platform. When IPMI shows a fault condition, depending on the severity, one of the following traps:

- hiQHardwareFailureTrap
- hiQSevereHardwareTrap
- hiQVerySevereHardwareFailureTrap

are generated. When IPMI shows that the fault condition is over, a hiQHardwareInServiceTrap is generated. The faulty hardware component is shown in the FaultyObject parameter of the SNMP trap.

4.1.2.6 Alarm Type: Equipment

A failed hardware component or link is reported as an equipment alarm, such as:

- Plug-In Card
  - Ethernet
  - SCSI
- Power Supply
- Disk
- Fan
- Complete Node
- Ethernet Link
- Ethernet LinkGroup (Bonding Driver)

System Specific Information

Generally, equipment alarms are automatically cleared.

The OpenScape Voice system detects hardware troubles using the Intelligent Platform Management Interface (IPMI) supported by the hardware platform. When IPMI shows a fault condition, depending on the severity, one of the following traps:

- hiQHardwareFailureTrap
- hiQSevereHardwareTrap
- hiQVerySevereHardwareFailureTrap

are generated. When IPMI shows that the fault condition is over, a hiQHardwareInServiceTrap is generated. The faulty hardware component is shown in the FaultyObject parameter of the SNMP trap.

4.1.2.7 Alarm Type: Database

This category contains database alarms that are reported by the SolidTechdatabase, such as:

- Act - Standby operation
- Backup
- Interface/connections to database
- Data corruption.

System Specific Information

In most cases, database alarms must be manually cleared.

4.1.2.8 Alarm Type: Security

This category contains security alarms, such as:

- Login failures
- Packets rejected due to filtering rules (failed security policy). This may need to be integrated with TCA counts.
- Security policy negotiation failures (cryptographic settings, wrong keys)

- RTP login failures
- Database connection login failures
- Inconsistency between active and default profiles for users "root" and "srx".

System Specific Information

Generally, security alarms are automatically cleared.

Other Characteristics

Alarm categories that are not used by the OpenScape Voice system, but are used by the RTP are: Environment, MIB, and Indeterminate. Indeterminate is used by OpenScape Voice for global alarm clearance events only

4.1.2.9 Alarm Type: Indication

Alarms of this type notify the administrator of important changes which do not need immediate attention, but may impact call processing in the future.

This alarm type comprises information about:

- Protection Switch (node, process, link)
- Disabled System function
  - locked audit
  - locked log file
  - disabled/filtered alarm reporting

System Specific Information

These alarms are automatically cleared.

Other Characteristics

Alarm categories that are not used by the OpenScape Voice system, but are used by the RTP are: Environment, MIB, and Indeterminate. Indeterminate is used by OpenScape Voice for global alarm clearance events only.

4.1.2.10 Alarm Severities

The importance of alarms and events and alarms is classified by the parameter severity.

The kinds of severity:

- Critical
  - service severely impacted
  - requires timely repair
- Major
  - requires timely repair
  - no or little service impact
  - loss of redundancy

- Minor
  - no service impact
  - case for deferred maintenance
  - requires offline analysis
- Warning
  - non-alarmed event, but still reported via SNMP traps
  - no clearance event necessary
  - corrective action in connection with scheduled maintenance
- Information
  - non-alarmed event
  - no clearance event necessary
- Clear / Normal
  - Alarm clearance event

4.1.2.11 How to View Alarms of a Device

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to **Common Management Platform**.
   Enter user name and password.
2) Select the domain from **Domain** selection list.
3) Navigate to **Maintenance** > **Inventory** > **Nodes & Applications** > **Nodes**.
4) Click on a Node/Device Name.

   The Node/Device **Dashboard** opens.

   An alarm summary of the active alarms for the device/node is displayed as part of the dashboard. The list shows the numbers of Critical, Major, Minor alarms and Warnings. The list cannot be edited - it is just available to view.
5) To obtain more information on the active alarms navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active**.
6) If alarms available: Click on the relative Alarm ID to get the alarm details.

4.1.2.12 How to View All Alarms

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to **Common Management Platform**.
   Enter user name and password.
2) Select the domain from **Domain** selection list.

3) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active**.

The **Active Alarms** window opens and displays one page of all the active alarms.

4.1.3 Active Alarms and Alarm Logs

Active Alarms are the alarm events that report to the administrator any problematic event. Alarms can be generated by the Symphonia Frameworks' Fault Handler Service when internal faults are detected or from external devices such as OpenScape Voice clusters sending traps to an SNMP Alarm Receiver in the CMP.

The alarms that have not been acknowledged or cleared are considered as active. When an alarm is detected by the administrator, he/she will take the appropriate maintenance action. This may result in acknowledging and/or clearing the alarm from the CMP.

Alarms only remain in the Active Alarm List for 7 days. After 7 days they are moved to the Alarm Log, where the become considered as alarm history. Alarms only remain in the Alarm Log for two weeks.

If an alarm is cleared then it is directly moved to the Alarm Log. If an alarm is simply marked as acknowledged by the administrator, then it remains on the active alarm list, but a copy is created in the alarm log for tracking the alarms' changing state.

A synchronization method runs on the CMP to ensure that the alarms reported by external devices (like OpenScape Voice nodes) are always in agreement with the Active Alarm List. In particular, if a trap was lost that reported an alarm clearance from the external server, the CMP Alarm List and external server will be in agreement after the next Alarm Synchonization.

The following details are provided on the Active Alarm List for each alarm listed:

- ID

  that uniquely identifies an alarm.
- Severity

  The severity level shows how critical an alarm is. The following severity levels can be displayed:

  – Critical (red)
  – Major (orange)
  – Minor (yellow)
  – Warning (cyan)
  – Information (blue)
  – Normal (green)
- Alarm Type

  Designates the type of alarm.
- Origin

  Specifies which application or which system has raised the alarm (e. g. OpenScape Voice).

- Managed Resource (alarm source ID)

  Describes the entity that has generated the alarm. This is either the Fault Handler or an external device such as OpenScape Voice system or OpenScape SBC gateway.
- Last Occurrence

  Date and time when this alarm last occurred.
- Acknowledged Status

  Indicates whether the alarm was set to an acknowledged status by an administrator.
- User

  Name or ID of the user associated with the alarm. If the alarm has not been acknowlegded, this display remains empty. If it was acknowledged, the administrator name is set as the User (administrator@system).
- Hit Count

  Shows how many times an identical alarm has been received since the last acknowledge action for that alarm.

Double-click on an individual alarm in the Active Alarm List yields more information about an alarm.

- General Tab

  Under the General Tab, the same information described in the Active List is presented in a tabular form.
- Description Tab

  Under the Description Tab, more information about the alarm is provided
- Notes Tab

  Under the Notes tab, there are additional notes that have been entered for the selected alarm
- Related Faults Tab

  Under the Related Faults tab, is a list of all the faults that caused the selected alarm. This is usually blank for alarms from external devices, but if the alarm was raised by the Fault Handler, where many different faults can trigger the same alarm, all the faults will be listed here.

NOTICE:

Place your mouse on top of each item on the list for a few seconds in order to view the whole name of:

Alarm Type, Managed Resource, Alarm Source Name

Related concepts

Concept of the Alarms and Fault Messages on page 149
Alarm Logging and Reporting on page 149

4.1.3.1 Active Alarms

In the Common Management Platform you can manage all alarms currently active in the system. All currently active alarms are displayed. In addition, an

overview shows the number of currently active alarms of a particular severity (e. g. Critical, Major, Minor, ...). Through selection of an alarm you can get alarm details.

The following Alarm Details are provided:

Below **General tab** the following information is given:

- **Alarm ID**

  that uniquely identifies an alarm.
- **Severity**

  The severity level shows how critical an alarm is. The following severity levelscan be displayed:

  – Critical (red)
  – Major (orange)
  – Minor (yellow)
  – Warning (cyan)
  – Information (blue)
  – Normal (green)
- **Origin**

  Specifies which application or which system has raised the alarm (e. g. OpenScape Voice).
- **Managed Resource (alarm source ID)**

  Describes the entity that has generated the alarm. This is either a Fault Handler or an SNMP Trap Receiver (which makes the connection to the OpenScape Voice system and the OpenScape SBC). The entity is referenced by a GUID (Global Unique Identifier). This GUID can be used to identify the alarm source in the system management.
- **Source Name:** Alarms source name
- **Alarm Type:**

  Designates the type of alarm.
- **Last Occurred**

  Date and time when this alarm last occurred.
- **Status**

  Indicates whether the alarm was confirmed by an administrator or whether it has not yet been confirmed.
- **Hit Count**

  Shows how many times an alarm has been triggered since the last acknowledge action.
- **User**

  Name or ID of the user associated with the alarm. If the alarm is unconfirmed the display remains empty.

When clicking on an Alarm ID, an Alarm Details window opens with several tabs providing more information about the alarm.

Below **Description tab** the following information is given:

- This shows you a more detailed description of the selected alarm.

Below **Notes tab** the following information is given:

- This displays additional notes that have been entered for the selected alarm.

Below **Related Faults tab** the following information is given:

- This shows a list of all faults that have caused a selected alarm.

4.1.3.2 How to Display Active Alarms

How to display Active Alarms

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.
   - A list of all active alarms currently active in the selected domain appears in the work area.

   NOTICE:

   Maybe you can’t see any alarms: Check the area **Advanced** for applied filters.

   NOTICE:

   Clicking on menu items of the alarm table in the window **Active alarms** sorts the sequence of entries.

2) Click on the **Alarm ID** of the desired alarm.

   NOTICE:

   Check your rights to be authorised to look at all alarms.

   The dialog with the associated information opens.
3) Click the tabs **General**, **Description**, **Notes** or **Related Faults** to get alarm details.

   NOTICE:

   Place your mouse on top of each item on the list for a few seconds in order to view the whole name of:

   Alarm Type, Managed Resource, Alarm Source Name

4.1.3.3 How to Set a Filter for Active Alarms

The filter feature allows you to search for specific active alarms by defining search criteria in a filter. Once a filter is selected only specific active alarms matching the criteria defined in the filter selected will be displayed. This reduces

the total number of active alarms displayed and makes it easier to find a specific alarm or group of alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

A list of all active alarms currently active in the selected domain appears in the work area.

2) Click **Advanced**.

A dialog showing the filter settings is displayed.

3) Click on the tab **General**.

4) Select an option in the area **Date**:

- **All**: All alarms are displayed.
- **After Date**: Only the alarms after the specified date are displayed
- **Before date**: Only the alarms before the specified date are displayed
- **Between dates**: Only the alarms within the specified date range are displayed.

5) Select an option in the area **User**:

- All users: All alarms of all users are displayed.
- Current user <user ID>: The alarms of the user currently logged in are displayed.

6) Select an option in the area **Alarm ID**:

- All: All alarms are displayed.
- Within alarm ID range: Only the alarms within the specified alarm ID range are displayed.

7) Click on the tab **Severity**.

a) In the area **Severity** deactivate the alarm categories which are not to be displayed.

b) In the area **Acknowledge Status** deactivate the alarm categories which are not to be displayed.

8) Click on the tab **Origin**.

9) Deactivate the systems for which the alarms are not to be displayed in the area **Origin**.

10) Click on the tab **Managed Resources**.

a) Deactivate the option **Disable filtering by resource** to filter the active alarms based on resources.

b) Mark the checkboxes of the resources the active alarms of which you want to display.

11) Click on the **Alarms Source Name** tab

a) Deactivate the option **Disable filtering by source** to filter the active alarms based on alarm sources.

b) Mark the checkboxes of the sources the active alarms of which you want to display.

12) Click **Apply** .

The active alarms list/alarm log only displays the alarms that correspond to the filter settings made.

4.1.3.4 How to Change Filter for Active Alarms

How to change Filter for Active Alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Click **Advanced**.

   A dialog showing the filter settings is displayed.
3) Apply changes to the filter settings.
4) Click **Apply**

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

4.1.3.5 How to Delete a Filter for Active Alarms

How to clear a filter for active Alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Click **Show All**.

The Filter field displays **No filter applied** and the list of active alarms contains all currently active alarms again.

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

4.1.3.6 Masked Alarms

To restrict the list of alarms you can mask individually selected alarms. This means that you can “hide” less important alarms, for example. These alarms are still present but they are no longer shown in the list of alarms.

Related tasks

How to Mask an Alarm on page 162

How to Display Masked Alarms on page 162

4.1.3.7 How to Mask an Alarm

How to mask an Alarm:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms / Alarm IDs you want to mask.
3) Click **Mask ID**.

The alarms with the selected Alarm IDs are masked and no longer visible in the active alarm list.

Related concepts

Masked Alarms on page 162

4.1.3.8 How to Display Masked Alarms

How to display masked alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Click **Show Masked**.

   The list shows alarms that are masked and the **Show Masked** button changes to **Show Unmasked** .

3) To unmask alarms displayed tick the relative checkbox and click **Unmask ID**.

Related concepts

Masked Alarms on page 162

4.1.3.9 How to Confirm Alarms

If you have verified an alarm or want to notify the system or other administrators that you are dealing with rectifying the fault, you can confirm this alarm. If an active alarm is confirmed, a copy of the alarm is automatically generated in the alarm log. Furthermore, the alarm stays in the list of active alarms to allow the tracking of its processing

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms you want to acknowledge.
3) Click **Acknowledge** button.

   The **Acknowledge** window opens. In the field **Add a note** you can enter information.
4) Continue with **Save**.

In the active alarms list the status of the selected alarms changes to a green dot in the column **Acknowledged** and your user ID is entered in the **User** column.

4.1.3.10 How to Cancel an Alarm Acknowledgement

You can cancel the confirmation for confirmed alarms.#How to cancel the confirmation for an active alarm:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.

2) Select the checkboxes of the alarms those acknowledgements you want to cancel.

NOTICE:

Only select those alarm confirmations that have the status *Acknowledged* in the column Acknowledged Status.

---

3) Click **Unacknowledge**.

The active alarms list the confirmation status of the selected alarms changes to Unacknowledged and the user ID is deleted in the **User** column.

4.1.3.11 How to Clear Alarms

If the fault for an alarm has been rectified or the alarm is no longer active for any other reason, you can clear the alarm.# If an active alarm is deleted, the alarm is automatically moved to the alarm log# and removed from the list of active alarms.#How to remove an alarm from the active alarms list:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms you want to delete.
3) Click **Clear**.

The selected alarms are deleted and no longer displayed in the active alarm list.

4.1.4 Alarm List

Alarm list is a collection of all possible alarms in OpenScape Voice.

Listed alarms are described with reason which may be responsible for raising. Under headline Maintenance Procedure a first instruction for repair actions is given.

Related concepts

Concept of the Alarms and Fault Messages on page 149

4.1.4.1 Alarm hiPathSIPCounterAboveHighThld

The event counter has exceeded the high alarm threshold for the type identified by FaultyObject.

Maintenance Procedure

If this event is unexpected, user should intervene to determine the cause of processing failures.

4.1.4.2 Alarm hiPathSIPCounterAboveLowThld

The event counter has exceeded the low alarm threshold for the type identified by FaultyObject.

Maintenance Procedure

If this event is unexpected, user should intervene to determine the cause of processing failures.

4.1.4.3 Alarm hiPathSIPCounterBelowThld

The event counter is now below the threshold allowed for the type identified by FaultyObject.

Maintenance Procedure

No action is needed.

4.1.4.4 Alarm hiqAccountDeletedTrap

Alarms were previously reported, indicating that the specified account has been inactive and subsequently disabled. The account was still not used and has now been deleted.

Maintenance Procedure

Manually clear the alarm.

4.1.4.5 Alarm hiQAccountDisabledTrap

The specified login account has not been used recently and may be deleted in the future.

Maintenance Procedure

Login to the account periodically if the account is still needed. Delete the account if no longer needed and manually clear this alarm.

4.1.4.6 Alarm hiQAccountInactiveTrap

The specified login account has not been used recently and may be disabled in the future.

Maintenance Procedure

Login to the account periodically if the account is still needed. Delete the account if no longer needed and manually clear this alarm.

4.1.4.7 Alarm hiQAucUscFileSeqNumberErrorTrap

The CDR file sequence number may be incorrect. This is caused by a database read or write error.

Maintenance Procedure

Check the status of the database.

Check sequence numbers of billing files. If numbers are in sequence and no apparent database errors, clear the alarm manually.

4.1.4.8 Alarm hiQAucUscLocalSecStorageOk

Secondary storage of CDR billing data is OK on this node.

Maintenance Procedure

This is a clearing alarm.

4.1.4.9 Alarm hiQAucUscPriStorNotPossibleTrap

Primary storage of CDR billing data is no longer possible on this node. This may be caused by lack of disk space or the cdr disk partition is not writable.

Maintenance Procedure

Check the status of the CDR disk partition for this node. Check space available and that it is writable.

4.1.4.10 Alarm hiQAucUscPriStorOkTrap

Primary storage of CDR billing data is possible on this node.

Maintenance Procedure

This is a clearing alarm.

4.1.4.11 Alarm hiQAucUscSecStorNotPossibleTrap

Secondary storage of CDR billing data is no longer possible on this node. This may be caused by lack of disk space or the CDR disk partition is not writable.

Maintenance Procedure

Check the status of the CDR disk partition for this node. Check space available and that it is writable.

4.1.4.12 Alarm hiQAucUscServerTxCdrTrap

The Usage Collection server has failed to send the CDR file to the FTP site.

Maintenance Procedure

Check FTP configuration between active CDR handler node and billing server. Check space available on billing server and that it is writable.

4.1.4.13 Alarm hiQAudAvailDiskSpBelowCritThld

The available space in a file system / disk partition is the space usable by non-superuser. The rest of the space is either used or reserved for superuser. The available space in a database depends on the type of database.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

---

4.1.4.14 Alarm hiQAudAvailDiskSpBelowMajorThld

The available space in a file system / disk partition is the space usable by non-superuser. The rest of the space is either used or reserved for superuser. The available space in a database depends on the type of database.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated

with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

---

4.1.4.15 Alarm hiQAudAvailDiskSpBelowMinorThld

The available space in a file system / disk partition is the space usable by non-superuser. The rest of the space is either used or reserved for superuser. The available space in a database depends on the type of database.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

---

4.1.4.16 Alarm hiQAudCpuUtilAboveCritThld

The current cpu utilization is too high. CPU utilization checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will then be issued.

Maintenance Procedure

Verify whether this is a temporary peak situation or a permanent one. You can check the CPU use between audit checks using the `sar` command, for example "`sar -u 10 15`". If the situation persists, the system may be equipped with too few CPUs for your purposes, audit thresholds may be configured too low for your needs or there may be processes consuming too much CPU time, for example looping processes. Identify those processes using the command ps repeatedly, for example: `ps -e -o` "pid=" `-o` "time=" `-o` "comm" " sort -t" `-k1` and compare the results.

Check whether processes with changed "time" values work correctly. For OSV software processes, events or process traces (RTT or RTP traces) may help to identify code blocks over which a process is continuously looping. For further analysis of any process the commands strace may be of use.

If a process is looping, it may help to restart it. If it is consuming a lot of cpu time without obviously looping and it seems to work correctly, this is most likely normal behaviour. If the problem persists for longer than 5 minutes,

Run the following command as the root user to collect system information:

```
RapidStat -c
```

Provide the output file that is generated to the next level of support.

4.1.4.17 Alarm hiQAudCpuUtilAboveMajorThld

The current CPU utilization is high. CPU utilization checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will then be issued.

Maintenance Procedure

Verify whether this is a temporary peak situation or a permanent one. You can check the CPU use between audit checks using the `sar` command, for example "`sar -u 10 15`". If the situation persists, the system may be equipped with too few CPUs for your purposes, audit thresholds may be configured too low for your needs or there may be processes consuming too much CPU time, for example looping processes. Identify those processes using the command ps repeatedly, for example: `ps -e -o` "pid=" `-o` "time=" `-o` "comm" " sort -t" `-k1` and compare the results.

Check whether processes with changed "time" values work correctly. For OSV software processes, events or process traces (RTT or RTP traces) may help to identify code blocks over which a process is continuously looping. For further analysis of any process the commands strace may be of use.

If a process is looping, it may help to restart it. If it is consuming a lot of cpu time without obviously looping and it seems to work correctly, this is most likely normal behaviour. If the problem persists for longer than 5 minutes,

Run the following command as the root user to collect system information:

```
RapidStat -c
```

Provide the output file that is generated to the next level of support.

4.1.4.18 Alarm hiQAudCpuUtilAboveMinorThld

The current CPU utilization is high. CPU utilization checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will then be issued.

Maintenance Procedure

Verify whether this is a temporary peak situation or a permanent one. You can check the CPU use between audit checks using the `sar` command, for example "`sar -u 10 15`". If the situation persists, the system may be equipped with too few CPUs for your purposes, audit thresholds may be configured too low for your needs or there may be processes consuming too much CPU time, for example looping processes. Identify those processes using the command ps repeatedly, for example: `ps -e -o` "pid=" `-o` "time=" `-o` "comm" " sort -t" `-k1` and compare the results.

Check whether processes with changed "time" values work correctly. For OSV software processes, events or process traces (RTT or RTP traces) may help to identify code blocks over which a process is continuously looping. For further analysis of any process the commands strace may be of use.

If a process is looping, it may help to restart it. If it is consuming a lot of cpu time without obviously looping and it seems to work correctly, this is most likely normal behaviour. If the problem persists for longer than 5 minutes,

Run the following command as the root user to collect system information:

```
RapidStat -c
```

Provide the output file that is generated to the next level of support.

4.1.4.19 Alarm hiQAudCpuUtilBelowThreshTrap

The current CPU utilization is now below the configured threshold.

Maintenance Procedure

This is a clearing alarm.

4.1.4.20 Alarm hiQAudCpuUtilChangedTrap

The current CPU utilization has changed but is still high.

Maintenance Procedure

Refer to the accompanying alarm that is subsequently reported.

4.1.4.21 Alarm hiQAudCpuUtilTrap

Information about the current CPU utilization.

Maintenance Procedure

This is a clearing alarm.

4.1.4.22 Alarm hiQAudFileGroupSizeChanged1Trap

This alarm indicates that the size of the given file group has changed but is still too high.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

4.1.4.23 Alarm hiQAudFileGroupSizeChanged2Trap

This alarm indicates that the size of the given file group has changed but is still too high.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

4.1.4.24 Alarm hiQAudFileGroupSizeChanged3Trap

This alarm indicates that the size of the given file group has changed but is still too high.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

---

4.1.4.25 Alarm hiQAudFileGroupSizeChanged4Trap

This alarm indicates that the size of the given file group has changed but is still too high.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

4.1.4.26 Alarm hiQAudFileGrpAboveCritThld

The size of the given file group is monitored by the audit process and has exceeded the maximum configured size.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

4.1.4.27 Alarm hiQAudFileGrpAboveMajorThld

The size of the given file group is monitored by the audit process and has exceeded the configured limit for a major alarm.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

---

4.1.4.28 Alarm hiQAudFileGrpAboveMinorThld

The size of the given file group is monitored by the audit process and has exceeded the configured limit for a minor alarm.

Maintenance Procedure

When an alarm for high disk space usage for a file group is reported, the RTP Recovery Manager should normally try to clean up older files associated with the file group but if the problem persists, manual deletion of files may be necessary.

A filesystem backup should be performed prior to removing files.

The following list shows each of the file groups and associated files to review and potentially remove.

coreFiles: /unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

traceFiles: /unisphere/srx3000/srx/40/trace/*

saTraceFiles: /unisphere/srx3000/srx/sa_trace/*

rtpTmpFiles: /unisphere/srx3000/srx/40/tmp/*

rtpLogFiles: /unisphere/srx3000/srx/40/log/*

snmpdmLogFile: /log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

mailcheck: /var/spool/mail/*

ovlDataFiles: /log/ovlData/*

IMPORTANT:

Only log files should removed from the corresponding folders. Non logfile files like “DBSnapshot”, “createRTP ”, “perf”, “updateRTP”, etc should NOT be removed

4.1.4.29 Alarm hiQAudFileGrpBelowThreshTrap

The size of the given file group has previously been reported to have grown beyond alarming threshold. The size of this file group has shrunk again below this limitation.

Maintenance Procedure

This is a clearing alarm.

4.1.4.30 Alarm hiQAudFileSystemAboveMinTrap

This alarm indicates that the available File system or database space has increased above the configured minimum threshold level.

Maintenance Procedure

This is a clearing alarm.

4.1.4.31 Alarm hiQAudFileSystemBelowMin1Trap

File system (disk partition) or database space has changed but it is still below the configured minimum level.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

Check if it is possible to get more space by removing files in a file system or unneeded tables in a database. Some databases may allow to grow its size during runtime and redistribute its tables.

The following file systems (disk partitions) have specific thresholds assigned, however, all file systems are checked against a default set of thresholds.

rootFs: /

cdrFs: /cdr

tpaFs: /tpa

softwareFs: /software

Execute the following command to determine disk usage per file system:

df -k

This will show the percentage of disk space per file system that is currently in use. Any partition showing 90% usage or greater should be analyzed to determine which files can be removed.

A filesystem backup should be performed prior to removing files.

Files in the following list should be automatically maintained and removed as necessary but they can be manually removed if needed.

/unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

/unisphere/srx3000/srx/40/trace/*

/unisphere/srx3000/srx/sa_trace/*

/unisphere/srx3000/srx/40/tmp/*

/unisphere/srx3000/srx/40/log/*

/log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

/var/spool/mail/*

/log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

4.1.4.32 Alarm hiQAudFileSystemBelowMin2Trap

File system (disk partition) or database space has changed but it is still below the configured minimum level. File system or database space error messages with a lower severity level than critical concerning the given data space will be automatically cleared with this abatement so that only the new critical alarm is left open.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

Check if it is possible to get more space by removing files in a file system or unneeded tables in a database. Some databases may allow to grow its size during runtime and redistribute its tables.

The following file systems (disk partitions) have specific thresholds assigned, however, all file systems are checked against a default set of thresholds.

rootFs: /

cdrFs: /cdr

tpaFs: /tpa

softwareFs: /software

Execute the following command to determine disk usage per file system:

df -k

This will show the percentage of disk space per file system that is currently in use. Any partition showing 90% usage or greater should be analyzed to determine which files can be removed.

A filesystem backup should be performed prior to removing files.

Files in the following list should be automatically maintained and removed as necessary but they can be manually removed if needed.

/unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

/unisphere/srx3000/srx/40/trace/*

/unisphere/srx3000/srx/sa_trace/*

/unisphere/srx3000/srx/40/tmp/*

/unisphere/srx3000/srx/40/log/*

/log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

/var/spool/mail/*

/log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

4.1.4.33 Alarm hiQAudFileSystemBelowMin3Trap

File system (disk partition) or database space has changed but it is still below the configured minimum level. File system or database space error messages with a lower severity level than critical concerning the given data space will be automatically cleared with this abatement so that only the new critical alarm is left open.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

Check if it is possible to get more space by removing files in a file system or unneeded tables in a database. Some databases may allow to grow its size during runtime and redistribute its tables.

The following file systems (disk partitions) have specific thresholds assigned, however, all file systems are checked against a default set of thresholds.

rootFs: /

cdrFs: /cdr

tpaFs: /tpa

softwareFs: /software

Execute the following command to determine disk usage per file system:

df -k

This will show the percentage of disk space per file system that is currently in use. Any partition showing 90% usage or greater should be analyzed to determine which files can be removed.

A filesystem backup should be performed prior to removing files.

Files in the following list should be automatically maintained and removed as necessary but they can be manually removed if needed.

/unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

/unisphere/srx3000/srx/40/trace/*

/unisphere/srx3000/srx/sa_trace/*

/unisphere/srx3000/srx/40/tmp/*

/unisphere/srx3000/srx/40/log/*

/log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

/var/spool/mail/*

/log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

4.1.4.34 Alarm hiQAudFileSystemBelowMin4Trap

File system (disk partition) or database space has changed but it is still below the configured minimum level. File system or database space error messages with a lower severity level than critical concerning the given data space will be automatically cleared with this abatement so that only the new critical alarm is left open.

The partitions can be:

/ - root partition

/cdr - call detail records

/enterprise - OSV applications

/global - used for malicious call trace and OMS measurements

/home - Solid Database, user accounts

/log - OSV and application log files

/opt - third-party software, RTP

/software - pstack, trace, backup file storage

/tmp - temporary files

/tpa - ticket pool

/unisphere - OSV software

/var - operating system logs, RPMs

Maintenance Procedure

Check if it is possible to get more space by removing files in a file system or unneeded tables in a database. Some databases may allow to grow its size during runtime and redistribute its tables.

The following file systems (disk partitions) have specific thresholds assigned, however, all file systems are checked against a default set of thresholds.

rootFs: /

cdrFs: /cdr

tpaFs: /tpa

softwareFs: /software

Execute the following command to determine disk usage per file system:

df -k

This will show the percentage of disk space per file system that is currently in use. Any partition showing 90% usage or greater should be analyzed to determine which files can be removed.

A filesystem backup should be performed prior to removing files.

Files in the following list should be automatically maintained and removed as necessary but they can be manually removed if needed.

/unisphere/srx3000/srx/core* , /unisphere/srx3000/srx/40/core/...

/unisphere/srx3000/srx/40/trace/*

/unisphere/srx3000/srx/sa_trace/*

/unisphere/srx3000/srx/40/tmp/*

/unisphere/srx3000/srx/40/log/*

/log/snmpd.log (requires /etc/init.d/snmpdm stop, then start)

/var/spool/mail/*

/log/ovlData/*

In addition, review the /tmp directory to determine if there are any files that can be safely deleted.

4.1.4.35 Alarm hiQAuditStartingTrap

The Audit Manager process is starting.

Maintenance Procedure

This is a clearing alarm. No action is needed.

4.1.4.36 Alarm hiQAudOSProcInstanceNotRunningTrap

No instance of the named process type is currently running.

Maintenance Procedure

Normally the system automatically recovers by restarting the failed process. If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available. The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in /log, e.g. as the root user:

`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

\"RapidStat -c\" can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.37 Alarm hiQAudOSProcNotRunningTrap

The named process is no longer running.

Maintenance Procedure

Normally the system automatically recovers by restarting the failed process. If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available. The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in /log, e.g. as the root user:

`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

\"RapidStat -c\" can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.38 Alarm hiQAudProcessNotRunningMajorTrap

The named process is currently not running.

Maintenance Procedure

Normally the system automatically recovers by restarting the failed process. If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available. The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in /log, e.g. as the root user:

`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.39 Alarm hiQAudProcessNotRunningMinorTrap

The named process is currently not running.

Maintenance Procedure

Normally the system automatically recovers by restarting the failed process. If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available. The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in /log, e.g. as the root user:

`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.40 Alarm hiQAudProcessRunningTrap

The named process is now running (again).

Maintenance Procedure

This is a clearing alarm.

4.1.4.41 Alarm hiQAudProcHeapAboveCritThld

The heap size of the named process is extremely high, i.e. the program has been dynamically allocating more and more memory but freeing only part of it again or none at all. This may be caused by a program error (memory leakage) or large input data from outside the process or a configuration error where the heap size limit for the named process is set too low in the audit configuration.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.42 Alarm hiQAudProcHeapAboveMajorThld

The heap size of the named process is high, i.e. the program has been dynamically allocating more and more memory but freeing only part of it again or none at all. This may be caused by a program error (memory leakage) or large input data from outside the process or a configuration error where the heap size limit for the named process is set too low in the audit configuration.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.43 Alarm hiQAudProcHeapAboveMinorThld

The heap size of the named process is high, i.e. the program has been dynamically allocating more and more memory but freeing only part of it again or none at all. This may be caused by a program error (memory leakage) or large input data from outside the process or a configuration error where the heap size limit for the named process is set too low in the audit configuration.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.44 Alarm hiQAudProcHeapSizeChanged1Trap

This is an information that the break size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.45 Alarm hiQAudProcHeapSizeChanged2Trap

This is an information that the break size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.46 Alarm hiQAudProcHeapSizeChanged3Trap

This is an information that the break size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.47 Alarm hiQAudProcHeapSizeChanged4Trap

This is an information that the break size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly. If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the OpenScape Voice application using the 'srxctl' tool.

4.1.4.48 Alarm hiQAudProcHeapSizeOkTrap

The break size of the process is now below the configured threshold.

Maintenance Procedure

This is a clearing alarm.

4.1.4.49 Alarm hiQAudProcNotRunningCriticalTrap

The named process is currently not running.

Maintenance Procedure

Normally the system automatically recovers by restarting the failed process. If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available. The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in /log, e.g. as the root user:

`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.50 Alarm hiQAudProcStackAboveCritThld

The program stack of the named process is extremely high. This might be caused by a programming error within recursive function calls, recursively defined input data or a configuration error where the stack size limit for the named process is set too low in audit configuration.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.51 Alarm hiQAudProcStackAboveMajorThld

The program stack of the named process is high. This might be caused by a programming error within recursive function calls, recursively defined input data or a configuration error where the stack size limit for the named process is set too low in audit configuration.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.52 Alarm hiQAudProcStackAboveMinorThld

The program stack of the named process is high. This might be caused by a programming error within recursive function calls, recursively defined input data or a configuration error where the stack size limit for the named process is set too low in audit configuration.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.53 Alarm hiQAudProcStackSizeChanged1Trap

This is an information that the stack size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.54 Alarm hiQAudProcStackSizeChanged2Trap

This is an information that the stack size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.55 Alarm hiQAudProcStackSizeChanged3Trap

This is an information that the stack size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.56 Alarm hiQAudProcStackSizeChanged4Trap

This is an information that the stack size of the named process has changed but is still too high.

Maintenance Procedure

To avoid main memory shortage and for reinitialization of the program, the RTP recovery manager may stop and restart the process, if configured accordingly.

If the problem occurs frequently, provide a trace for the named process together with the corresponding events.

If redundancy is available or if there is no callp traffic one potential repair step is to stop and restart the Openscape Voice application using the 'srxctl' tool.

4.1.4.57 Alarm hiQAudProcStackSizeOkTrap

The stack size of the process is now below the configured threshold.

Maintenance Procedure

This is a clearing alarm.

4.1.4.58 Alarm hiQAudSemUtilAboveCritThld

The number of currently used semaphores is high. Semaphore utilization checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of semaphores, some functions of the system may fail in an unpredictable manner.

Maintenance Procedure

Check whether this is a temporary peak situation or a permanent one. Either wait for the next check cycles or use the command ipcs to check the semaphore utilization over some time between audit checks, e.g. calling '`ipcs -s`' as user 'root' will get information about which user created (field owner of ipcs output) how many (field nsems) semaphores.

If the situation persists, the system may be configured with too few semaphores for your purposes, audit thresholds may be configured too low and have to be adapted by the system integrator to the special needs of your system or there may be processes which needlessly use up semaphores. Identifying processes which needlessly use up semaphores, is not an easy task and may require special knowledge about the processes.

It would be helpful if there were information about semaphore usage during normal operation to compare to. Consult the RTP Installation and Configuration Guide about resource usage of each component.

Run '`RapidStat -c`' to collect additional data.

Provide all data to the next level of support.

4.1.4.59 Alarm hiQAudSemUtilAboveMajorThld

The number of currently used semaphores is high. Semaphore utilization checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of semaphores, some functions of the system may fail in an unpredictable manner.

Maintenance Procedure

Check whether this is a temporary peak situation or a permanent one. Either wait for the next check cycles or use the command ipcs to check the semaphore utilization over some time between audit checks, e.g. calling '`ipcs -s`' as user 'root' will get information about which user created (field owner of ipcs output) how many (field nsems) semaphores.

If the situation persists, the system may be configured with too few semaphores for your purposes, audit thresholds may be configured too low and have to be adapted by the system integrator to the special needs of your system or there may be processes which needlessly use up semaphores. Identifying processes which needlessly use up semaphores, is not an easy task and may require special knowledge about the processes.

It would be helpful if there were information about semaphore usage during normal operation to compare to. Consult the RTP Installation and Configuration Guide about resource usage of each component.

Run '`RapidStat -c`' to collect additional data.

Provide all data to the next level of support.

4.1.4.60 Alarm hiQAudSemUtilAboveMinorThld

The number of currently used semaphores is high. Semaphore utilization checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of semaphores, some functions of the system may fail in an unpredictable manner.

Maintenance Procedure

Check whether this is a temporary peak situation or a permanent one. Either wait for the next check cycles or use the command ipcs to check the semaphore utilization over some time between audit checks, e.g. calling '`ipcs -s`' as user 'root' will get information about which user created (field owner of ipcs output) how many (field nsems) semaphores.

If the situation persists, the system may be configured with too few semaphores for your purposes, audit thresholds may be configured too low and have to be adapted by the system integrator to the special needs of your system or there may be processes which needlessly use up semaphores. Identifying processes which needlessly use up semaphores, is not an easy task and may require special knowledge about the processes.

It would be helpful if there were information about semaphore usage during normal operation to compare to. Consult the RTP Installation and Configuration Guide about resource usage of each component.

Run '`RapidStat -c`' to collect additional data.

Provide all data to the next level of support.

4.1.4.61 Alarm hiQAudSemUtilBelowThreshTrap

The number of currently used semaphores is now below the configured threshold.

Maintenance Procedure

This is a clearing alarm.

4.1.4.62 Alarm hiQAudSemUtilChangedTrap

The number of currently used semaphores has changed but is still above the configured thresholds.

Maintenance Procedure

The semaphore utilization has changed and will be reported by another event. Reference that event for details.

4.1.4.63 Alarm hiQAudSemUtilTrap

Information about the current semaphore utilization.

Maintenance Procedure

This is a clearing alarm.

4.1.4.64 Alarm hiQAudShMemUtilBelowThreshTrap

The number of currently used shared memory IDs is now below the configured threshold.

Maintenance Procedure

This is a clearing alarm.

4.1.4.65 Alarm hiQAudShMemUtilChangedTrap

The number of currently used shared memory IDs has changed, but is still above the configured thresholds.

Maintenance Procedure

The shared memory utilization has changed and will be reported by another event. Reference that event for details.

4.1.4.66 Alarm hiQAudShMemUtilTooAboveCritThld

The number of currently used shared memory segments is high. Shared memory segment checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of shared memory, some functions of the system may fail in an unpredictable manner.

Maintenance Procedure

Check whether this is a temporary peak situation or a permanent one.

Use the command `ipcs`, for example: `ipcs -mp` as user "root" will get information about which process created (field cpid) and uses which shared memory segment.

If the situation persists, the system may be configured with too few segments for your purposes, audit thresholds may be configured too low or there may be processes which needlessly use up shared memory segments.

Information about process specific shared memory segment usage during normal operation may help. Identify processes which create a lot of segments using the above command.

Compare total numbers of segments, numbers of segments created by the same process (cpid), compare with "normal" values.

Check whether these processes work correctly. For RTP node manager controlled processes events or traces may help to identify code blocks over which a process is continuously looping. Use strace for further analysis. It may help to restart a looping process.

4.1.4.67 Alarm hiQAudShMemUtilTooAboveMajorThld

The number of currently used shared memory segments is high. Shared memory segment checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of shared memory, some functions of the system may fail in an unpredictable manner.

Maintenance Procedure

Check whether this is a temporary peak situation or a permanent one.

Use the command `ipcs`, for example: `ipcs -mp` as user "root" will get information about which process created (field cpid) and uses which shared memory segment.

If the situation persists, the system may be configured with too few segments for your purposes, audit thresholds may be configured too low or there may be processes which needlessly use up shared memory segments.

Information about process specific shared memory segment usage during normal operation may help. Identify processes which create a lot of segments using the above command.

Compare total numbers of segments, numbers of segments created by the same process (cpid), compare with "normal" values.

Check whether these processes work correctly. For RTP node manager controlled processes events or traces may help to identify code blocks over which a process is continuously looping. Use strace for further analysis. It may help to restart a looping process.

4.1.4.68 Alarm hiQAudShMemUtilTooAboveMinorThld

The number of currently used shared memory segments is high. Shared memory segment checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of shared memory, some functions of the system may fail in an unpredictable manner.

Maintenance Procedure

Check whether this is a temporary peak situation or a permanent one.

Use the command `ipcs`, for example: `ipcs -mp` as user "root" will get information about which process created (field cpid) and uses which shared memory segment.

If the situation persists, the system may be configured with too few segments for your purposes, audit thresholds may be configured too low or there may be processes which needlessly use up shared memory segments.

Information about process specific shared memory segment usage during normal operation may help. Identify processes which create a lot of segments using the above command.

Compare total numbers of segments, numbers of segments created by the same process (cpid), compare with "normal" values.

Check whether these processes work correctly. For RTP node manager controlled processes events or traces may help to identify code blocks over which a process is continuously looping. Use strace for further analysis. It may help to restart a looping process.

4.1.4.69 Alarm hiQAudShMemUtilTrap

Information about the current shared memory ID utilization.

Maintenance Procedure

This is a clearing alarm.

4.1.4.70 Alarm hiQAudSwapFrequencyAboveCritThld

The RTP Audit swap frequency detector has detected high swap out activities. This may affect the system's performance and compromise your running RTP if these activities continue. The average number of swapped pages per second over the last 10 seconds is derived from /proc/vmstat (pswpout) and rounded up to the next integer. This alarm is raised when that value reaches a configured threshold.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.71 Alarm hiQAudSwapFrequencyAboveMajorThld

The RTP Audit swap frequency detector has detected high swap out activities. This may affect the system's performance and compromise your running RTP if these activities continue. The average number of swapped pages per second over the last 10 seconds is derived from /proc/vmstat (pswpout) and rounded up to the next integer. This alarm is raised when that value reaches a configured threshold.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.72 Alarm hiQAudSwapFrequencyAboveMinorThld

The RTP Audit swap frequency detector has detected high swap out activities. This may affect the system's performance and compromise your running RTP if these activities continue. The average number of swapped pages per second over the last 10 seconds is derived from /proc/vmstat (pswpout) and rounded up to the next integer. This alarm is raised when that value reaches a configured threshold.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.73 Alarm hiQAudSwapFrequencyAboveWarningThld

The RTP Audit swap frequency detector has detected high swap out activities. This may affect the system's performance and compromise your running RTP if these activities continue. The average number of swapped pages per second over the last 10 seconds is derived from /proc/vmstat (pswpout) and rounded up to the next integer. This alarm is raised when that value reaches a configured threshold.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.74 Alarm hiQAudSwapFrequencyBelowThreshTrap

Current swap frequency below the configured threshold.

Maintenance Procedure

Nothing to do.

4.1.4.75 Alarm hiQAudSwapFrequencyUtilChangedTrap

The swap frequency has changed but is still too high.

Maintenance Procedure

No action is needed. The current swap level will be reported with another event.

4.1.4.76 Alarm hiQAudSwapFrequencyUtilTrap

Information about the current swap frequency.

Maintenance Procedure

Nothing to do.

4.1.4.77 Alarm hiQAudSwapSpaceAboveCritThld

The system is running out of swap space. Swap space checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of swap space, the system may experience unpredictable failures, including a system crash.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.78 Alarm hiQAudSwapSpaceAboveMajorThld

The system is running out of swap space. Swap space checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of swap space, the system may experience unpredictable failures, including a system crash.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.79 Alarm hiQAudSwapSpaceAboveMinorThld

The system is running out of swap space. Swap space checks are done periodically by audit and if this is a temporary situation which no longer exists during the next check cycle, a clearing event will be issued. If the system runs out of swap space, the system may experience unpredictable failures, including a system crash.

Maintenance Procedure

There may be a high demand for resident memory or there may be processes which needlessly consume swap space, e.g. processes with a memory leak. Information about process sizes during normal operation can be used to compare with the existing process sizes.

Save the output from the command '`top -b -n 5 >top.txt`' and look for processes with high RES (resident memory) values. Search for events in the RtpDumpLog output from the audit process about stack, break, or heap size of these processes and if a process was reported, it may help to restart it.

Run the command '`RapidStat -c`'.

Provide the collected data to the next level of support.

4.1.4.80 Alarm hiQAudSwapUtilBelowThreshTrap

Current swap space use is now below the configured threshold.

Maintenance Procedure

This is a clearing alarm.

4.1.4.81 Alarm hiQAudSwapUtilChangedTrap

The swap space utilization has changed but is still too high.

Maintenance Procedure

The swap space usage has changed and will be reported by another event. Reference that event for details.

4.1.4.82 Alarm hiQAudSwapUtilTrap

Information about the current swap space utilization.

Maintenance Procedure

This is a clearing alarm.

4.1.4.83 Alarm hiQCacHighThreshTrap

This event is used to report a CaC specific major alarm.

Maintenance Procedure

No action is needed.

4.1.4.84 Alarm hiQCacLowThreshTrap

This event is used to report a CaC specific clear alarm.

Maintenance Procedure

No action is needed.

4.1.4.85 Alarm hiQCritOperationModeStateChange

The Operation Mode has transitioned to a new state.

Shown below are the possible state values. A non-Normal Operation Mode describes the node operation while the cluster x-channel is unavailable. Scenarios are split mode upgrade, HW failure and network failure. SMU indicates operation modes for Split Mode Upgrade.

- OM_STATE_INITIAL
- OM_STATE_INITIAL_PROMPT
- OM_STATE_NORMAL

  Both nodes and x-channel are active or one node is down and the active partner knows it.
- OM_STATE_NORMAL_C

  Node is booting with the partner already active and accessible.
- OM_STATE_STANDALONE_PRIMARY

  No active virtual partner IP address, partner status is unknown
- OM_STATE_STANDALONE_SYNC

  Same as OM_STATE_STANDALONE_PRIMARY but synchronizing from partner, partner node is shutting down
- OM_STATE_STANDALONE

  No new provisioning, no active partner virtual IP address, the x-channel is down and the Survival Authority has not yet selected the primary node
- OM_STATE_STANDALONE_SECONDARY

  No new provisioning, no active virtual partner IP address, partner status is unknown
- OM_STATE_SHUTTING_DOWN

  Synchronizing with partner and preparing to restart.
- OM_STATE_SPLIT - SMU

  Start of upgrade state, no x-channel

- OM_STATE_STOP_DB - SMU

  No changes to the OSV database, including subscriber controlled input. The database is backed up and installed at the new software load
- OM_STATE_SYNC - SMU

  Call data synchronization to the new side
- OM_STATE_NO_TRAFFIC - SMU

  IP addresses are blocked, no call processing
- OM_STATE_INIT - SMU

  Re-initialization of transient data in preparation for fallback
- OM_STATE_BEFORE_TRAFFIC - SMU

  No active OSV applications
- OM_STATE_TRAFFIC - SMU

  IP addresses active
- OM_STATE_UNKNOWN

  State of the partner node if the x-channel is down

Maintenance Procedure

If the OSV is in one of the following operation modes:

OM_STATE_STANDALONE

OM_STATE_STANDALONE_PRIMARY

OM_STATE_STANDALONE_SECONDARY

OM_STATE_UNKNOWN

then communication with the partner node via the x-channel has been lost and the network connectivity problem must be identified and corrected. Once communication with the partner node has been re-established, the operation mode of each node should transition back to the normal operation mode.

The operation mode pair of the two nodes shall never be:

Primary - Primary or Primary - Normal

In such a scenario the OSV database is in state primary-alone on both nodes without being able to synchronize data. This will lead to inconsistent and corrupted data. Change the operation mode via CLI or CMP to Primary - Secondary or reboot one of the nodes.

The SMU modes apply to operation modes during Split Mode Upgrade and the operation state should transition back to normal when the upgrade is complete.

4.1.4.86 Alarm hiQForeignProcessTrap

Foreign process launch attempt has been identified.

Maintenance Procedure

No need to repair. This alarm can only be cleared manually.

4.1.4.87 Alarm hiQGlobalCommsEstablishedTrap

This event is used to report that communication with the element specified in the faultyObject has been established.

Maintenance Procedure

No action is needed.

4.1.4.88 Alarm hiQGlobalCommsOperationalTrap

The specified communication link is fully operational.

Maintenance Procedure

This is a clearing alarm.

4.1.4.89 Alarm hiQGlobalCriticalLossOfCommsTrap

This trap is used to report a critical loss of communication alarm.

Communication alarms are reported for example for:

- Survival Authority

  A failure to communicate with the Survival Authority
- Maintenance Controllers (RSA, IMM, iRMC)

  This communication failure can cause a failure to remove the partner node from service in the event of a partner node failure, creating the potential for a split-brain scenario where both nodes are independently active and writing to the database.
- RSH

  A background test of SSH connectivity between two nodes of a cluster has failed, causing reduced maintenance functionality.
- ENUM

  A failure to communicate with the ENUM server has occurred and could cause reduced call processing functionality.
- GUT_MEDIA_SERVER

  The media server is operationally blocked.
- XDM:SIP Endpoint

  A proxy failed to respond to a SIP Invite and subsequent audit, resulting in call processing failures to and from that proxy.
- Billing Server

  A communication failure has occurred between the OSV and one or more billing servers. This can cause a loss of billing (call detail recording) records.
- Router

  A linkDown SNMP trap was received for a tunnel. The IP address of the router is specified in the faultyObject.

Maintenance Procedure

Some of the frequent causes of communication errors and potential solutions are shown below.

Survival Authority: Communication alarms with the Survival Authority may be due to an incorrect configuration in the OSV, network failure, or due to the Survival Authority itself.

Verify the correct Survival Authority IP address is configured by displaying the value for the RTP parameter:

`Srx/Main/SurvivalAuthority`

Maintenance controllers (RSA, IMM, iRMC): Communication failures with the maintenance controllers are typically due to misconfiguration on the OSV, incorrect configuration of the maintenance controller, or incorrect cabling. First verify that the Ethernet port for the maintenance controller is properly connected to the Admin network. As root, run \"`/unisphere/srx3000/callp/bin/rsaConfig -l`\" to list the current configuration settings of the maintenance controller. The settings can be compared with the rsa_* parameters contained in the file `/etc/hiq8000/node.cfg` as well as the configuration found in `/opt/SMAW/SMAWrtp/SMAWhaext/sa_ipmi.cfg`, which overrides some of the original settings in node.cfg. Alternatively, you can just run rsaConfig without any parameter to reprogram the maintenance controller.

RSH - This should rarely happen but can be caused by corruption or misconfiguration of the ssh security keys for either the root or srx users as well as a failure of one of the ssh daemons. Contact the next level of support.

NTP: The command \"`ntpq -pn`\" can be used to show the status of the ntp server.

Most communication alarms will be cleared automatically when communication is restored with the partner.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure.

4.1.4.90 Alarm hiQGlobalFuncAvailTrap

The system function identified in the faulty object is available.

Maintenance Procedure

This is a clearing alarm.

4.1.4.91 Alarm hiQGlobalFuncUnavailTrap

The system function identified by the faulty object is not available.

An alarm with faultyObject = Function: Registration Audit/Timer is reported when the registration audit cannot set a timer to periodically check for expired registrations.

An alarm with faultyObject = PacketFilter is raised if the Security Manager could not successfully apply all of the packet filter rules. In that case, the final

DROP rules may not be applied, possibly allowing network access to ports or IP addresses that should be blocked.

An alarm with faultyObject = NTP/NTPDaemon is raised if the ntp daemon is down or no NTP servers are configured.

An alarm with faultyObject = NTP/Sync is raised if the OSV system time is not synchronized with an NTP server.

Maintenance Procedure

For an alarm with faultyObject = Function: Registration Audit/Timer, the system will recover alone as soon as a new registration comes in and timers become available again. If new registrations are not expected it does not matter whether the licenses audit is running or not. Regarding the registration audit it can be disabled and reenabled again to trigger it.

For an alarm with faultyObject = PacketFilter, use the CLI to display all packet filter rules. Run `iptables -vnL` to obtain the current filter rules that are applied. Obtain the `/etc/hosts` file and `/log/HiqLogSwError.log`. Provide all information to the next level of support.

For an alarm with faultyObject = NTP/NTPDaemon, execute `systemctl status ntpd` to determine if the daemon is running. Use the date command to verify that the system time is within 11 minutes of the actual time. If not, follow the documented procedures for changing the system time on the OSV. If it is, execute `systemctl restart ntpd` to attempt to restart the NTP daemon and note any problems reported. Check `/var/ntp/ntp.log` for errors.

For an alarm with faultyObject = NTP/Sync, execute `ntpq -pn` to show the status of each time source. Verify that the configured time sources are correct and on a cluster, verify that one of the sources is the partner node IP address. Verify that UDP port 123 is not blocked by a firewall.

If problem persists, contact the next level of support.

4.1.4.92 Alarm hiQGlobalMajorLossOfCommsTrap

This event is used to report a major loss of communication alarm.

Communication alarms are reported for example for:

- Survival Authority - A failure to communicate with the Survival Authority
- Maintenance Controllers (RSA, IMM, iRMC) - This communication failure can cause a failure to remove the partner node from service in the event of a partner node failure, creating the potential for a split-brain scenario where both nodes are independently active and writing to the database.
- RSH - A background test of SSH connectivity between two nodes of a cluster has failed, causing reduced maintenance functionality.
- ENUM - A failure to communicate with the ENUM server has occurred and could cause reduced call processing functionality.
- GUT_MEDIA_SERVER - The media server is operationally blocked.
- XDM:SIP Endpoint - A proxy failed to respond to a SIP Invite and subsequent audit, resulting in call processing failures to and from that proxy.
- Billing Server - A communication failure has occurred between the OSV and one or more billing servers. This can cause a loss of billing (call detail recording) records.

- Router - A linkDown SNMP trap was received for a tunnel. The IP address of the router is specified in the faultyObject.

Maintenance Procedure

Some of the frequent causes of communication errors and potential solutions are shown below.

- Survival Authority:

  Communication alarms with the Survival Authority may be due to an incorrect configuration in the OSV, network failure, or due to the Survival Authority itself. Verify the correct Survival Authority IP address is configured by displaying the value for the RTP parameter:
- Srx/Main/SurvivalAuthority
- Maintenance controllers (RSA, IMM, iRMC):

  Communication failures with the maintenance controllers are typically due to misconfiguration on the OSV, incorrect configuration of the maintenance controller, or incorrect cabling. First verify that the Ethernet port for the maintenance controller is properly connected to the Admin network. As root, run \"/unisphere/srx3000/callp/bin/rsaConfig -l\" to list the current configuration settings of the maintenance controller. The settings can be compared with the rsa_* parameters contained in the file /etc/hiq8000/node.cfg as well as the configuration found in /opt/SMAW/SMAWrtp/SMAWhaext/sa_ipmi.cfg, which overrides some of the original settings in node.cfg. Alternatively, you can just run rsaConfig without any parameter to reprogram the maintenance controller.
- RSH

  This should rarely happen but can be caused by corruption or misconfiguration of the ssh security keys for either the root or srx users as well as a failure of one of the ssh daemons. Contact the next level of support.
- NTP:

  The command \"ntpq -pn\" can be used to show the status of the ntp server.

Most communication alarms will be cleared automatically when communication is restored with the partner.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure.

4.1.4.93 Alarm hiQGlobalMinorLossOfCommsTrap

This event is used to report a minor loss of communication alarm.

Communication alarms are reported for example for:

- Survival Authority - A failure to communicate with the Survival Authority
- Maintenance Controllers (RSA, IMM, iRMC) - This communication failure can cause a failure to remove the partner node from service in the event of a partner node failure, creating the potential for a split-brain scenario where both nodes are independently active and writing to the database.
- RSH - A background test of SSH connectivity between two nodes of a cluster has failed, causing reduced maintenance functionality.

- ENUM - A failure to communicate with the ENUM server has occurred and could cause reduced call processing functionality.
- GUT_MEDIA_SERVER - The media server is operationally blocked.
- XDM:SIP Endpoint - A proxy failed to respond to a SIP Invite and subsequent audit, resulting in call processing failures to and from that proxy.
- Billing Server - A communication failure has occurred between the OSV and one or more billing servers. This can cause a loss of billing (call detail recording) records.
- Router - A linkDown SNMP trap was received for a tunnel. The IP address of the router is specified in the faultyObject.

Maintenance Procedure

Some of the frequent causes of communication errors and potential solutions are shown below.

- Survival Authority:

  Communication alarms with the Survival Authority may be due to an incorrect configuration in the OSV, network failure, or due to the Survival Authority itself. Verify the correct Survival Authority IP address is configured by displaying the value for the RTP parameter:
- Srx/Main/SurvivalAuthority
- Maintenance controllers (RSA, IMM, iRMC):

  Communication failures with the maintenance controllers are typically due to misconfiguration on the OSV, incorrect configuration of the maintenance controller, or incorrect cabling. First verify that the Ethernet port for the maintenance controller is properly connected to the Admin network. As root, run \"/unisphere/srx3000/callp/bin/rsaConfig -l\" to list the current configuration settings of the maintenance controller. The settings can be compared with the rsa_* parameters contained in the file /etc/hiq8000/node.cfg as well as the configuration found in /opt/SMAW/SMAWrtp/SMAWhaext/sa_ipmi.cfg, which overrides some of the original settings in node.cfg. Alternatively, you can just run rsaConfig without any parameter to reprogram the maintenance controller.
- RSH

  This should rarely happen but can be caused by corruption or misconfiguration of the ssh security keys for either the root or srx users as well as a failure of one of the ssh daemons. Contact the next level of support.
- NTP:

  The command \"ntpq -pn\" can be used to show the status of the ntp server.

Most communication alarms will be cleared automatically when communication is restored with the partner.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure.

4.1.4.94 Alarm hiQGlobalMsgQueueAboveHighThld

The number of elements in the specified queue has exceeded a defined threshold limit. The Internal Resource Manager will report this alarm if the internal message queue exceeds a predefined limit.

Maintenance Procedure

If problem persists, contact the next level of support.

4.1.4.95 Alarm hiQGlobalMsgQueueAboveLowThld

The number of elements in the specified queue has exceeded a defined threshold limit. The Internal Resource Manager will report this alarm if the internal message queue exceeds a predefined limit.

Maintenance Procedure

If problem persists, contact the next level of support.

4.1.4.96 Alarm hiQGlobalMsgQueueAboveMedThld

The number of elements in the specified queue has exceeded a defined threshold limit. The Internal Resource Manager will report this alarm if the internal message queue exceeds a predefined limit.

Maintenance Procedure

If problem persists, contact the next level of support.

4.1.4.97 Alarm hiQGlobalMsgQueueBelowThld

The number of elements in the specified queue is below the defined threshold limit.

Maintenance Procedure

No action is needed.

4.1.4.98 Alarm hiQGlobalProcAbnormalTermTrap

The process exited due to an error condition.

Maintenance Procedure

Check logs with category PROC_EXIT in `HiQLogAlert.log`.

The process that exited should automatically be restarted.

If problem persists, contact the next level of support.

4.1.4.99 Alarm hiQGlobalProcessAliasGrpAvail

At least one process servicing the RTP message queue for the given alias group is now running.

Maintenance Procedure

This is a clearing alarm.

4.1.4.100 Alarm hiQGlobalProcessAliasGrpUnavail

All members that service the RTP message queue for the given alias group are unavailable which means that the OSV cluster no longer provides any service associated with this Alias group function.

Maintenance Procedure

Run the command:

```
srxctrl -v
```

to display any look for any processes that are not currently running.

Attempt to restart any processes that are not running.

If problem persists, contact the next level of support.

4.1.4.101 Alarm hiQGlobalProcessInitActiveTrap

The process has started successfully.

Maintenance Procedure

This is a clearing alarm.

4.1.4.102 Alarm hiQGlobalProcPartialInitFailTrap

The process encountered an error during initialization but not severe enough to keep the process from running.

Maintenance Procedure

Check the log file `hiQLOgAlert` for logged intitialization failures of the process reported with category PROC_INIT_FAILURE.

Contact the next level of support.

4.1.4.103 Alarm hiQGlobalProcSevereInitFailTrap

The process encountered an error during initialization failure and cannot continue.

Maintenance Procedure

The process should exit and be automatically restarted. If problem persists, contact the next level of support.

4.1.4.104 Alarm hiQGlobalResourceExceedLimitTrap

The resource specified in the faultyObject parameter of the alarm has exceeded a defined limit.

Possible faultyObject values include:

- RapidStat

  RapidStat has run a test and determined that a Warning or Error condition exists that should be investigated and corrected.
- SIP

  The SIP signaling manager has multiple tables in shared memory and each has a maximum size that cannot be increased. When the table capacity has reached a threshold (e.g.: 80%), the SIP Resource Monitor will raise an alarm, specifying the table name in the faultyObject.

Maintenance Procedure

Varies, depending on the resourcethat is specified in the faultyObject parameter of the alarm.

Possible faultyObject values include:

- RapidStat: Run RapidStat -s to generate a report containing the current status of the OSV. The reason for the alarm should be displayed.
- SIP - Report to the next level of support to investigate the capacity issue. When the capacity level of the table given in the faultyObject is below a threshold (e.g.: 75%), the alarm will be automatically cleared.

4.1.4.105 Alarm hiQGlobalResourceWithinLimitTrap

The specified resource usage is within the defined limit.

Maintenance Procedure

No action is needed.

4.1.4.106 Alarm hiQGlobalSevereDegradedCommsTrap

The specified communication link is either congested or operating in a degraded state. If this alarm is reported with a faultyObject containing CAC Group, backup routing policy has been activated for the specified CAC group.

Maintenance Procedure

Verify the specified communication link is configured properly and the communication path is available.

If the faultyObject contains a CAC Group, the alarm will be automatically cleared when the primary routing policy has been reinstated.

4.1.4.107 Alarm hiQHardwareFailureTrap

This event is used to report a hardware-related minor alarm.

Listed below are the typically reported hardware alarms along with the frequency that the status of each is checked:

- Ethernet link or Bonding Group is inactive (checked every minute)
- RAID storage failures (checked every 5 minutes)
- Disk errors (checked in real-time)
- Platform Hardware errors (Temperature, Voltage, etc) detected via IPMI sensors (checked every 30 seconds)

Maintenance Procedure

The action to take depends on the specific alarm.

Ethernet - verify that an Ethernet cable is connected correctly between the specified port on the OSV and the interfacing network device.

RAID - use the mpt-status command to view the status of the logical RAID volume and associated physical drives and correct any problem that is identified.

Disk - A disk error specifying a device (e.g.: /sda3) is due to either a total failure of the RAID array or RAID controller or a failure of a disk drive not configured in a RAID array. This indicates that data is corrupt or lost on the primary storage device and must be corrected as soon as possible. If this occurs in a cluster configuration, the node with the disk error should be automatically shut down. If not, attempt to gracefully shut down the node with the failure.

IPMI hardware sensors:

- Temperature - verify that the server has proper cooling and ventilation.
- Power Supply Unit - verify that the redundant power supply, if applicable, is plugged in and connected to a power source.

If the problem is not easily identified and corrected, contact the next level of support. Some alarms may require support from the hardware manufacturer.

4.1.4.108 Alarm hiQHardwareInServiceTrap

This event is used to clear a hardware-related alarm.

Listed below are the typically reported hardware alarms along with the frequency that the status of each is checked:

- Ethernet link or Bonding Group is inactive (checked every minute)
- RAID storage failures (checked every 5 minutes)
- Disk errors (checked in real-time)
- Platform Hardware errors (Temperature, Voltage, etc) detected via IPMI sensors (checked every 30 seconds)

Maintenance Procedure

No action is needed.

4.1.4.109 Alarm hiQImportantFuncUnavailTrap

The system function identified by the faulty object is not available.

An alarm with faultyObject = Function: Registration Audit/Timer is reported when the registration audit cannot set a timer to periodically check for expired registrations

An alarm with faultyObject = PacketFilter is raised if the Security Manager could not successfully apply all of the packet filter rules. In that case, the final DROP rules may not be applied, possibly allowing network access to ports or IP addresses that should be blocked.

An alarm with faultyObject = NTP/NTPDaemon is raised if the ntp daemon is down or no NTP servers are configured.

An alarm with faultyObject = NTP/Sync is raised if the OSV system time is not synchronized with an NTP server.

An alarm with faultyObject = <user>/<profile file name> is raised if the OSV node’s active profile does not match the default profile for user "root" or user "srx".

Maintenance Procedure

For an alarm with faultyObject = Function: Registration Audit/Timer, the system will recover alone as soon as a new registration comes in and timers become available again. If new registrations are not expected it does not matter whether the licenses audit is running or not. Regarding the registration audit it can be disabled and reenabled again to trigger it.

For an alarm with faultyObject = PacketFilter, use the CLI to display all packet filter rules. Run `iptables -vnL` to obtain the current filter rules that are applied. Obtain the `/etc/hosts` file and `/log/HiqLogSwError.log`. Provide all information to the next level of support.

For an alarm with faultyObject = NTP/NTPDaemon, execute `systemctl status ntpd` to determine if the daemon is running. Use the date command to verify that the system time is within 11 minutes of the actual time. If not, follow the documented procedures for changing the system time on the OSV. If it is,

execute `systemctl restart ntpd` to attempt to restart the NTP daemon and note any problems reported. Check `/var/ntp/ntp.log` for errors.

For an alarm with faultyObject = NTP/Sync, execute ntpq -pn to show the status of each time source. Verify that the configured time sources are correct and on a cluster, verify that one of the sources is the partner node IP address. Verify that UDP port 123 is not blocked by a firewall.

For an alarm with faultyObject = Function: <root | srx>/<filename>, Function: Unavailable, the alarm is raised when a user (root or srx) logs into the node using any client like ssh or CMP/Assistant and the Pluggable Authentication Module (PAM) identifies a difference between the active profile and the default profile of the node. The PAM immediately restores the active profile from the default profile and saves the bad active profile file in the same directory after appending a timestamp to the file name. The PAM automatically clears the alarm without the need for user intervention.

If problem persists, contact the next level of support.

4.1.4.110 Alarm hiQLicenseCountMismatchTrap

The license count is different between the two nodes of the hiQ cluster for the type identified by FaultyObject. The system's behavior will change if the node that is currently hosting the primary license manager process fails or if the process itself is shut down and the secondary becomes the primary. This happens during rolling upgrade, for example. All license functionality uses the values in the primary license manager, the secondary is only used to take over if the primary is shut down. If there is a license count mismatch then license violations may be detected in error during upgrades or if a node failure occurs. This in turn may cause licensing restrictions to be activated in error.

Maintenance Procedure

If the condition is not resolved automatically, administrative action is necessary.

4.1.4.111 Alarm hiQLicenseCountOkTrap

The number of assigned licenses is now within the limit allowed by the number of licenses.

Maintenance Procedure

This is a clearing alarm.

4.1.4.112 Alarm hiQLicenseCountSyncTrap

The license count is now the same between the two nodes of the OpenScape Voice cluster for the type identified by faultyObject.

Maintenance Procedure

No action is needed.

4.1.4.113 Alarm hiQLicenseRestoreTrap

The LicenseManager started and determined that 72 or more hours had passed since the last license database use.

Maintenance Procedure

No action is needed.

4.1.4.114 Alarm hiQLicenseSessionCountOKTrap

The number of license sessions is now below the warning threshold for the type identified by FaultyObject.

Maintenance Procedure

No action is needed.

4.1.4.115 Alarm hiQLicenseSessionsTrap

The number of license sessions exceeds the warning threshold for the type identified by FaultyObject.

Maintenance Procedure

Install additional licenses, or reduce the number currently assigned within the product.

4.1.4.116 Alarm hiQLicensesExceededTrap

The number of assigned licenses has exceeded the number of activated licenses for the type identified by FaultyObject. This indicates that a license violation has been detected and will be recorded for the current 24-hour period. After 10 such violations have been detected then licensing enforcement is activated and will activate related licensing restrictions, for example, disabling the creation of new elements associated with the specified license type.

Maintenance Procedure

Install additional licenses, or reduce the number currently assigned within the product.

4.1.4.117 Alarm hiQMajorOperationModeStateChange

The Operation Mode has transitioned to a new state.

Shown below are the possible state values. SMU indicates operation modes for Split Mode Upgrade.

- OM_STATE_INITIAL
- OM_STATE_INITIAL_PROMPT

- OM_STATE_NORMAL

  Both nodes and x-channel are active or one node is down and the active partner knows it.
- OM_STATE_NORMAL_C

  Node is booting with the partner already active and accessible.
- OM_STATE_STANDALONE_PRIMARY

  No active virtual partner IP address, partner status is unknown
- OM_STATE_STANDALONE_SYNC

  Same as OM_STATE_STANDALONE_PRIMARY but synchronizing from partner, partner node is shutting down
- OM_STATE_STANDALONE

  No new provisioning, no active partner virtual IP address, the x-channel is down and the Survival Authority has not yet selected the primary node
- OM_STATE_STANDALONE_SECONDARY

  No new provisioning, no active virtual partner IP address, partner status is unknown
- OM_STATE_SHUTTING_DOWN

  Synchronizing with partner and preparing to restart.
- OM_STATE_SPLIT - SMU

  Start of upgrade state, no x-channel
- OM_STATE_STOP_DB - SMU

  No changes to the OSV database, including subscriber controlled input. The database is backed up and installed at the new software load
- OM_STATE_SYNC - SMU

  Call data synchronization to the new side
- OM_STATE_NO_TRAFFIC - SMU

  IP addresses are blocked, no call processing
- OM_STATE_INIT - SMU

  Re-initialization of transient data in preparation for fallback
- OM_STATE_BEFORE_TRAFFIC - SMU

  No active OSV applications
- OM_STATE_TRAFFIC - SMU

  IP addresses active
- OM_STATE_UNKNOWN

  State of the partner node if the x-channel is down

Maintenance Procedure

If the OSV is in one of the following operation modes:

OM_STATE_STANDALONE

OM_STATE_STANDALONE_PRIMARY

OM_STATE_STANDALONE_SECONDARY

OM_STATE_UNKNOWN

then communication with the partner node via the x-channel has been lost and the network connectivity problem must be identified and corrected. Once communication with the partner node has been re-established, the operation mode of each node should transition back to the normal operation mode.

The operation mode pair of the two nodes shall never be:

Primary - Primary or Primary - Normal

In such a scenario the OSV database is in state primary-alone on both nodes without being able to synchronize data. This will lead to inconsistent and corrupted data. Change the operation mode via CLI or CMP to Primary - Secondary or reboot one of the nodes.

The SMU modes apply to operation modes during Split Mode Upgrade and the operation state should transition back to normal when the upgrade is complete.

4.1.4.118 Alarm hiQMinorOperationModeStateChange

The Operation Mode has transitioned to a new state.

Shown below are the possible state values. A non-Normal Operation Mode describes the node operation while the cluster x-channel is unavailable. Scenarios are split mode upgrade, HW failure and network failure. SMU indicates operation modes for Split Mode Upgrade.

- OM_STATE_INITIAL
- OM_STATE_INITIAL_PROMPT
- OM_STATE_NORMAL

  Both nodes and x-channel are active or one node is down and the active partner knows it.
- OM_STATE_NORMAL_C

  Node is booting with the partner already active and accessible.
- OM_STATE_STANDALONE_PRIMARY

  No active virtual partner IP address, partner status is unknown
- OM_STATE_STANDALONE_SYNC

  Same as OM_STATE_STANDALONE_PRIMARY but synchronizing from partner, partner node is shutting down
- OM_STATE_STANDALONE

  No new provisioning, no active partner virtual IP address, the x-channel is down and the Survival Authority has not yet selected the primary node
- OM_STATE_STANDALONE_SECONDARY

  No new provisioning, no active virtual partner IP address, partner status is unknown
- OM_STATE_SHUTTING_DOWN

  Synchronizing with partner and preparing to restart.
- OM_STATE_SPLIT - SMU

  Start of upgrade state, no x-channel
- OM_STATE_STOP_DB - SMU

  No changes to the OSV database, including subscriber controlled input. The database is backed up and installed at the new software load

- OM_STATE_SYNC - SMU

  Call data synchronization to the new side
- OM_STATE_NO_TRAFFIC - SMU

  IP addresses are blocked, no call processing
- OM_STATE_INIT - SMU

  Re-initialization of transient data in preparation for fallback
- OM_STATE_BEFORE_TRAFFIC - SMU

  No active OSV applications
- OM_STATE_TRAFFIC - SMU

  IP addresses active
- OM_STATE_UNKNOWN

  State of the partner node if the x-channel is down

Maintenance Procedure

If the OSV is in one of the following operation modes:

OM_STATE_STANDALONE

OM_STATE_STANDALONE_PRIMARY

OM_STATE_STANDALONE_SECONDARY

OM_STATE_UNKNOWN

then communication with the partner node via the x-channel has been lost and the network connectivity problem must be identified and corrected. Once communication with the partner node has been re-established, the operation mode of each node should transition back to the normal operation mode.

The operation mode pair of the two nodes shall never be:

Primary - Primary or Primary - Normal

In such a scenario the OSV database is in state primary-alone on both nodes without being able to synchronize data. This will lead to inconsistent and corrupted data. Change the operation mode via CLI or CMP to Primary - Secondary or reboot one of the nodes.

The SMU modes apply to operation modes during Split Mode Upgrade and the operation state should transition back to normal when the upgrade is complete.

4.1.4.119 Alarm hiQNmAliasMembersExceededTrap

The RTP parameter Rtp/Nm/ProcsPerAlias specified the maximal number of members for all aliases. This parameter must suffice for all alias members configured by tcn files or CLI/GUI.

Maintenance Procedure

Contact the next level of support.

4.1.4.120 Alarm hiQNmAliasTableLenExceededTrap

The RTP parameter Rtp/Nm/MaxAliases must be greater or equal to the number of aliases configured by `tcn` files or by the GUI/CLI.

Maintenance Procedure

Contact the next level of support.

4.1.4.121 Alarm hiQNmDbMaxProcGrpExceededTrap

The database contains more `<processes/groups>` than can be handled by the node manager. These entries are ignored by the node manager.

Maintenance Procedure

Check whether the database is installed correctly.

Contact the next level of support.

4.1.4.122 Alarm hiQNmDbTableNotClosedTrap

The database table could not be closed by the node manager.

Maintenance Procedure

Check whether the database is installed correctly and if the table exists.

If problem persists, contact the next level of support.

4.1.4.123 Alarm hiQNmDbTableNotOpenedTrap

The database table could not be opened by the node manager.

Maintenance Procedure

Check whether the database is installed correctly and if the table exists.

4.1.4.124 Alarm hiQNmDbUnreachable1Trap

The database could not be reached from the node manager.

Maintenance Procedure

Check whether the database is installed correctly and running.

The following diagnostics files provide information to analyze the problem:

- The latest snmlog* files in $HOME/$PLID/log.
- solid/RtpSolid.log*
- solid.ini, solmsg.out and solerr.out in $SOLIDDIR.

4.1.4.125 Alarm hiQNmDbUnreachable2Trap

The database could not be reached from the node manager.

Maintenance Procedure

Check whether the database is installed correctly and running.

The following diagnostics files provide information to analyze the problem:

- The latest snmlog* files in $HOME/$PLID/log.
- solid/RtpSolid.log*
- solid.ini, solmsg.out and solerr.out in $SOLIDDIR.

If problem persists, contact the next level of support.

4.1.4.126 Alarm hiQNmDiagnosticErrorTrap

The occurrence of this event means that a process has terminated while acquiring or releasing an RTP queue lock. The RTP fixes any resulting inconsistencies automatically, but the behaviour of the platform should be carefully monitored.

Maintenance Procedure

Observe your RTP platform.

If subsequent errors accumulate, use `srxctrl` to bring the node to state 3 and back to state 4. If this fails, try rebooting the node.

If problem persists, contact the next level of support..

4.1.4.127 Alarm hiQNmNodeDownMsgErrorTrap

When trying to send the NODEDOWN message to the specified node, an error occurred. The NODEDOWN message is very important for an orderly termination of the shutdown.

Maintenance Procedure

RTP failed to send the RTP_MSG_NM_NODEDOWN message.

If this problem persists when the node is stopped, contact the next level of support.

4.1.4.128 Alarm hiQNmNodeMgrSignalRestartTrap

A signal of type `SIGTERM`, `SIGINT` or `SIGQUIT` was sent to the node manager. The pid and possibly the logical name of the sending process can be found in [].

Maintenance Procedure

Check why the signal was sent. This may not be an error if a signal was deliberately sent by a command.

4.1.4.129 Alarm hiQNmNodeMgrStartingTrap

The RTP local node manager is starting on <NodeName>.

Maintenance Procedure

No action is needed.

4.1.4.130 Alarm hiQNmNodeShutdownTrap

Node <node> will be stopped on behalf of process <LogicalName>.

Maintenance Procedure

Nothing to be done.

4.1.4.131 Alarm hiQNmProcessCoreCreatedTrap

The core is found in the directory $HOME/$PLID/core if the core was written by RtpWriteCore(). The process aborted and is normally automatically restarted.

Maintenance Procedure

The generation of core files on the OSV is disabled by default but if this alarm occurs, check the directory $RTP_HOME/40/core for any core files or pstack files. Provide these files to the next level of support.

4.1.4.132 Alarm hiQNmProcessExecvErrorTrap

The binary could not be started since execv returned the errno. If restart is set for the RTP process, RTP will try to start it again.

Maintenance Procedure

Verify that the specified binary exists and has executable permission if the binary was manually modified.

Contact the next level of support.

4.1.4.133 Alarm hiQNmProcessExitedwithCodeTrap

An RTP process terminated unexpectedly. The string in parentheses contains an exit status or signal number. If the exit status is unknown, the process was not a child of the RTP node manager. The event also tells whether the node manager will attempt to restart the process or not.

Maintenance Procedure

Maintenance Procedure

Look up the meaning of the exit status (if any) in the source code or documentation of the binary. This helps to tell why the process failed.

Normally the system automatically recovers by restarting the failed process.

If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available.

The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in `/log`, e.g. as the root user:`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt` and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.134 Alarm hiQNmProcessHealthChkTimeoutTrap

The given process did not answer the healthcheck in time. The RTP healthcheck kills non-reponding processes (e.g. deadlock or endess loops) so that they can be restarted by RTP.

Maintenance Procedure

Check whether the process comes up properly again.

Normally the system automatically recovers by restarting the failed process.

If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available.

The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in `/log`, e.g. as the root user:`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt` and save the output file.

\"RapidStat -c\" can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.135 Alarm hiQNmProcessInitCompleteTrap

The Process <LogicalName> called RtpNmReady() to indicate, that it finished its initialization phase successfully.

Maintenance Procedure

No action is needed.

4.1.4.136 Alarm hiQNmProcessReadyTimeoutTrap

The given process did not inform RTP that it had completed initialization before the configured timeout expired. RTP will attempt to restart the process.

Maintenance Procedure

This is an indication that the process parameters timeUntilReady and restartTimeUntilReady may not be configured correctly.

The command srxqry -v can be used to display the status of all OSV processes and that can be used to verify whether or not the specified process is actually running.

Normally the system automatically recovers by restarting the failed process.

If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available.

The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in `/log`, e.g. as the root user:`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt` and save the output file.

\"RapidStat -c\" can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.137 Alarm hiQNmProcessRestartShortTimeTrap

Process <LogicalName> restarts too soon. To avoid frequent restarts, the node manager will now wait `<number>` seconds, before it tries again to bring the process up.

Maintenance Procedure

Check whether process %s is configured correctly.

Normally the system automatically recovers by restarting the failed process.

If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available.

The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in `/log`, e.g. as the root user:`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt` and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.138 Alarm hiQNmQueueAllocErrorTrap

The process queue of %s could not be allocated, due to problems with shared memory.

Maintenance Procedure

Look up man pages of shmget(), shmat() for a description of errno. Look up man pages of shmget(), shmat() for a description of errno.

Run the command `""top -b -n 1 >top.txt'` to collect further information and provide the output to the next level of support.

4.1.4.139 Alarm hiQNmQueueCorruptedTrap

The queue of the process is not in a consistent state. To avoid further problems the process is killed and should come up with a new clean queue.

Maintenance Procedure

Check whether the process %s comes up again.

Normally the system automatically recovers by restarting the failed process.

If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem. That should only be attempted during periods of low system activity and if redundancy is available.

The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

/`unisphere/srx3000/srx/40/core/`

Save the system log files in /log, e.g. as the root user:

`tar -cvzf logfiles.tar.gz /log/`

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.140 Alarm hiQNmResizeGlobalProcTblTrap

The number of processes on another node has changed due to a node restart.

Maintenance Procedure

This is a problem with shared memory probably due to memory saturation. As a consequence the process table for that node must be resized.

Contact the next level of support.

4.1.4.141 Alarm hiQNodeDownAfterFailedRecovery

Since the reported problem could not be resolved by a node restart, the node is being stopped.

Maintenance Procedure

Contact the next level of support.

4.1.4.142 Alarm hiQNodeRecovery

After a node restart, the problem that triggered the restart has not occurred again within the specified time interval.

Maintenance Procedure

No action is necessary.

4.1.4.143 Alarm hiQNodeRecoveryByRestart

A condition that warrants restarting the node in an attempt to clear an error condition has been detected and the node will now be restarted.

Maintenance Procedure

Reference the associated alarm event that triggered the node restart (e.g.: rolling process restarts).

4.1.4.144 Alarm hiQNodeRecoveryFailed

After a node restart, the problem that triggered the restart occurred again. This alarm is cleared and the node is brought down, raising a different alarm.

Maintenance Procedure

No action is necessary.

4.1.4.145 Alarm hiQNormalOperationMode

The Operation Mode has transitioned to the Normal state.

Shown below are the possible state values. A non-Normal Operation Mode describes the node operation while the cluster x-channel is unavailable. Scenarios are split mode upgrade, HW failure and network failure. SMU indicates operation modes for Split Mode Upgrade.

- OM_STATE_INITIAL
- OM_STATE_INITIAL_PROMPT
- OM_STATE_NORMAL

  Both nodes and x-channel are active or one node is down and the active partner knows it.

- OM_STATE_NORMAL_C

  Node is booting with the partner already active and accessible.
- OM_STATE_STANDALONE_PRIMARY

  No active virtual partner IP address, partner status is unknown
- OM_STATE_STANDALONE_SYNC

  Same as OM_STATE_STANDALONE_PRIMARY but synchronizing from partner, partner node is shutting down
- OM_STATE_STANDALONE

  No new provisioning, no active partner virtual IP address, the x-channel is down and the Survival Authority has not yet selected the primary node
- OM_STATE_STANDALONE_SECONDARY

  No new provisioning, no active virtual partner IP address, partner status is unknown
- OM_STATE_SHUTTING_DOWN

  Synchronizing with partner and preparing to restart.
- OM_STATE_SPLIT - SMU

  Start of upgrade state, no x-channel
- OM_STATE_STOP_DB - SMU

  No changes to the OSV database, including subscriber controlled input. The database is backed up and installed at the new software load
- OM_STATE_SYNC - SMU

  Call data synchronization to the new side
- OM_STATE_NO_TRAFFIC - SMU

  IP addresses are blocked, no call processing
- OM_STATE_INIT - SMU

  Re-initialization of transient data in preparation for fallback
- OM_STATE_BEFORE_TRAFFIC - SMU

  No active OSV applications
- OM_STATE_TRAFFIC - SMU

  IP addresses active
- OM_STATE_UNKNOWN

  State of the partner node if the x-channel is down

Maintenance Procedure

No action is needed.

4.1.4.146 Alarm hiQOperationModeStateChange

The Operation Mode has transitioned to a new state.

Shown below are the possible state values. A non-Normal Operation Mode describes the node operation while the cluster x-channel is unavailable. Scenarios are split mode upgrade, HW failure and network failure. SMU indicates operation modes for Split Mode Upgrade.

- OM_STATE_INITIAL

- OM_STATE_INITIAL_PROMPT
- OM_STATE_NORMAL

  Both nodes and x-channel are active or one node is down and the active partner knows it.
- OM_STATE_NORMAL_C

  Node is booting with the partner already active and accessible.
- OM_STATE_STANDALONE_PRIMARY

  No active virtual partner IP address, partner status is unknown
- OM_STATE_STANDALONE_SYNC

  Same as OM_STATE_STANDALONE_PRIMARY but synchronizing from partner, partner node is shutting down
- OM_STATE_STANDALONE

  No new provisioning, no active partner virtual IP address, the x-channel is down and the Survival Authority has not yet selected the primary node
- OM_STATE_STANDALONE_SECONDARY

  No new provisioning, no active virtual partner IP address, partner status is unknown
- OM_STATE_SHUTTING_DOWN

  Synchronizing with partner and preparing to restart.
- OM_STATE_SPLIT - SMU

  Start of upgrade state, no x-channel
- OM_STATE_STOP_DB - SMU

  No changes to the OSV database, including subscriber controlled input. The database is backed up and installed at the new software load
- OM_STATE_SYNC - SMU

  Call data synchronization to the new side
- OM_STATE_NO_TRAFFIC - SMU

  IP addresses are blocked, no call processing
- OM_STATE_INIT - SMU

  Re-initialization of transient data in preparation for fallback
- OM_STATE_BEFORE_TRAFFIC - SMU

  No active OSV applications
- OM_STATE_TRAFFIC - SMU

  IP addresses active
- OM_STATE_UNKNOWN

  State of the partner node if the x-channel is down

Maintenance Procedure

If the OSV is in one of the following operation modes:

OM_STATE_STANDALONE

OM_STATE_STANDALONE_PRIMARY

OM_STATE_STANDALONE_SECONDARY

OM_STATE_UNKNOWN

then communication with the partner node via the x-channel has been lost and the network connectivity problem must be identified and corrected. Once communication with the partner node has been re-established, the operation mode of each node should transition back to the normal operation mode.

The operation mode pair of the two nodes shall never be:

Primary - Primary or Primary - Normal

In such a scenario the OSV database is in state primary-alone on both nodes without being able to synchronize data. This will lead to inconsistent and corrupted data. Change the operation mode via CLI or CMP to Primary - Secondary or reboot one of the nodes.

The SMU modes apply to operation modes during Split Mode Upgrade and the operation state should transition back to normal when the upgrade is complete.

4.1.4.147 Alarm hiQOvlCongLevelChangeTrap

The Overload Manager is preparing to report a new CPU congestion level. This event will clear the previous CPU congestion level alarm prior to reporting the new level.

Maintenance Procedure

No action is needed.

4.1.4.148 Alarm hiQOvlCongLevelToCL0Trap

The Overload Manager reports that a CPU overload condition no longer exists. The previous congestion level is indicated in the text.

Maintenance Procedure

No measures necessary.

4.1.4.149 Alarm hiQOvlCongLevelToCL1Trap

The congestion level has changed to congestion level 3. This indicates a minor CPU overload situation in the node and may severely degrade performance of the OSV. The previous congestion level is indicated in the text.

Maintenance Procedure

Check whether any unimportant system administrative work on the node can be postponed until the load situation improves.

If the problem persists for longer than 5 minutes, run the following command as the root user to collect system information:

```
RapidStat -c
```

Provide the output file that is generated to the next level of support.

4.1.4.150 Alarm hiQOvlCongLevelToCL2Trap

The congestion level has changed to congestion level 3. This indicates a major CPU overload situation in the node and may severely degrade performance of the OSV. The previous congestion level is indicated in the text.

Maintenance Procedure

Reduce system load as soon as possible by stopping any system administrative work on the node.

If the problem persists for longer than 5 minutes, run the following command as the root user to collect system information:

```
RapidStat -c
```

Provide the output file that is generated to the next level of support.

4.1.4.151 Alarm hiQOvlCongLevelToCL3Trap

The congestion level has changed to congestion level 3. This indicates a severe CPU overload situation in the node and may severely degrade performance of the OSV. The previous congestion level is indicated in the text.

Maintenance Procedure

Reduce system load immediately by stopping any system administrative work on the node.

If the problem persists for longer than 5 minutes, run the following command as the root user to collect system information:

```
RapidStat -c
```

Provide the output file that is generated to the next level of support.

4.1.4.152 Alarm hiQRapidStatErrorsFound

RapidStat has found errors.

Maintenance Procedure

Run RapidStat in status display mode for detailed info.

4.1.4.153 Alarm hiQRapidStatSevereErrorsFound

RapidStat has found severe errors.

Maintenance Procedure

Run RapidStat in status display mode for detailed info.

4.1.4.154 Alarm hiQRapidStatStarting

RapidStat is starting. All potentially reported alarms by a previously run RapidStat are cleared. They will be re-generated if found again.

Maintenance Procedure

No action needed.

4.1.4.155 Alarm hiQRapidStatVerySevereErrorsFound

RapidStat has found severe errors.

Maintenance Procedure

Run RapidStat in status display mode for detailed info.

4.1.4.156 Alarm hiQRapidStatWarningsFound

RapidStat has generated warnings.

Maintenance Procedure

Run RapidStat in status display mode for detailed info.

4.1.4.157 Alarm hiQResourceHighLimitExceeded

The specified resource has exceeded the defined high limit.

Maintenance Procedure

Varies, depending on the resource.

4.1.4.158 Alarm hiQResourceMediumLimitExceeded

The specified resource has exceeded the defined medium limit.

Maintenance Procedure

Varies, depending on the resource.

4.1.4.159 Alarm hiQRollingProcessRestart

This event is used to report that a process monitored by the RTP node manager is restarting frequently.

Maintenance Procedure

Normally the system automatically recovers by restarting the failed process. If a process restarts repeatedly, it could be due to shared memory corruption and bringing the node to state 3 and back to state 4 may correct the problem.

That should only be attempted during periods of low system activity and if redundancy is available. The Recovery Escalation feature may automatically perform the same RTP restart.

Obtain the following data:

Collect any associated pstack and pmap files that were created from the directory:

`/unisphere/srx3000/srx/40/core/`

Save the system log files in `/log`, e.g. as the root user:

```
tar -cvzf logfiles.tar.gz /log/
```

As the srx user, run `RtpDumpLog -o outputFile.txt`

and save the output file.

`\"RapidStat -c\"` can be run as an alternative to all of the above since it will collect all of the same information and more.

If continuous tracing was active, save the trace files.

It may also be helpful to run an OSV process trace.

Provide all data that was collected to the next level of support.

4.1.4.160 Alarm hiQSecurityFirewallTrigClearTrap

The condition causing the triggering of the firewall has been cleared.

Maintenance Procedure

No action is needed.

4.1.4.161 Alarm hiQSecurityFirewallTrigTrap

The number of packets per second that were received from an endpoint exceeded the rate limit. Network packets from that IP address are blocked by the firewall for 60 seconds. .

Maintenance Procedure

Investigate the log files to determine the IP address that triggered the firewall to start blocking packets from that address. If it is determined that the high packet rate is valid from the given IP address, that IP address added to the list of trusted hosts to prevent triggering of the firewall.

Log files that may contain further details are:

- `/var/log/snort/snortsam.log`
- `/var/log/messages`
- `/var/log/snort/tcpdump`

4.1.4.162 Alarm hiQSevereHardwareTrap

This event is used to report a hardware-related major alarm.

Listed below are the typically reported hardware alarms along with the frequency that the status of each is checked:

Ethernet link or Bonding Group is inactive (checked every minute)

RAID storage failures (checked every 5 minutes)

Disk errors (checked in real-time)

Platform Hardware errors (Temperature, Voltage, etc) detected via IPMI sensors (checked every 30 seconds)

Maintenance Procedure

The action to take depends on the specific alarm.

- Ethernet - verify that an Ethernet cable is connected correctly between the specified port on the OSV and the interfacing network device.
- RAID - use the mpt-status command to view the status of the logical RAID volume and associated physical drives and correct any problem that is identified.
- Disk - A disk error specifying a device (e.g.: `/sda3`) is due to either a total failure of the RAID array or RAID controller or a failure of a disk drive not configured in a RAID array. This indicates that data is corrupt or lost on the primary storage device and must be corrected as soon as possible. If this occurs in a cluster configuration, the node with the disk error should be automatically shut down. If not, attempt to gracefully shut down the node with the failure.
- IPMI hardware sensors:
  - Temperature - verify that the server has proper cooling and ventilation.
  - Power Supply Unit - verify that the redundant power supply, if applicable, is plugged in and connected to a power source.

If the problem is not easily identified and corrected, contact the next level of support. Some alarms may require support from the hardware manufacturer.

4.1.4.163 Alarm hiQSmdiREcvIPAddrPortError

Cannot listen on SMDI virtual IP address/port needed to receive SMDI messages from a Voice Message System over a TCP link.

Maintenance Procedure

Cannot process SMDI messages over the TCP link. Only RTP Backup Status and Shutdown messages can be processed.

4.1.4.164 Alarm hiQSmdiRecvIPAddrPortOk

Can listen on SMDI virtual IP address/port needed to receive SMDI messages from a Voice Message System over a TCP link.

Maintenance Procedure

No action is necessary.

4.1.4.165 Alarm hiQSnmNodeInfoMismatchTrap

The super node manager detects a mismatch between the own node information (name and ID) listed in the RtpClustertab and the node information supplied by the cluster software.

Maintenance Procedure

Contact the next level of support to check and repair the RtpClustertab file.

4.1.4.166 Alarm hiQSnmRebootForSubsystemTrap

The health detector script requires a reboot of the system. Refer to the logfile of the health detector script in `$HOME/$PLID/log` for more information.

Maintenance Procedure

If drastic action is enabled the system will be rebooted, if not it is recommended to reboot the system.

The default setting on the OSV is that drastic action is enabled, however, all subsystems are configured with normal priority so this alarm should never be reported when using the default configuration.

Observe the RTP to see if it runs without further problems.

4.1.4.167 Alarm hiQSnmRtpNodeDownTrap

The RTP node with the given ID is detected as DOWN when the super node manager is starting.

Maintenance Procedure

No action required.

4.1.4.168 Alarm hiQSnmRtpNodeDownWasUpTrap

The RTP node with the given ID changed its state from UP to DOWN. This may be the result of an administrative shutdown, but also of a node or communication failure.

Maintenance Procedure

If the node terminated unexpectedly, check its state and reboot it if needed.

4.1.4.169 Alarm hiQSnmRtpNodeUpTrap

The RTP node with the given ID is detected as UP when the super node manager is starting.

Maintenance Procedure

This is a clearing alarm.

4.1.4.170 Alarm hiQSnmRtpNodeUpWasDownTrap

The RTP node with the given ID changed its state from DOWN to UP.

Maintenance Procedure

This is a clearing alarm.

4.1.4.171 Alarm hiQSnmRtpRestartForSubsystemTrap

The health detector script of the mentioned subsystem requires to restart the whole RTP. Refer to the logfile of the health detector script in `$HOME/$PLID/log` for the reason.

Maintenance Procedure

The RTP will be stopped and restarted. Observe the RTP if it runs without further problems.

4.1.4.172 Alarm hiQSnmSpecialActScrExecTrap

The health detector script of the mentioned subsystem requires to execute the special action script. Refer to the logfile of the health detector script in `$HOME/$PLID/log` for more information.

Maintenance Procedure

Collect `RtpDumpLog` output and escalate to the next level of support to analyze the cause of the subsystem failure. The special action script will be executed. Observe the RTP to verify that it runs without further problems.

4.1.4.173 Alarm hiQSnmSpecialActScrSuccessTrap

The special action script of the mentioned subsystem returns successfully.

Maintenance Procedure

This is a clearing alarm.

4.1.4.174 Alarm hiQSnmStartupFailedTrap

The super node manager fails to start a single subsystem during the start of the whole RTP. For this reason, the start of the RTP cannot be continued, and all subsystems having been started so far, are stopped.

Maintenance Procedure

Check why the mentioned subsystem could not be started inspecting the recently created log files in the `/log` and the `$RTP_HOME/40/log` directories..

4.1.4.175 Alarm hiQSnmStartupSuccessTrap

The super node manager process started successfully. After successful start of the subsystems, it continues to observe the RTP.

Maintenance Procedure

This is a clearing alarm.

4.1.4.176 Alarm hiQSnmSubsysAdmInterventionTrap

The health detector script of the mentioned subsystem requires an administrator intervention.

Maintenance Procedure

Check the exit code of the health detector script and refer to the logfile of the health detector script in `$HOME/$PLID/log` for more information.

4.1.4.177 Alarm hiQSnmSubsysAlreadyRunningTrap

The super node manager tried to start an already running subsystem.

Maintenance Procedure

Nothing to do.

4.1.4.178 Alarm hiQSnmSubsysRestartSuccessTrap

The super node manager has tried to restart the subsystem without success in the past, but now the subsystem is detected as running again.

Maintenance Procedure

No action necessary. The super node manager confirms that a previous repair action was successful.

4.1.4.179 Alarm hiQSnmSubsystemStartErrorTrap

The super node manager can not start the mentioned subsystem. The associated start script returns an error.

Maintenance Procedure

Check the exit code of the start script and refer to the logfile of the start script in `$HOME/$PLID/log` for more informations.

4.1.4.180 Alarm hiQSnmSystemSwitchOffTrap

The health detector script requires to switch off the system. Refer to the logfile of the health detector script in `$HOME/$PLID/log` for more information.

Maintenance Procedure

If drastic action is enabled the system will be switched off.

If drastic action is not enabled, then if the partner node is active, the failed node should be shut down using `srxctl` and powered off. Escalate for immediate repair. Closely monitor the now non-reduntant system to be ready for immediate repair in case of an additional failure causing a total outage.

The default setting on the OSV is that drastic action is enabled, however, all subsystems are configured with normal priority so this alarm should never be reported when using the default configuration.

Observe the RTP on the remaining nodes in the cluster if it runs without further problems.

4.1.4.181 Alarm hiQSolidBackupFailedTrap

The Solid backup failed.

Maintenance Procedure

No action defined.

4.1.4.182 Alarm hiQSolidBothHSBDbPrimaryTrap

Both Solid hot standby databases are marked as primary.

Maintenance Procedure

No action defined.

4.1.4.183 Alarm hiQSolidCreateNewDbFailedTrap

A failure occurred when creating a new Solid database.

Maintenance Procedure

No action defined.

4.1.4.184 Alarm hiQSolidDatabaseStartedTrap

The Solid database was started.

Maintenance Procedure

No action defined.

4.1.4.185 Alarm hiQSolidDbBrokenCopyTrap

The Solid database is a broken hot standby or netcopy database.

Maintenance Procedure

No action defined.

4.1.4.186 Alarm hiQSolidDbConvertedTrap

The Solid database was successfully converted.

Maintenance Procedure

This is a clearing alarm.

4.1.4.187 Alarm hiQSolidDbDoesNotExistsTrap

Cannot create a new database, because the server is not running as a foreground process.

Maintenance Procedure

To create a new database, start the server as a foreground process with `-f` option.

4.1.4.188 Alarm hiQSolidDbIndexErrorTrap

The index for the specified Solid database is not OK.

Maintenance Procedure

No action defined.

4.1.4.189 Alarm hiQSolidDbIndexTestSuccessTrap

The Solid database index has been tested and is OK.

Maintenance Procedure

This is a clearing alarm.

4.1.4.190 Alarm hiQSolidDbOpenFailureTrap

The Solid database failed to open.

Maintenance Procedure

No action defined.

4.1.4.191 Alarm hiQSolidDbOpeningProblemTrap

A problem was encountered when opening a Solid database.

Maintenance Procedure

Check the configuration.

NOTICE:

Only the file(s) defined with the largest FileSpec_n definition(s) should be missing.

4.1.4.192 Alarm hiQSolidDbServerCorruptTrap

The single database server is corrupted.

Maintenance Procedure

To restore the last (or proper) database backup is needed. You must stop the RTP and its applications before the database restore, if the state of the restored database differs with the state of RTP or of its applications.

4.1.4.193 Alarm hiQSolidDbTstConnectFailureTrap

The Solid database failed to connect for testing with a fatal error.

Maintenance Procedure

No action defined.

4.1.4.194 Alarm hiQSolidDbTstOpenFailureTrap

The Solid database failed to open for testing with a fatal error.

Maintenance Procedure

No action defined.

4.1.4.195 Alarm hiQSolidFatalErrSrvNotStartTrap

The Solid database server was not started due to a fatal error.

Maintenance Procedure

No action defined.

4.1.4.196 Alarm hiQSolidFatalErrSrvShutdownTrap

An emergency shutdown of the Solid database server has occurred due to a fatal error.

Maintenance Procedure

No action defined.

4.1.4.197 Alarm hiQSolidFlowEngineIntErrorTrap

The Solid FlowEngine process has encountered an internal error and is unable to continue normally.

Maintenance Procedure

No action defined.

4.1.4.198 Alarm hiQSolidHSBSwitchPrimErrTrap

Failed to switch hot standby role to primary with the specified error.

Maintenance Procedure

No action defined.

4.1.4.199 Alarm hiQSolidHSBSwitchSecErrTrap

Failed to switch hot standby role to secondary with the specified error.

Maintenance Procedure

No action defined.

4.1.4.200 Alarm hiQSolidLocalDbServerCorruptTrap

The local database server failed, it is not possible to restart it, because the database content is inconsistent.

Maintenance Procedure

The Watchdog tries to repair the database, no further action is needed.

4.1.4.201 Alarm hiQSolidNewConnsAllowedTrap

New database connections are allowed.

Maintenance Procedure

No action defined.

4.1.4.202 Alarm hiQSolidNewDbNotCreatedTrap

The new Solid database was not created.

Maintenance Procedure

No action defined.

4.1.4.203 Alarm hiQSolidNoNewConnsAllowedTrap

The Solid database server is in a fatal state - no new connections are allowed.

Maintenance Procedure

No action defined.

4.1.4.204 Alarm hiQSolidOldDbVersionTrap

The Solid database is from an older version of Solid.

Maintenance Procedure

To convert database for use with this version, start server with option -x convert.

Please note that after conversion, database cannot be used with older versions of server anymore.

4.1.4.205 Alarm hiQSolidServerStartFailedTrap

The Solid database failed to start.

Maintenance Procedure

No action defined.

4.1.4.206 Alarm hiQSolidShutdownTrap

The Solid database was shut down.

Maintenance Procedure

No action defined.

4.1.4.207 Alarm hiQSolidStartedHSBPrimaryTrap

Started as a hot standby primary.

Maintenance Procedure

No action defined.

4.1.4.208 Alarm hiQSolidStartedHSBSecondaryTrap

Started as a hot standby secondary.

Maintenance Procedure

No action defined.

4.1.4.209 Alarm hiQSolidTableConvertedTrap

The specified Solid database table was converted.

Maintenance Procedure

This is a clearing alarm.

4.1.4.210 Alarm hiQSolidTooManyClientsTrap

The specified user failed to connect due to too many connected clients.

Maintenance Procedure

No action defined.

4.1.4.211 Alarm hiQSubMgmtRemoveResourceError

The job to remove resources failed.

Maintenance Procedure

Remove the resources manually.

4.1.4.212 Alarm hiQSubMgmtRemoveResourceSuccess

The job to remove subscriber management resources completed successfully.

Maintenance Procedure

This is a clearing alarm.

4.1.4.213 Alarm hiQTcaClearedTrap

The number of logged entries for the specified log category has not crossed the threshold that caused a previous alarm for a certain period of time.

Maintenance Procedure

This is a clearing alarm.

4.1.4.214 Alarm hiQTcaL1CommunicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature. The alarm can be cleared manually or, if configured accordingly, it will clear automatically after a certain time period without threshold crossing event.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- END_POINT_OOS

  Endpoint is out of service or not responding
- COM_EXT_PROTOCOL_ERR

  Internal communications and other errors
- COM_EXT_TIME_OUT

  External communications - response timeout
- COM_EXT_BAD_SYNTAX

  External communications - bad message syntax
- COM_EXT_RESP_ERR_RX

  External communications - bad message syntax
- COM_INT_BAD_SYNTAX

  Internal communications - bad syntax
- COM_INT_PROTOCOL_ERR

  Internal communications - other errors
- COM_INT_TIME_OUT

  Internal communications - response timeout
- END_POINT_INVALID

  Endpoint is not known to the OSV
- DNS_UNAVAILABLE

  DNS is unavailable
- RSIP_RX

  MGCP RSIP received
- RES_MGMT_COMM_ERR

  Resource Manager communication error
- LINK_ERR

  CSTA link connection status

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Communication errors may be caused by hardware failures, configuration/ provisioning errors, or network problems.

Check whether a majority of the communication problems point to a particular device or network. Determine if something has changed in the network recently (hardware change or configuration update) or if a software upgrade has recently been performed. The problem could also be due to configuration changes in the packet filter (firewall) rules.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure.

4.1.4.215 Alarm hiQTcaL1DatabaseTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature. The alarm can be cleared manually or, if configured accordingly, it will clear automatically after a certain time period without threshold crossing event.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- AUDIT_ERR

  Audit errors
- DATABASE_CON_ERR

  Database connection errors
- DATABASE_SQL_ERR

  Database SQL errors
- DATABASE_ERR

  General database errors
- DATA_ERR

  Data problems, e.g.: consistency checks
- PROVISIONING_ERR

  Provisioning errors
- SUB_PROVISIONING_ERR

  Subscriber provisioning errors

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Provisioning and audit errors need to be analyzed one by one. Display the subscriber settings in order to determine the type of registration (static vs dynamic) as well as the protocol and compare those settings with what is seen in a network trace of the call.

If the problem/solution cannot be identified, contact the next level of support.

4.1.4.216 Alarm hiQTcaL1EnvironmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature. The alarm can be cleared manually or, if configured accordingly, it will clear automatically after a certain time period without threshold crossing event.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.217 Alarm hiQTcaL1EquipmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.218 Alarm hiQTcaL1IndicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.219 Alarm hiQTcaL1MibTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.220 Alarm hiQTcaL1ProcessingTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- API_ERR

  Errors returned from a non-RTP API call
- RTP_API_ERR

  Errors returned from RTP API calls
- CALL_PROC_ERR

  General processing errors
- CLUSTER_COM_PROBLEM

  Inter-cluster communication problems
- END_POINT_EXPIRED

  Endpoint expired
- OVERLOAD

  Transactions rejected due to overload
- RESOURCE_LIMIT

  Resource limit reached
- SRVR_OR_GW_OVERLOAD

  Server or gateway overload
- MAINTENANCE

  Maintenance related
- SW_ERR

  Software errors
- PROC_INIT_FAILURE

  Process initialization failure
- PROC_EXIT

  Process exit due to failure
- VIP_SUBSCRIBER_PROBLEM

  VIP subscriber problems

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Most processing errors need to be escalated if occurring in a larger number as they may be an indication of a software error.

Cluster_COM_Problems need analysis:

- Check connectivity and bandwidth of the x-channel.
- Did the network change? Equipment, transmission, firewall, new devices connected, more traffic. Continuous cluster-com-problems may cause OSV performance reduction and synchronization failures between the two OSV nodes. This will lead to call failures after a node switchover.

For OVERLOAD alarms, run the command `\"top -b -n 3 >topOutput.txt\"` during the period of overload and provide the output to the next level of support.

4.1.4.221 Alarm hiQTcaL1SecurityTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm is reported for log category:

- OP_LOG_CAT_IPSEC_ERR

  IP security
- LOG_FAILURE

  Failure to log event in security log files `/var/log/Rtp*Ev*`

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.222 Alarm hiQTcaL1ServiceTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.223 Alarm hiQTcaL2CommunicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the hiQ logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- END_POINT_OOS

  Endpoint is out of service or not responding
- COM_EXT_PROTOCOL_ERR

  Internal communications and other errors
- COM_EXT_TIME_OUT

  External communications - response timeout
- COM_EXT_BAD_SYNTAX

  External communications - bad message syntax
- COM_EXT_RESP_ERR_RX

  External communications - bad message syntax
- COM_INT_BAD_SYNTAX

  Internal communications - bad syntax
- COM_INT_PROTOCOL_ERR

  Internal communications - other errors
- COM_INT_TIME_OUT

  Internal communications - response timeout
- END_POINT_INVALID

  Endpoint is not known to the OSV
- DNS_UNAVAILABLE

  DNS is unavailable
- RSIP_RX

  MGCP RSIP received
- RES_MGMT_COMM_ERR

  Resource Manager communication error
- LINK_ERR

  CSTA link connection status

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Communication errors may be caused by hardware failures, configuration/ provisioning errors, or network problems.

Check whether a majority of the communication problems point to a particular device or network. Determine if something has changed in the network recently (hardware change or configuration update) or if a software upgrade has recently

been performed. The problem could also be due to configuration changes in the packet filter (firewall) rules.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure..

4.1.4.224 Alarm hiQTcaL2DatabaseTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

AUDIT_ERR

Audit errors

DATABASE_CON_ERR

Ddatabase connection errors

DATABASE_SQL_ERR

Database SQL errors

DATABASE_ERR

General database errors

DATA_ERR

Data problems, e.g.: consistency checks

PROVISIONING_ERR

Provisioning errors

SUB_PROVISIONING_ERR

Subscriber provisioning errors

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Provisioning and audit errors need to be analyzed one by one. Display the subscriber settings in order to determine the type of registration (static vs dynamic) as well as the protocol and compare those settings with what is seen in a network trace of the call.

If the problem/solution cannot be identified, contact the next level of support.

4.1.4.225 Alarm hiQTcaL2EnvironmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.226 Alarm hiQTcaL2EquipmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.227 Alarm hiQTcaL2IndicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the hiQ logging feature. The alarm can be cleared manually or, if configured accordingly, it will clear automatically after a certain time period without threshold crossing event.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.228 Alarm hiQTcaL2MibTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.229 Alarm hiQTcaL2ProcessingTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the hiQ logging feature. The alarm can be cleared manually or, if configured accordingly, it will clear automatically after a certain time period without threshold crossing event.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- API_ERR

  Errors returned from a non-RTP API call
- RTP_API_ERR

  Errors returned from RTP API calls
- CALL_PROC_ERR

  General processing errors
- CLUSTER_COM_PROBLEM

  Inter-cluster communication problems
- END_POINT_EXPIRED

  Endpoint expired
- OVERLOAD

  Transactions rejected due to overload
- RESOURCE_LIMIT

  Resource limit reached
- SRVR_OR_GW_OVERLOAD

  Server or gateway overload
- MAINTENANCE

  Maintenance related
- SW_ERR

  Software errors
- PROC_INIT_FAILURE

  Process initialization failure
- PROC_EXIT

  Pprocess exit due to failure
- VIP_SUBSCRIBER_PROBLEM

  VIP subscriber problems

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Most processing errors need to be escalated if occurring in a larger number as they may be an indication of a software error.

Cluster_COM_Problems need analysis:

- Check connectivity and bandwidth of the x-channel.
- Did the network change? Equipment, transmission, firewall, new devices connected, more traffic. Continuous cluster-com-problems may cause OSV performance reduction and synchronization failures between the two OSV nodes. This will lead to call failures after a node switchover.

For OVERLOAD alarms, run the command `\"top -b -n 3 >topOutput.txt\"` during the period of overload and provide the output to the next level of support.

4.1.4.230 Alarm hiQTcaL2SecurityTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm is reported for log category:

OP_LOG_CAT_IPSEC_ERR

IP security

LOG_FAILURE

Failure to log event in security log files /var/log/Rtp*Ev*

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.231 Alarm hiQTcaL2ServiceTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.232 Alarm hiQTcaL3CommunicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the hiQ logging feature. The alarm can be cleared manually or, if configured accordingly, it will clear automatically after a certain time period without threshold crossing event.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- END_POINT_OOS

  Endpoint is out of service or not responding
- COM_EXT_PROTOCOL_ERR

  Internal communications and other errors
- COM_EXT_TIME_OUT

  External communications - response timeout
- COM_EXT_BAD_SYNTAX

  External communications - bad message syntax
- COM_EXT_RESP_ERR_RX

  External communications ad message syntax
- COM_INT_BAD_SYNTAX

  Internal communications - bad syntax
- COM_INT_PROTOCOL_ERR

  Internal communications - other errors
- COM_INT_TIME_OUT

  Internal communications - response timeout
- END_POINT_INVALID

  Endpoint is not known to the OSV
- DNS_UNAVAILABLE

  DNS is unavailable
- RSIP_RX

  MGCP RSIP received
- RES_MGMT_COMM_ERR

  Resource Manager communication error
- LINK_ERR

  CSTA link connection status

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Communication errors may be caused by hardware failures, configuration/ provisioning errors, or network problems.

Check whether a majority of the communication problems point to a particular device or network.

Determine if something has changed in the network recently (hardware change or configuration update) or if a software upgrade has recently been performed. The problem could also be due to configuration changes in the packet filter (firewall) rules.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure.

4.1.4.233 Alarm hiQTcaL3DatabaseTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- AUDIT_ERR

  Audit errors
- DATABASE_CON_ERR

  Database connection errors
- DATABASE_SQL_ERR

  Database SQL errors
- DATABASE_ERR

  General database errors
- DATA_ERR

  Data problems, e.g.: consistency checks
- PROVISIONING_ERR

  Provisioning errors
- SUB_PROVISIONING_ERR

  Subscriber provisioning errors

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Provisioning and audit errors need to be analyzed one by one. Display the subscriber settings in order to determine the type of registration (static vs dynamic) as well as the protocol and compare those settings with what is seen in a network trace of the call.

If the problem/solution cannot be identified, contact the next level of support.

4.1.4.234 Alarm hiQTcaL3EnvironmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.235 Alarm hiQTcaL3EquipmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the hiQ logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.236 Alarm hiQTcaL3IndicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature. Currently no alarm category is configured to generate this event/alarm.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.237 Alarm hiQTcaL3MibTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event

4.1.4.238 Alarm hiQTcaL3ProcessingTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- API_ERR

  Errors returned from a non-RTP API call
- RTP_API_ERR

  Errors returned from RTP API calls

- CALL_PROC_ERR

  General processing errors
- CLUSTER_COM_PROBLEM

  Inter-cluster communication problems
- END_POINT_EXPIRED -

  Endpoint expired
- OVERLOAD

  Transactions rejected due to overload
- RESOURCE_LIMIT

  Resource limit reached
- SRVR_OR_GW_OVERLOAD

  Server or gateway overload
- MAINTENANCE

  Maintenance related
- SW_ERR

  Software errors
- PROC_INIT_FAILURE

  Process initialization failure
- PROC_EXIT

  Process exit due to failure
- VIP_SUBSCRIBER_PROBLEM

  VIP subscriber problems

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Most processing errors need to be escalated if occurring in a larger number as they may be an indication of a software error.

Cluster_COM_Problems need analysis:

- Check connectivity and bandwidth of the x-channel.
- Did the network change? Equipment, transmission, firewall, new devices connected, more traffic. Continuous cluster-com-problems may cause OSV performance reduction and synchronization failures between the two OSV nodes. This will lead to call failures after a node switchover.

For OVERLOAD alarms, run the command `\"top -b -n 3 >topOutput.txt\"` during the period of overload and provide the output to the next level of support.

4.1.4.239 Alarm hiQTcaL3SecurityTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm is reported for log category:

- OP_LOG_CAT_IPSEC_ERR

  IP security
- LOG_FAILURE

  Failure to log event in security log files /var/log/Rtp*Ev*

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.240 Alarm hiQTcaL3ServiceTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.241 Alarm hiQTcaL4CommunicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- END_POINT_OOS

  Endpoint is out of service or not responding
- COM_EXT_PROTOCOL_ERR

  Internal communications and other errors
- COM_EXT_TIME_OUT

  External communications - response timeout
- COM_EXT_BAD_SYNTAX

  External communications - bad message syntax
- COM_EXT_RESP_ERR_RX

  External communications - bad message syntax

- COM_INT_BAD_SYNTAX

  Internal communications - bad syntax
- COM_INT_PROTOCOL_ERR

  Internal communications - other errors
- COM_INT_TIME_OUT

  Internal communications - response timeout
- END_POINT_INVALID

  Endpoint is not known to the OSV
- DNS_UNAVAILABLE

  DNS is unavailable
- RSIP_RX

  MGCP RSIP received
- RES_MGMT_COMM_ERR

  Resource Manager communication error
- LINK_ERR

  CSTA link connection status

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Communication errors may be caused by hardware failures, configuration/ provisioning errors, or network problems.

Check whether a majority of the communication problems point to a particular device or network. Determine if something has changed in the network recently (hardware change or configuration update) or if a software upgrade has recently been performed. The problem could also be due to configuration changes in the packet filter (firewall) rules.

If the problem causing the communication failure cannot be determined and corrected, provide Ethereal/Wireshark trace files obtained from both the OSV as well as the communication partner in order to help determine the point of failure.

4.1.4.242 Alarm hiQTcaL4DatabaseTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- AUDIT_ERR

  Audit errors
- DATABASE_CON_ERR

  Database connection errors

- DATABASE_SQL_ERR

  Database SQL errors
- DATABASE_ERR

  General database errors
- DATA_ERR

  Data problems, e.g.: consistency checks
- PROVISIONING_ERR

  Provisioning errors
- SUB_PROVISIONING_ERR

  Subscriber provisioning errors

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Provisioning and audit errors need to be analyzed one by one. Display the subscriber settings in order to determine the type of registration (static vs dynamic) as well as the protocol and compare those settings with what is seen in a network trace of the call.

If the problem/solution cannot be identified, contact the next level of support.

4.1.4.243 Alarm hiQTcaL4EnvironmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.244 Alarm hiQTcaL4EquipmentTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.245 Alarm hiQTcaL4IndicationTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.246 Alarm hiQTcaL4MibTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.247 Alarm hiQTcaL4ProcessingTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

This alarm can be reported for any of the following log categories (categories are prefixed with OP_LOG_CAT_):

- API_ERR

  Errors returned from a non-RTP API call
- RTP_API_ERR

  Errors returned from RTP API calls
- CALL_PROC_ERR

  General processing errors
- CLUSTER_COM_PROBLEM

  Inter-cluster communication problems
- END_POINT_EXPIRED

  Endpoint expired
- OVERLOAD

  Transactions rejected due to overload
- RESOURCE_LIMIT

  Resource limit reached
- SRVR_OR_GW_OVERLOAD

  Server or gateway overload

- MAINTENANCE

  Maintenance related
- SW_ERR

  Software errors
- PROC_INIT_FAILURE

  Process initialization failure
- PROC_EXIT

  Process exit due to failure
- VIP_SUBSCRIBER_PROBLEM

  VIP subscriber problems

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

Most processing errors need to be escalated if occurring in a larger number as they may be an indication of a software error.

Cluster_COM_Problems need analysis:

- Check connectivity and bandwidth of the x-channel.
- Did the network change? Equipment, transmission, firewall, new devices connected, more traffic. Continuous cluster-com-problems may cause OSV performance reduction and synchronization failures between the two OSV nodes. This will lead to call failures after a node switchover.

For OVERLOAD alarms, run the command `\"top -b -n 3 >topOutput.txt\"` during the period of overload and provide the output to the next level of support.

4.1.4.248 Alarm hiQTcaL4SecurityTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature. This alarm is reported for log category: OP_LOG_CAT_IPSEC_ERR - IP security or LOG_FAILURE - failure to log event in security log files /var/log/Rtp*Ev*.

Maintenance Procedure

Retrieve and analyze OSV event log that is specified in the alarm text to further isolate the problem.

- The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.
- The log entry should provide an indication of the specific problem. Verify the related configuration using the CLI. If unable to determine and correct the problem, contact the next level of support.

4.1.4.249 Alarm hiQTcaL4ServiceTrap

The number of logged entries for the specified log category has crossed the high threshold of logs per time interval as defined by the OSV logging feature.

Maintenance Procedure

Retrieve and analyze OSV event logs to further isolate the problem.

The alarm can be cleared manually via the Assistant or the CLI or, if configured accordingly, it will clear automatically after a certain time period without a threshold crossing event.

4.1.4.250 Alarm hiQTestCallGeneratorNotOkTrap

The test call generator has encountered call processing failures. SW processes will be restarted.

Maintenance Procedure

No action is needed.

4.1.4.251 Alarm hiQTestCallGeneratorOkTrap

Call processing is working on this node.

Maintenance Procedure

No action is needed.

4.1.4.252 Alarm hiQTestCallGeneratorProvErrTrap

The test call feature has been disabled due to invalid provisioning data.

Maintenance Procedure

Manual intervention required. Check provisioning of the Test Call Generator subsystem.

4.1.4.253 Alarm hiQTestCallGenNotOkNodeRestart

After a node restart callp is still not working. The node is taken out of service (level-3) to allow the partner node to continue call processing.

Maintenance Procedure

Node taken out of service. Manual repair necessary.

4.1.4.254 Alarm hiQTestCallGenNotOkProcRestart

Still no active call processing after process restarts.

Maintenance Procedure

No service intervention necessary. The node will be restarted once.

4.1.4.255 Alarm hiQTestCallGenOverloadDetTrap

The test call generator has encountered overload for more than the specified number of minutes.

Maintenance Procedure

No immediate action is needed.

4.1.4.256 Alarm hiQTicCopyToTicketPoolFailed

In order to move a ticket file from or to the central ticket pool, the copy command failed.

Maintenance Procedure

Check the RTP state - especially for available ticket files of the appropriate ticket type.

If no problem can be found, contact the service team.

4.1.4.257 Alarm hiQTicDiskFullTicketPoolFailed

A new ticket file has to be created by the ticket manager. However, a check of the available free disc space failed: there is not enough disc space to create the new ticket file.

Maintenance Procedure

Check the local ticket directory disc. Check the ticket manager configuration.

Run the command `df -k` to show the disk partition usage and provide that to the next level of support.

4.1.4.258 Alarm hiQTicPoolDiskDevNotAccessible

During ticket initialization, an error occurred; the configured disk device for the central ticket pool was not accessible.

Maintenance Procedure

Run the command `df -k` to show all disk partitions and provide the output to the next level of support.

4.1.4.259 Alarm hiQUCEServicesRegisteringTrap

This event is used to report that UCE services registering is started.

Maintenance Procedure

No action is needed.

4.1.4.260 Alarm hiQUCEServicesRegistrationFailedTrap

This event is used to report that UCE services failed registration.

Maintenance Procedure

No action is needed.

4.1.4.261 Alarm hiQVeryImportantFuncUnavailTrap

The system function identified by the faulty object is not available.

- An alarm with faultyObject = Function is raised:

  Registration Audit/Timer is reported when the registration audit cannot set a timer to periodically check for expired registrations
- An alarm with faultyObject = PacketFilter is raised:

  if the Security Manager could not successfully apply all of the packet filter rules. In that case, the final DROP rules may not be applied, possibly allowing network access to ports or IP addresses that should be blocked.
- An alarm with faultyObject = NTP/NTPDaemon is raised:

  if the ntp daemon is down or no NTP servers are configured.
- An alarm with faultyObject = NTP/Sync is raised:

  if the OSV system time is not synchronized with an NTP server.

Maintenance Procedure

- For an alarm with faultyObject = Function:

  Registration Audit/Timer, the system will recover alone as soon as a new registration comes in and timers become available again. If new registrations are not expected it does not matter whether the licenses audit is running or not. Regarding the registration audit it can be disabled and reenabled again to trigger it.
- For an alarm with faultyObject = PacketFilter:

  Use the CLI to display all packet filter rules. Run iptables -vnL to obtain the current filter rules that are applied. Obtain the `/etc/hosts` file and `/log/HiqLogSwError.log`. Provide all information to the next level of support.
- For an alarm with faultyObject = NTP/NTPDaemon:

  Execute `systemctl status ntpd` to determine if the daemon is running. Use the date command to verify that the system time is within 11 minutes of the actual time. If not, follow the documented procedures for changing the system time on the OSV. If it is, execute `systemctl restart ntpd` to

attempt to restart the NTP daemon and note any problems reported. Check `/var/ntp/ntp.log` for errors.

- For an alarm with faultyObject = NTP/Sync:

  Execute `ntpq -pn` to show the status of each time source. Verify that the configured time sources are correct and on a cluster, verify that one of the sources is the partner node IP address. Verify that UDP port 123 is not blocked by a firewall.

If problem persists, contact the next level of support.

4.1.4.262 Alarm hiQVerySevereHardwareFailureTrap

This event is used to report a hardware-related critical alarm.

Listed below are the typically reported hardware alarms along with the frequency that the status of each is checked:

- Ethernet link or Bonding Group is inactive (checked every minute)
- RAID storage failures (checked every 5 minutes)
- Disk errors (checked in real-time)
- Platform Hardware errors (Temperature, Voltage, etc) detected via IPMI sensors (checked every 30 seconds)

Maintenance Procedure

The action to take depends on the specific alarm.

- Ethernet

  Verify that an Ethernet cable is connected correctly between the specified port on the OSV and the interfacing network device.
- RAID

  Use the mpt-status command to view the status of the logical RAID volume and associated physical drives and correct any problem that is identified.
- Disk

  A disk error specifying a device (e.g.: `/sda3`) is due to either a total failure of the RAID array or RAID controller or a failure of a disk drive not configured in a RAID array. This indicates that data is corrupt or lost on the primary storage device and must be corrected as soon as possible. If this occurs in a cluster configuration, the node with the disk error should be automatically shut down. If not, attempt to gracefully shut down the node with the failure.
- IPMI hardware sensors:
  - Temperature

    Verify that the server has proper cooling and ventilation.
  - Power Supply Unit

    Verify that the redundant power supply, if applicable, is plugged in and connected to a power source.

If the problem is not easily identified and corrected, contact the next level of support. Some alarms may require support from the hardware manufacturer.

5 Serviceability - Logging and Diagnostics

These features provide mechanisms to improve serviceability.

5.1 System Monitoring

System monitoring features deliver information on the system, especially alarms and fault messages automatically from the system components as base for maintenance actions. System processes are written to logging files find out different reasons about erroneous behavior. Audit log logs all important activities performed by the Common Management Platform users.

5.1.1 Fault Logs

A fault is a condition in the system, detected by the system, where the system does not behave as specified. All the Faults are predefined by the system and can’t be changed.

When a fault is recognized by the system it is raised to the system fault management in the following way in order to be processed adequately:

- System internal service or component recognize a fault
- System fault management is informed about the fault.
- System internal service or component recognize a fault
- Fault is stored in the fault history log persistently
- Fault is evaluated whether it matches a certain alarm condition.
- Configured alarm action for the alarm condition is executed (e.g. send alarm via SNMP)
- System internal service or component recognize a fault
- Alarm is set to the **active** (ON) state.
- If the alarm is switched on and there is already the same alarm active, the new alarm data is taken over. This means the timestamp of the active alarm is set to the new occurrence. In addition, the alarm hit count is increased by one.
- A corresponding alarm history entry is created in the alarm history log.

If for any reason forwarding of faults is not possible, then the faults will be stored and system will retry to send them later. Retry sending of faults should cover at least 4 hours.

The Fault message is divided into different sections:

- Fault identification containing Fault ID, Fault classification, Fault priority, System ID, Time/Date, impacted component (e.g., name of the software component)
- Fault description containing all relevant fault Cause information.

- Optionally, proposed actions may contain mainly service-relevant proposals to fix the problem, e.g. check interface to a partner system or line connections, tracer activities etc.

All faults that have occurred in the system are stored and displayed in a log file. For each fault detailed information about reason and faulty system parts are given

This list contains for each entry the following information:

Tab **General**:

- **Fault ID**: ID that uniquely identifies a fault. If you click on the fault ID the settings of the relevant alarm are displayed.
- **Service ID:** The ID number assigned to the service.
- **Container ID**: The ID number assigned to the container.
- **Node ID**: The ID number assigned to the node.
- **Application ID:** The ID number assigned to the application.
- **Level**

  Possible Values:

  – 0 = normal fault:

    Component that has signaled the fault is still able to operate.
  – 1 = fatal fault:

    Component that has signaled the fault is no longer operable or only operable to a certain extent.
  – 99 = Reset: Fault is cleared.
- **Date/Time**: Specifies at which date and time the fault occurred last.
- **Description**: Displays a short general fault information.

Tab **Description**:

- The description part shows a more detailed description of the selected fault.

Related concepts

Concept of the Alarms and Fault Messages on page 149

5.1.1.1 How to Display the Fault Log

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.

2) Click on the **Logs** > **Fault**

A list of all Faults logged in the selected domain appears in the work area.

3) Click on the **Fault ID** of the desired fault.

The dialog with the associated detailed information opens.

4) Click the tabs to get fault details.

5.1.1.2 How to Set a Filter for a Fault Log

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.
2) Click on the **Logs** > **Fault**

   A list of all Faults logged in the selected domain appears in the work area.
3) Click **Advanced**.

   The dialog with the filter settings opens.
4) Select an option in the area **Time**:
   - **All**: All faults are displayed.
   - **After Date**: Only the faults after the specified date are displayed
   - **Before date**: Only the faults before the specified date are displayed
   - **Between dates**: Only the faults within the specified date range are displayed.
5) Select an option in the area **Type**:
   - All, Active, Reset
6) Apply changes.
7) Click **Apply**.

The logged faults list only displays the faults that correspond to the filter settings made.

5.1.1.3 How to Change a Filter for a Fault Log

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.
2) Click on the **Logs** > **Fault**

   A list of all Faulst logged in the selected domain appears in the work area.
3) Click **Advanced**.

   The dialog with the current settings of the applied filter is displayed.
4) Apply changes to the filter settings.
5) Click **Apply**.

5.1.1.4 How to Clear a Filter for a Fault Log

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.
2) Click on the **Logs** > **Fault**
   A filtered list of all faults logged in the selected domain appears in the work area
3) Click **Show All**.

The Filter field displays **No filter applied** and the list of active alarms contains all currently active alarms again.

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

5.1.2 Alarm Destination

Framework alarms raised in the system are sent to alarm destinations. These alarm destinations can be displayed in an alarm destination list. An alarm destination consists of an IP address and a Layer-3 port.

For SNMP traps, the alarm destination is the IP address or the host name of an external fault management system and the default value for the port is 162. Every SNMP Trap is sent to the global list of alarm destinations.

Related concepts

Concept of the Alarms and Fault Messages on page 149

5.1.2.1 How to Add an OpenScape Voice Alarm Destination

To add an **OpenScape Voice** Alarm Destination using CLI:

Prerequisites

Read sections CLI (Command Line Interface) and How to Open a CLI (Command Line Interface) Session.

Adequate administrative permissions

Step by Step

1) Open a startCLI instance and login

2) From the **Main Menu**

The Main Menu is displayed.

Example:

```
Main Menu:

Configuration Management.....................1
Fault Management.............................2
Performance Management.......................3
Security Management..........................4
System Management............................5
Application-level Management.................6

Open Logfile.........................94
Show Callback Output.................95
Wait for Callbacks...................96
Change Password......................97
Expert Mode..........................98
Exit.................................99

Selection: 2
```

3) Type **2** and press ENTER.

NOTICE:

You can alternatively use the Expert Mode (option 98).

Example: evtCreateSnmpEventFilter "172.25.99.66" { } { 1 2 } 3 -1 "RtpSnmp1" evtCreateSnmpEventFilter "172.25.99.66" { 5 25 104 } { 3 4 5 } 2 8086 evtCreateSnmpEventFilter "172.25.99.66" {} {} 1 -1

The **Fault Management** menu is displayed.

Example:

```
Fault Management:

Events.......................................1
Alarms.......................................2
Trace........................................3
Audit........................................4
Recovery.....................................5

Return.............................99

Selection: 1
```

4) Type **1** and press ENTER.

   The **Events (methods)** menu is displayed.

   Example:

```
Events (methods)

registerForEvents.............................1
unregisterForEvents...........................2
reRegisterForEvents...........................3
recoverEvents.................................4
getEventSets..................................5
getEventBasicDescriptions.....................6
getFullEventDescription.......................7
modifyEventParameters.........................8
getEventEscalationFilters.....................9
addEventEscalationFilter.....................10
removeEventEscalationFilter..................11
removeEvents.................................12
getLatestEventSequenceNumber................13
createSnmpEventFilter........................14
modifySnmpEventFilter........................15
removeSnmpEventFilter........................16
getSnmpEventFilters..........................17

Return.....................................99

Selection: 14
```

5) Type **14** and press ENTER.

6) Type the IP Address, the event set, the Trap severities you want to allow to go through as traps, the SNMP version and the trap destination port, followed by pressing ENTER.

   Example:

```
executing method createSnmpEventFilter...

ipAddr: 127.0.0.1

eventSets[0] <end: <Return>>:

severities[0] <EVT_SEV_CRITICAL: 1,

EVT_SEV_MAJOR: 2,

EVT_SEV_MINOR: 3,

EVT_SEV_WARNING: 4,

EVT_SEV_INFORMATION: 5,

EVT_SEV_CLEAR: 6,

end: <Return>>: 1

....

Do you want to execute this action? (default: yes):

Press <Return> to continue
```

7) Press ENTER.

5.1.2.2 How to Modify an OpenScape Voice Alarm Destination

To modify an **OpenScape Voice** Alarm Destination:

Prerequisites

Read sections CLI (Command Line Interface) and How to Open a CLI (Command Line Interface) Session.

Adequate administrative permissions

Step by Step

1) Open a startCLI instance and login

2) From the **Main Menu**

The Main Menu is displayed.

Example:

```
Main Menu:

Configuration Management.....................1
Fault Management.............................2
Performance Management.......................3
Security Management..........................4
System Management............................5
Application-level Management.................6

Open Logfile.........................94
Show Callback Output.................95
Wait for Callbacks...................96
Change Password......................97
Expert Mode..........................98
Exit.................................99

Selection: 2
```

3) Type **2** and press ENTER.

The **Fault Management** menu is displayed.

Example:

```
Fault Management:

Events.......................................1
Alarms.......................................2
Trace........................................3
Audit........................................4
Recovery.....................................5

Return.............................99

Selection: 1
```

4) Type **1** and press ENTER.

   The **Events (methods)** menu is displayed.

   Example:

```
Events (methods)

registerForEvents.............................1
unregisterForEvents...........................2
reRegisterForEvents...........................3
recoverEvents.................................4
getEventSets..................................5
getEventBasicDescriptions.....................6
getFullEventDescription.......................7
modifyEventParameters.........................8
getEventEscalationFilters.....................9
addEventEscalationFilter.....................10
removeEventEscalationFilter..................11
removeEvents.................................12
getLatestEventSequenceNumber................13
createSnmpEventFilter........................14
modifySnmpEventFilter........................15
removeSnmpEventFilter........................16
getSnmpEventFilters..........................17

Return.....................................99

Selection: 15
```

5) Type **15** and press ENTER.

6) Type the IP Address, the event set, the Trap severities you want to allow to go through as traps, the SNMP version and the trap destination port, followed by pressing ENTER.

   Example:

```
executing method modifySnmpEventFilter...

ipAddr: 127.0.0.1

eventSets[0] <end: <Return>>:

severities[0] <EVT_SEV_CRITICAL: 1,

EVT_SEV_MAJOR: 2,

EVT_SEV_MINOR: 3,

EVT_SEV_WARNING: 4,

EVT_SEV_INFORMATION: 5,

EVT_SEV_CLEAR: 6,

end: <Return>>: 1

Do you want to execute this action? (default: yes):

Press <Return> to continue
```

7) Press ENTER.

5.1.2.3 How to Clear Alarm Destinations

To clear **OpenScape Voice** Alarm Destinations:

Prerequisites

Read sections CLI (Command Line Interface) and How to Open a CLI (Command Line Interface) Session.

Adequate administrative permissions

Step by Step

1) Open a startCLI instance and login

2) From the **Main Menu**

The Main Menu is displayed.

Example:

```
Main Menu:

Configuration Management.....................1
Fault Management.............................2
Performance Management.......................3
Security Management..........................4
System Management............................5
Application-level Management.................6

Open Logfile.............................94
Show Callback Output.....................95
Wait for Callbacks.......................96
Change Password..........................97
Expert Mode..............................98
Exit.....................................99

Selection: 2
```

3) Type **2** and press ENTER.

The **Fault Management** menu is displayed.

Example:

```
Fault Management:

Events.......................................1
Alarms.......................................2
Trace........................................3
Audit........................................4
Recovery.....................................5

Return.....................................99

Selection: 1
```

4) Type **1** and press ENTER.

The **Events (methods)** menu is displayed.

Example:

```
Events (methods)

registerForEvents.............................1
unregisterForEvents...........................2
reRegisterForEvents...........................3
recoverEvents.................................4
getEventSets..................................5
getEventBasicDescriptions.....................6
getFullEventDescription.......................7
modifyEventParameters.........................8
getEventEscalationFilters.....................9
addEventEscalationFilter.....................10
removeEventEscalationFilter..................11
removeEvents.................................12
getLatestEventSequenceNumber.................13
createSnmpEventFilter........................14
modifySnmpEventFilter........................15
removeSnmpEventFilter........................16
getSnmpEventFilters..........................17

Return.................................99

Selection: 16
```

5) Type **16** and press ENTER.

Example:

```
executing method removeSnmpEventFilter...

ipAddr: 127.0.0.1

Do you want to execute this action? (default: yes):

Press <Return> to continue
```

6) Press ENTER.

5.1.3 Logging

Important OpenScape system data are recorded by each node in the background and stored in log files. This data is called diagnostics data and can be downloaded from each node if required.

5.1.3.1 Configuration Files

The configuration files contain the settings that define which diagnostics data is to be recorded. These configuration files are xml files and can be customized as needed by using any editor.

Functional Sequence

To customize the configuration files, they can be downloaded from the system, edited locally, and then uploaded to the system again. Multiple configuration files can be loaded on a node, but only one configuration file can be active at any given time.

A default configuration file is provided by the system for every node. Even the default configuration file can be customized with an editor and uploaded back to the node. In addition, the node can also be reset back to the default configuration file.

The following tasks can be performed for a node :

- **Node Info**

  Shows information about selected node.
- **File Info**

  Shows information about configuration file.
- **Start / Stop C.O. (Cyclic Overwriting)**

  Starts or stops the overwriting of log files.
- **Start / StopTrace**

  Starts or stops the online tracing of the selected nodes.
- **Upload to Node**

  Choose a configuration file and upload the file to the selected node.
- **Start new Log File**

  All activities logged from this point are stored in the new log file. For the selected nodes the content of the old log file is stored in a backup log file.
- **Activate default configuration**

  If errors occur in other configuration files you can reset the configuration to the default settings.

System Specific Information

The following detailed information is displayed:

- **Node**

  Name of the node
- **Node Type**

  Type of the node
- **Active file**

  Name of the configuration file on which the node is active.
- **Provider Name**

  Provider name
- **Version**

  Version of the diagnose configuration

- **Description**

  Configuration file description
- **Trace**

  Indicator that shows if an online trace has been started.
- **C.O**

  Shows whether the Round Robin process is activated for the logging

---

Related concepts

Online Trace on page 283

5.1.3.2 How to Display Configuration Files

How to display configuration files:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area. This list contains for each entry the detailed information.

   - **Node**

     Name of the node
   - **Node Type**

     Type of the node
   - **Active file**

     Name of the configuration file on which the node is active.
   - **Provider Name**

     Provider name
   - **Version**

     Version of the diagnose configuration
   - **Description**

     Configuration file description
   - **Trace**

     Indicator that shows if an online trace has been started.
   - **C.O**

     Shows whether the Round Robin process is activated for the logging
3) The active configuration file of a node is to be find in the list entry **Active File**.
4) To display all available configuration files of a node click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
5) Click **Close**.

5.1.3.3 How to Display Metadata of a Configuration File

How to display the configuration files:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click the name of the node the configuration file of which holds the metadata you want to display.

   Configuration Files window opens, which displays all available configuration files of the node.
4) Click the name of the configuration file for which you want to display the metadata.

   The **Configuration File** dialog opens, which displays all available metadata of the configuration file.

5.1.3.4 How to Modify Logging Cycle

For the log files each node uses a file system with several files by default. These files are filled with diagnostics data by the Round-Robin procedure. For each appender of a configuration file the following log files are used by default: One current log file and ten backup log files. Each of these files may amount up to 10MB by default

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click the name of the node for which you want to change the settings of the Round-Robin procedure.

   A dialog opens, which displays all available configuration files of the node.
4) Click the name of the configuration file for which you want to change the settings of the Round-Robin procedure.

   A dialog opens, which displays all available metadata of the configuration file.
5) Switch to the **Log File Information** tab.

6) Click the name of the appender for which you want to change the settings of the Round-Robin procedure.

   Appender Configuration window opens, which shows the settings of the Round-Robin procedure.

7) Customize the settings.
8) Click **Save**.

   The entered settings are from now on used for logging.

5.1.3.5 How to Start / Stop Cyclic Overwriting

If required, the Round-Robin procedure can be temporarily interrupted for logging. This enables the storage of diagnostics data in a single log file for a longer, consecutive period. If the Round-Robin procedure is restarted at a later date, it continues the data storage where it was interrupted.

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkboxes of the nodes for which you want to start a new log file.
4) Click **Start / Stop C.O.**.

IMPORTANT:

The Round-Robin procedure should only be interrupted for a short period. The resulting log file my otherwise become unintentionally large. This may lead to resource problems on the computer system of the relevant node.

-
- If the Round-Robin procedure is **interrupted**:

  From this point on the diagnostics data of the relevant node is not stored in the log file with the backup log files but in a single file.
- If the Round-Robin procedure is **restarted**:

  From this point on the diagnostics data of the relevant node is stored again in the log file and the backup log files

5.1.3.6 How to Activate a Loaded Configuration File

How to activate a configuration file:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
4) Select the checkbox of the configuration file that you want to activate for the node.

   NOTICE: Only one configuration file can be activated
5) Click **Activate**.

   The dialog with the additional activation information opens.
6) Enter your **User Data** and the **Reason** on the **General** tab.
7) Click **Activate**.

   The new configuration file is activated. If a configuration file was activated earlier, it will be deactivated automatically.
8) Click **Close**.

5.1.3.7 How to Upload and Activate a Configuration File

How to upload a configuration file to the node and then activate it:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkbox of the node to which you want to upload the configuration file.
4) Click **Upload to Node**.

   The file selection window opens.
5) Click **Browse**. Select the file which you want to upload to the node.
6) Click **Load**.to upload the configuration file

   The dialog with the additional activation information opens.
7) Enter **User Data** and the **Reason** on the **General** tab.
8) Click **Activate**.

   The new configuration file is activated. If a configuration file was activated earlier, it will be deactivated automatically.
9) Click **Close**.

5.1.3.8 How to Backup Configuration Files

How to export configuration files of a node:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
4) Select the checkboxes of the configuration files that you want to export.
5) Click **Download to Client PC**.

   The configuration files are loaded to the client PC as Zip file.
6) Open or save the file as usual.
7) Click **Close**.

5.1.3.9 How to Delete a Configuration File

How to delete configuration files of a node:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
4) Select the checkboxes of the configuration files that you want to delete.
5) Click **Delete**.
6) Click **OK** to confirm the deletion of the selected configuration files.

   The selected configuration files will be deleted.
7) Click **Close**.

5.1.3.10 How to Restore the Default Configuration

How to reactivate the default configuration file on a node:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   The **Configuration Files** list view opens, displaying the list of configured nodes, each with its active configuration file for Logging and Tracing.
3) Check the node´s checkbox to select the node for which you want to restore the default configuration.
4) Click **Activate default configuration**

   The default configuration file for Logging and Tracing is restored and activated for the selected node.

5.1.4 Diagnostic

The Diagnostic documents those mechanisms available in the OpenScape Voice system that accurately, quickly and efficiently collect and identify troublespots in the system. In doing so, administrators can quickly classify and categorize problem areas and thus facilitate repair time.

The following diagnostic tools or methods are outlined:

- Call Trace:

  traces one particular call; used on demand by local operating technicians to diagnose problems reported by an individual subscriber.
- Continuous Call Trace:

  traces constantly in real time.
- RTT (Real-time Trace) Methods:

  traces for a limited time after trace flags are set for a particular failure scenario; used on demand under expert supervision to diagnose OpenScape Voice server-specific voice call related troubles.
- Query of Subscriber Transient Operational Status:

  determines details about the connections active for subscribers.
- Process Debug Tool:

  provides online debug options allowing different levels of logging and tracing.
- DIPAZ (Data Storage Indexing and Compressing) tool:

  is a component of OSVTM (Openscape Voice Trace Manager) that reads the trace files, indexes them and creates compressed trace files and PCAP (Packet Capture)t) files.
- FADE:

  is a component of OSVTM (Openscape Voice Trace Manager) that is responsible for freezing trace files of a particular time frame, selecting trace files, analyzing selected trace files and exporting selected files
- Quasi-Real-Time Network Health Visuals:

  is a component of OSVTM (Openscape Voice Trace Manager)that is to visualize service affecting network conditions and to localize them to repairable network elements in a clearly arranged manner.

5.1.4.1 Diagnostics Data

Internal system processes are logged for the entire system in the background and saved as diagnostics data. The configuration files activated on a node determine which specific diagnostics data is recorded.

Functional Sequence

The diagnostics data for each node is recorded individually in log files (*.xml). The diagnostics data for all nodes can be downloaded in the form of a compressed diagnostics file. You can optionally download all saved diagnostics data or selected information (diagnostics components). The diagnostics components offered for downloading depends on the node and the installed applications.

It is also possible to initiate logging with a new diagnostics file to provide better transparency when troubleshooting errors, for example. The data will then be written to a new diagnostics file from that point onward.

5.1.4.2 How to Export Diagnostics Data

How to export diagnostics data

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Diagnostics Data Download** in the navigation tree.

   The window **Export diagnostics data** opens.
3) Select the checkboxes of the components that diagnostics data you want to export.
4) Click **Export**.
5) A Zip file is loaded to the client PC, which you can view and/or save as usual.

   The Zip file contains two ZIP files. One contains configuration data, the other# contains framework or OpenScape logging data.
6) Click **Close**.

5.1.4.3 How to Start a New Diagnostics Log File

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.

2) Navigate to **Tools&Utilities** > **Configuration Files**in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkboxes of the nodes for which you want to start a new diagnostics file.
4) Click **Start new Log File**.
   The diagnostics data logged from now on are saved in new diagnostics files for the selected nodes. The old diagnostics files are saved in the `/log` directory of the respective nodes.

5.1.4.4 Online Trace

An online trace can be used to output the diagnostics data of all nodes to an external diagnostics tool.

Functional Sequence

A network port is reserved for transmitting diagnostics data via an online trace.If this port is already being used by another application, then the port for transmitting diagnostics data must be changed. Subsequently, the port in the diagnostics tool must also be modified to the same value

System Specific Information

Since the transmission of the diagnostics data does not occur via a secure protocol, no security mechanisms such as authentication or encryption are possible. If the diagnostics data is to be transmitted over unsecured networks, it is necessary to also use IPSec for this purpose.

Related concepts

Configuration Files on page 275

5.1.4.5 How to Start / Stop an Online Trace

How to start/stop the online trace:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkboxes of the nodes for which you want to start the online trace.
4) Click **Start / Stop Trace**.
   The online trace is subsequently started / stopped.
5) Invoke the external diagnostics tool to receive the diagnostics data.

5.1.4.6 How to Download Trace Files

How to Download Trace Files:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Trace File** in the navigation tree.

   The **Generate and Download Trace Files** window opens.
3) Click **Start**.
   The generation of trace file for download is started.
4) Click **Download**.
   The online trace is subsequently downloaded. Trace files can also be found in folder `/enterprise/trace` or `/opt/siemens/trace` for onboard or external assistant, respectively.
5) Click **Close**.

5.1.4.7 How to Change the Port for an Online Trace

How to change the port for an online trace:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Inventory** navigation menu item.
2) In the navigation tree click **System Status** > **Nodes**.

   A list of all system nodes and external links available in the entire system is displayed in the work area.
3) Click the system node name on which OpenScape UC Application is installed.

   A dashboard of the selected node opens.
4) Click **Show** next to **Actions** - **Show services status**.
   A dialog box opens with a list of all components that are available for the selected system node.
5) Look in the list for the **Online Trace** component and select the associated checkbox.
6) Stop the online trace if running: Click **Start / Stop**.

   The **Online Trace** is stopped.
7) Click **Edit**.

   The dialog with the settings of the Online Trace component opens.
8) Enter the port number that is to be used for the online trace in the **portNr.** field.

9) Click **Save**.

   The dialog with the settings of the **Online Trace** component opens.

10) Verify that in the components list the checkbox for the **Online Trace** component is still selected.

11) Click **Start / Stop**.

    The Online Trace is started with the new settings.

12) Change in the external diagnostics tool the communication port used to the same value.

5.1.4.8 Online Trace Tools

The online trace tools consist of a set of RTT command utilities and scripts that mainly control the activation and capture of RTT trace on the OpenScape Voice system. Some capabilities are provided for online trace decoding and analysis however these are not recommended for use on a live switch due to possible system performance impacts.

Administration of the online RTT subsystem is done using a set of RTT command line utilities and/or the RTP Command Line Interface (CLI). The following sections describe the functional details of each of these command interfaces.

The following command line utilities exist as part of the RTT feature:

- `oprtt_ctl` - controls which trace records are captured.
- `oprtt_read` - reads and displays captured trace records
- `OP_RTT_READ` - wrapper around the oprtt_read command to handle file aging.
- `oprtt_startup_ctl` - controls the initialization of RTT flags on process startup.

  When activated, the command oprtt_startup_ctl will allow RTT to continue tracing a particular process, even if such process restarts and generates a pstack core dump. By doing so, service staff will be able to capture traces for further investigation on a server that is experiencing frequent pstacks.
- `createRttOff` - Offline tool package creation script.

5.1.5 Dashboard

Dashboard is the tool for status visibility and access to all system components (OpenScape Voice, integrated Media Server, phones, and gateways).

Dashboard

The Dashboard is a status display tool showing the current system alarm and system operating status information of a specific switch in a simple and intuitive form.

Once the Common Management Platform has started, system information and information relating to the applications installed, subdivided into a number of areas, is displayed in the work area. Some of the areas are independent of the system and are always displayed, other areas are displayed depending on the installed systems and applications. The areas described below are always displayed.

The Dashboard comprises the following areas:

- Alarm summary

  for Component and Shared Services
- System Info

  CPU and Memory Load/Date/Time/Last Reboot
- Status

  Operational /Redundancy Status/Servers
- Applications

  Application/Software Version

  The application **Name** and the **Software Version** are displayed with the following naming convention:

  Vx Ry.p.e

  Where:

  x=Major Release

  y=Minor Release

  p=Patchset

  e=Emergency Patch

  For example, V7 R1.5.2 means Version 7,minor release 1,patchset 5,emergency patch 2
- Actions
  - Rapidstat Messages (Check Node Health)

    Rapid Stat can display system health information on the screen. When the system information report is completed, you can click F5 key to refresh the form. Page is automatically refreshed every one minute.
  - Services Status

    List of Components/Alarms/State/Version

    Functions: Edit, Restart, Stop
  - Software Packages

    Software/Version/Installation Media/Date/Update Media/Date
- Note

  General information and private notes.

5.1.5.1 How to Launch Dashboard

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to **Common Management Platform**.
Enter the user name and password.

2) Select the domain from **Domain** selection list.

3) Navigate to **Maintenance** > **Inventory** > **Nodes& Applications > Nodes**.
4) Select a node in the **Nodes** list view by clicking on the node's name.

   The **Dashboard** opens, displaying the system status of the selected node.

5.1.6 RapidStat

RapidStat provides a means to collect system health status information before and after scheduled maintenance activities such as the following: Generic software upgrades, patching, system maintenance releases, hardware repair, log file retrieval for debugging and repair and other activities as determined by administrators and/or local operating procedures.

This tool eliminates the need to manually perform the system interrogation required to verify system health, which reduces human error and escalations. As a result, maintenance activities are reduced and potential service impacts (outages) can be avoided.

In addition, it supports pro-active surveillance by Network Operations Centers (NOCs) because it can be configured to automatically run at specified times during the day, and generates an alarm (Simple Network Management Protocol (SNMP) trap) if an irregularity is found.

If RapidStat finds irregularities, that alerts operators to irregularities that may cause or lead to service degradation, and may not otherwise be alarmed.

Functional Sequence

RapidStat has the following modes of operation:

- Status display mode

  It generates a system health report for immediate analysis. RapidStat can also be configured to run in status display mode periodically as a cron-job. It is recommended that it be run twice daily, at the following times, to generate an alarm (SNMP trap) if an irregularity is found:

  – Just before the business opens for the day.
  – At a low traffic period during open hours, for example, lunchtime
- Data collection mode

  It executes debugging commands, collects resulting log files, and prepares a file that can be securely sent to authorized service personnel for further analysis.

System Specific Information

RapidStat:

- Reports the system configuration type (specified by node.cfg), e.g., Integrated Simplex, Standard Duplex, Integrated Duplex, Geo-Redundant.

- Checks the status of only the components (HW and SW) present for a given system configuration (specified by node.cfg).

  It does not report "missing" components that are not valid for the given configuration. This check has be restricted to OpenScape Voice application only.

  NOTICE:

  No hardware check will be done on virtual systems.

- Verifies cluster status and ensures that shutdown agent files are identical on both nodes.
- Checks disk partitioning scheme (imaged or non-imaged, if imaged reports alss active/fallback partitions and their load) and disku usage.
- Verifies that survival authority IP is configured (for geo-separated and virtual standard duplex systems).
- Compares Rtp configuration between nodes, checks the value of HealthcheckSignal against default and report differences..
- Checks the number of subscribers registered on each node and reports a warning if an imbalance higher than 20% is found.
- Provides a "Warning" if the SIP endpoint registration audit is disabled. (RTP parameter Srx/Xdm/ProcessAuditFlag has value 0).

Other Characteristics

RapidStat is executed by running a script as a Linux user on OpenScape Voice. It can also be invoked via the OpenScape Voice Assistant GUI. Status Display mode can also be configured to run periodically, at a certain time, at least twice daily.

Carrier specific platform and service health indicators are no longer reported.

Updates are introduced to accommodate changes in HW platforms, and OpenScape Voice configurations specific to Enterprise deployments.

Run time performance is optimized for Enterprise deployments.

5.1.6.1 Automatic Operation and Alarm Generation

The RapidStat tool automatically runs and generates an alarm (SNMP trap), if an irregularity is found. This behavior includes a state-lock (anti-concurrent) mechanism in order to avoid the generation of false alarms and prohibit multiple instances of RapidStat's operation (especially when running as a cron-job).

These enhancements support pro-active surveillance by Network Operations Centers (NOCs).

RapidStat, in status display mode, should be configured as a timed job ("cronjob"), to run just before business open hour, and at a low traffic period during open hours (e.g., such as lunch time). RapidStat's scheduled functionality must be configured manually by maintenance personnel.

IMPORTANT:

Improper configuration or usage of a scheduled RapidStat operation is a responsibility held by maintenance personnel only. Development cannot provide information on how to

address issues of such nature since scheduled configuration of RapidStat (as a cron-job) may vary from customer to customer.

During its initialization, RapidStat looks for a file that states its operating status (running or not running). If no other instance of RapidStat is running, then it generates the file that states its operation (and propagates it to the other node, for cluster systems). Otherwise, if RapidStat is already running, it notifies the enduser (or the application that invoked it) that it will exit (because it is already running) and exits. After passing the checkpoint regarding its operating status, RapidStat checks if an alarm is generated by a previous operation and if that is true, then it clears the alarm.

If any error or warning messages are produced during RapidStat's operation, then it generates an alarm based on the existing API /CLI "SendAlarm()".

The FaultyObject of the minor alarm will be:

<node-id>/RapidStat/Error

or

<node-id>/RapidStat/Warning.

IMPORTANT:

If RapidStat is invoked in a very short timeframe prior to its scheduled operation (as a cron-job), then (based on its anti-concurrent mechanism) the scheduled operation of RapidStat will be automatically canceled. This will not affect the generation of an alarm by the current operating mode of RapidStat.

5.1.6.2 Content of Crontab File for RapidStat

The crontab command creates a crontab file containing commands and how often cron should execute them. Each entry in a crontab file consists of six fields separated by spaces.

Functional Sequence

Each entry in a crontab file consists of six fields separated by spaces and is formatted as follows:

```
minute hour day month day-of-week command_to_be_executed
```

System Specific Information

The acceptable values for each of the six fields in the crontab file. The first five are integer patterns, and the sixth is the command to be executed.

Field	Description	Range of Value
minute	The exact minute that the command sequence executes.	0-59
hour	The hour of the day that the command sequence executes.	0-23

Field	Description	Range of Value
day of the month	The day of the month that the command sequence executes.	1-31
month	The month of the year that the command sequence executes.	1-12
day of the week	The day of the week that the command sequence executes.	0-7 (where both 0 and 7 mean Sun, 1 = Mon, 2 = Tue, etc)
command_to_be_executed	The complete command sequence variable that is to be executed.	The command to run along with the parameters to that command, if any.

Each of the patterns from the first five fields may either be an asterisk (*) (meaning all legal values) or a list of elements separated by commas. An element is either a number or two numbers separated by a minus sign (meaning an inclusive range).

NOTICE:

Note that the specification of days may be made by two fields (day of the month and day of the week). If both are specified as a list of elements, both are followed.

Related concepts

Common Options on page 292

Related tasks

How to Configure RapidStat as a Cronjob on page 290
How to Configure RapidStat Cronjob - Example Week on page 300
How to Configure RapidStat Cronjob - Example Sunday on page 301

5.1.6.3 How to Configure RapidStat as a Cronjob

This task presents an example on how to configure RapidStat as a cron-job. It is a guideline to show how to schedule RapidStat to run in a specific time and what type of alarm(s) should be expected in case of warnings or errors. These alarms indicate to NOC personnel that there might be potential issues and they are highly advised to run RapidStat (in status display mode) for detailed information.

Prerequisites

It is recommended that configuring RapidStat as a cron-job be done by administrators who have experience using a Linux-based operating system.

Adequate administrative permissions

IMPORTANT:

If RapidStat is invoked in a very short timeframe prior to its scheduled operation (as a cron-job), then (based on its anti-concurrent mechanism) the scheduled operation of RapidStat will be automatically canceled. This will not affect the generation of an alarm by the currently running RapidStat job.

Step by Step

1) Open the `crontab` file in Edit mode (as root).
2) Enter the command `crontab -e`.

   The crontab file is now open and ready for editing. The output may look like the following:

   ```
   # DO NOT EDIT THIS FILE - edit the master and
   reinstall.# (garb installed on Fri May 23 13:57:56
   2008)# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17
   03:20:37vixie Exp $)# DO NOT EDIT THIS FILE - edit
   the master and reinstall.# (tf2 installed on Fri May
   23 13:57:22 2008)# (Cron version -- $Id: crontab.c,v
   2.13 1994/01/17 03:20:37vixie Exp $)# DO NOT EDIT
   THIS FILE - edit the master and reinstall.# (/var/
   tmp/root.9941 installed on Fri May 23 13:32:34 2008)#
   (Cron version -- $Id: crontab.c,v 2.13 1994/01/17
   03:20:37vixie Exp $)# EMANATE: restarts daemons that
   died0,5,10,15,20,25,30,35,40,45,50,55 * * * * /bin/sh
   -c "[ -x/usr/share/SMAWemanate/bin/EMANATEcron ] && /
   usr/share/SMAWemanate/bin/EMANATEcron"1 0 * * * su -
   srx -c /unisphere/srx3000/srx/bin/SrxUscCDRDelete > /
   log/SrxUscCDRDelete.log## Admin Login Account Monitor##
   The program "cronjob.srx" runs as root. It must be in
   synchwith cronjob.srx# Author: John Smith#01 06 * * * /
   etc/cronjob.sys*/2 * * * * /opt/unisphere/srx3000/cla/
   bin/checkcla
   ```
3) Enter the values for time and date that the command sequence executes and the complete command sequence variable that is to be executed.
4) From the Edit mode, close the crontab file.
5) Type the following command to verify the changes: `crontab -l` (letter L lowercase).

Next steps

To run RapidStat twice daily you would add another crontab entry.

The naming convention for the `RapidStat.out` and `RapidStat.error` files should be different in this case.

```
13 6 * * * /unisphere/srx3000/srx/bin/RapidStat -b -R > /
log/RapidStat1.out 2>/log/RapidStat1.error
```

```
15 12 * * * /unisphere/srx3000/srx/bin/RapidStat -b -R > /
log/RapidStat2.out 2>/log/RapidStat2.error
```

These entries would run RapidStat at 0613 and 1215 hours daily. This syntax is used on a cluster node.

For a simplex node the `-b` option would be replaced with `-t`.

Related concepts

Content of Crontab File for RapidStat on page 289

Related tasks

How to Configure RapidStat Cronjob - Example Week on page 300
How to Configure RapidStat Cronjob - Example Sunday on page 301

5.1.6.4 Common Options

In conjunction with the -s (Status Display mode) and -c (Data Collection mode) options, more options may be used to automate the use of the RapidStat tool.

The following options may be used:

NOTICE:

If `-t` or `-b` flags are not used, in cluster systems, RapidStat asks whether to run it on the other node as well.

Command Option	Description
-t	Checks only the node where the script is run (it will not check the other node)
-b	Checks both nodes (for cluster systems)
-v	Displays only software versions
-s	Displays System Status (functions as running ./RapidStat)
-c	Collects information report (and put them in compressed tar.gz files)
-R	Suppress printing of rotating activity symbol
-h	Displays a help page with all modes for standalone operation

Related concepts

Content of Crontab File for RapidStat on page 289

5.1.6.5 Checks of RapidStat

Specific checks of the health of the system can be assigned by the administrator in RapidStat.

The table lists the particular commands of a RapidStat check.

Task	Check
SMU STATE	Check **Split Mode Upgrade** (SMU) status by looking `/lock/state.lock` file.

Task	Check
Checking the SSH connection with remote node	Use `srxqry-s` check to determine the communication status between the two nodes. Report an error if a timeout occurred (while trying to connect to the other node).
Comparing Date Comparing Time Comparing Time Zone	Execute date cmd (locally and remotely) and report time and timezone differences.
Daylight Saving Time Settings	Execute `date` and `/etc/localtime` (locally and and remotely). Report differences found in Daylight Saving Time Settings.
Checking HWClock	Grep hardware clock characteristics from `/etc/sysconfig/clock` (UTC or Local Time)
NTP server(s)	Use **ntpq** utility to query NTP servers IPs defined in `node.cfg`. Report if synchronised or not. Report a warning in case none of them corresponds to a synchronised server. Report an error in case there is no NTP IP defined but their number is greater than zero.
Solid Version Solid Role Solid Status Solid Merge Count	Display DB info through `solsql` commands: • `Role` (displays the hotstandby (hsb) state, e.g. `PRIMARY/SECONDARY/STANDALONE`) • `Version` (displays the actual solidDB version) • Status (displays the status of solidDB database, ACTIVE/ALONE) • Merge Count (displays the solidDB status regarding size of Bonsai Tree). Report an error when count greater than limit of 10,000. This error is an indication of uncommitted transactions.
Local Node Remote Node Signaling Managers: This Node: Signaling Managers: Remote Node	Analyse the **srxqry** output in terms of RTP and signaling managers state (Status of all hiPath and RTP processes).
Cluster Status	Report online node(s)

Task	Check
• Checking SSH keys for user srx host: node1name node2name clusternode1-priv clusternode2-priv • Checking SSH keys for user root host: node1name node2name clusternode1-priv clusternode2-priv	Check SSH keys by remote shell (rsh) cmd in hostX (`node1name, clusternode1-priv, node2name, clusternode2-priv`), as userY (`root, srx`). Report an error if permission denied or the other node is inaccessible (ping test fails).
Comparing Patch Levels (pkgversion) Comparing Patch Levels (pkginfo) Comparing PatchSet Level	• Check for partially installed patches on each node (`pkgversion -p`). • Compare patch levels (`pkgversion -ps` and `pkginfo`) between two nodes. • Compare patchset levels between two nodes.
Comparing Binaries with `pkgversion`	Compare all HiPath binaries versions (fileversion) with the patchset versions (`pkgversion`). Report an error if there is a mismatch.
Checking for Upgrade flag	Check if a **Rolling Upgrade** procedure is in progress. Report an error if rolling upgrade flags are on the system.
Checking RTP/ HiPath8000 Processes	Obtain a list of all RTP/hiPath processes (`srxqry -v`) to verify that all are running.Report an error if at least one is in **NOT_RUNNING** state.
Checking for MOP information (Installation/ Removal) MOP information for: node1name node2name Looking for differences in MOPs	Check for differences between MOP install/removal procedures. Report MOPs installed in each node (`pkgversion -m`). Report differences found (`pkgversion -m` in both local and remote)

Task	Check
Testing Soap Communication Link Testing SoapServer Database Access Number Of Subscribers	Testing Soap Communication Link by **TestSendSoapReq** script. Perform a Soap Server Database Access test by requesting the Number Of Subscribers. Report an error if unable to connect.
Number of Subs in RSS	Display the number of subscribers in RSS shared memory using **rsstest**
Checking SIP endpoint registration audit	Report the state of SIP endpoint registration audit (enabled/disabled) by checking the Srx/Xdm/ProcessAuditFlag RTP parameter value (RtpCfgShow)
License Usage Violations	Report a warning if any License Usage Violations found (cmd licEndPointDisplay in RtpAdmCli). Display License Usage Indicator information.
Subscribers balancing (registered endpoints)	Connect in Solid Db and perform a `solsql` command to read the registered endpoints counter. Display the number of subscribers assigned (on each node and in totally). Report a warning if imbalance between the two nodes if found.
Number of MG's in RTM Number of MG's in DB	Display the number of MGs stored in Database and in RTM shared memory (`callp/bin/smm`). Report an error if a mismatch found.
Number of DNs in DB Number of Office Codes in DB	Perform a Solid DB read and display number of DNs (E164_DN_T) and number of office codes (E164_OFFICE_CODE_T).
Checking DNS configuration	The `/etc/resolv.conf` file is checked and the following cases are examined: **1)** If valid but no name servers included, report that the test is skipped. **2)** If valid and name servers included, for all IPs, check DNS communication via the dig cmd in a bogus FQDN. Report any warnings/errors depending the response time. **3)** If invalid, report an error.
Mount points	Use `df` cmd and verify that the following mount points exist: `/dev`, `/cdr`, `/global`, `/home`, `/log`, `/opt`, `/software`, `/tmp`, `/tpa`, `/unisphere`, `/var`. Report an error in case at least one is not shown.

Task	Check
Checking RTP **HealthcheckSignal**	Verify that the value (through `RtpCfgShow`) of the RTP parameter **Rtp/Nm/HealthcheckSignal** is equal to 6 (allow core files generation). Report an error if not.

Task	Check
Comparing `.tcn` and `.parm` files located at `$RTP_HOME/cust_conf` from both nodes. Copying `node1name` files to: `/tmp/RapidStat_tmp/node1name /cust_conf` Copying `node2name` files to: `/tmp/RapidStat_tmp/node2name /cust_conf` Comparing files located at `$RTP_HOME/conf` from both nodes. Copying `node1name` files to: `/tmp/RapidStat_tmp/node1name /conf` Copying `node2name` files to: `/tmp/RapidStat_tmp/node2name /conf` Comparing non .parm and .tcn files located at `$RTP_HOME/cust_conf` from both nodes. Copying `node1name` files to: `/tmp/RapidStat_tmp/node1name /non_cust_conf` Copying `node2name` files to: `/tmp/RapidStat_tmp/`	Compare `$RTP_HOME/conf` and `$RTP_HOME/cust_conf` directories of both nodes and report an error if RTP conf differs.

Task	Check
`node2name / non_cust_conf`	
Checking `startRTP.pl`...	Verify that there is not a defunct `startRTP.pl` process in the system and report a warning if not.
Shutdown Agent status retrieval	Retrieve the status of the stonith device configured as shutdown agent.
Checking if CLA is running in local_node_name	Check CL A status and report a warning if not running.
Comparing HWClock and OS time	Use `date` and `hwclock` commands. Compare OS time and hardware clock time and report any differences.
Display Node Weight	Display the `/usr/bin/cl_status` output. The weight, agent and timeout parameters are populated with their respective values.
Compare `saDevSwitch.cfg` (shutdown agent files) from both nodes	Compare shutdown agent file of both nodes and report an error if differences found.
Partition Scheme	Determine node's partition scheme (PRIMARY/ SECONDARY/NON_IMAGED). Verify disk usage is not high on any partition. Report a warning if the disk utilization of at least one mount point is more than 60%.
Checking directory / var/mail	Display the total size of `/var/mail` directory and report a warning if more than 1KB. Check the size of files contained in `/var/mail` and display those that have some data (>1B).
Disk info	Display disk group status. Report an error if disk information is not available or RAID is not configured.
Bond Groups	Display bond groups' info (**Bond/Interface/Status**). Report an report an error if no bonding devices are found.
Checking Snort	Verify that snort is running properly and report a warning if not.
Interfaces Info	Display interfaces info (**Interface/Speed/Duplex/ Auto_Neg/Link_Status**). Report a warning if an interface is down or runs in half-duplex mode.

Task	Check
Network Interface Quality Summary	Display Network interface statistics using the `/proc/net/dev` file
Checking DROP policy entry in chain 9000	Checking if there is a DROP policy entry in chain 9000 and report an error if missing.
Checking for locked Semaphores	Check all semaphores and for those that are locked at the moment in time. Determine the time of the last action and flag an error if the lock time is over 1 sec.
Checking UCE Context usage	Use the RTP utility "RtpCtxDiagSnap" to check RTP Context Usage. Report a warning if the usage threshold of 75% is reached.
pstacks within the last 24hrs	Check for core dumps found in `/software/rtpcore/` in the last 24h. Report a warning if **pstacks** found.
Binaries	Check binaries for valid version labels. Report an error if binaries with unknown labels found.
Checking Test Call Generator	For each **Test Call Generator** process, get current state/status.
Checking SNMP daemon Checking SNMP response	Check that SNMP deamon is running and is responding to a request (`getone`). Report an error if not running or/ and not responding.
Checking if auditing is enabled in current node	Get the current status of audit (`auditctl -s`) and check if it is enabled.
Checking CDR method	Checking CDR method (**mainGetOfficeWideParm** in **RtpAdmCli**) and display if configured PULL or PUSH.
Process Utilization	Check process CPU utilization. Report a warning if there is a process over the usage threshold of 10%.
Checking for RTT facilities.	Checking if there are processes being traced by an RTT facility.Report a warning if one or more processes found.
Checking FTP connectivity	Verify that there is Ftp connectivity using `UscFtpTest` and report an error if not.
Checking if elements in use exceed 60%	Display sipsm shared memory status (`sipsmdump`). Report a warning if there are elements in use that exceed threshold of 60%.
Call Statistics Snapshot	Display UCE call statistics from Solid DB.
Memory Usage	Display a snap shot of system memory usage through `vmstat`.

Task	Check
Platform compatibility check	It checks motherboards for supported motherboards etc. Performed with: `platform_detection.sh`

5.1.6.6 How to Configure RapidStat Cronjob - Example Week

RapidStat must run each night at 11.30 pm EST.

Prerequisites

It is recommended that configuring RapidStat as a cronjob be done by administrators who have experience using a Linux-based operating system.

Adequate administrative permissions

Step by Step

1) Depending on the system, the following crontab line is input:

- For simplex node:

```
30 23 * * * /bin/ksh /unisphere/srx3000/srx/
bin/RapidStat -t -R > /log/RapidStat.out 2>/log/
RapidStat.error
```

- For cluster node:

```
30 23 * * * /bin/ksh /unisphere/srx3000/srx/
bin/RapidStat -b -R > /log/RapidStat.out 2>/log/
RapidStat.error
```

NOTICE:

Whereas:

30 - represents the minute of cron work

23 - represents the hour of the day

* - represents every day, month, and weekday.

IMPORTANT:

With the syntax indicated for the cluster RapidStat will be run on both nodes. There is no need for a RapidStat crontab entry on the partner node.

---

2) From the Edit mode, close the crontab file.

3) Type the following command to verify the changes: `crontab -l` (letter L lowercase).

Related concepts

Content of Crontab File for RapidStat on page 289

Related tasks

How to Configure RapidStat as a Cronjob on page 290

5.1.6.7 How to Configure RapidStat Cronjob - Example Sunday

RapidStat must run every Sunday at 11.30 pm EST.

Prerequisites

It is recommended that configuring RapidStat as a cronjob be done by administrators who have experience using a Linux-based operating system.

Adequate administrative permissions

Step by Step

1) Depending on the system, the following crontab line is input:

- For simplex node:

  ```
  30 23 * * 0 /bin/ksh /unisphere/srx3000/srx/
  bin/RapidStat -t -R > /log/RapidStat.out 2>/log/
  RapidStat.error
  ```

- For cluster node:

  ```
  30 23 * * 0 /bin/ksh /unisphere/srx3000/srx/
  bin/RapidStat -b -R > /log/RapidStat.out 2>/log/
  RapidStat.error
  ```

  NOTICE:

  Whereas:

  30 - represents the minute of cron work

  23 - represents the hour of the day

  * - represents every date, every month

  0 - represents Sunday

  IMPORTANT:

  With the syntax indicated for the cluster RapidStat will be run on both nodes. There is no need for a RapidStat crontab entry on the partner node.

2) From the Edit mode, close the crontab file.

3) Type the following command to verify the changes: `crontab -l` (letter L lowercase).

Related concepts

Content of Crontab File for RapidStat on page 289

Related tasks

How to Configure RapidStat as a Cronjob on page 290

5.1.6.8 How to Create a System Information Report with RapidStat

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes& Applications** > **Nodes**.

   A list of all system nodes and 3rd party system connections available in the entire system is displayed.
2) Click on the **Name** of the Communication System (OSV) node.

   NOTICE:

   Reports of OpenScape Branch nodes are described in the OpenScape Branch documentation.
3) In the **Dashboard** go to area **Actions**. Select the corresponding **Rapidstat** and click **Start**.
4) Mark the checkbox **Collect system information report**.
5) Click **RapidStat**.

5.1.7 Audit Log

The audit log logs all important activities performed by the Common Management Platform users. Activities comprise all entries and actions at the Common Management Platform.

5.1.7.1 System and Security Log Concept

The System and Security logs register all important activities performed by the Common Management Platform users. Activities comprise all entries and actions at the Common Management Platform.

The size and number of log files can be defined. If the definable size of the log file is exceeded, the file is automatically closed and backed up, and a new file is created.

The System and Security log can be exported and saved as log file. Older log files with past activities can be imported in the system.

System and Security Specific Information

The log files delivers the following information:

- **Date/Time**: Shows the date and time stamp of the logged activities.
- **User**: Shows the user of the logged activities.
- **Command**: Displays the executed action or command.
- **Result**: Shows the result of the activity or command.
- **Additional Info**: Shows additional information on the activity or command, as e.g. JobName and JobInfo.
- **Parameters**: Shows additional parameter information on the activity or command.

5.1.7.2 Backing up the Log Files

In order to keep the storage space required for log files within reasonable limits, older log files are deleted automatically when the number of files exceeds a definable value.

If the log files to be backed up permanently, the backup unit audit log files must be included in the backup concept of Common Management Platform.

NOTICE: According to the concept of Common Management Platform the audit log files will be backed up as an encrypted file.

It is recommended to create a scheduled backup for this purpose.

So that you can configure an appropriate backup interval for this scheduled backup, you need to previously determine how long it takes until the log file created first is deleted.

5.1.7.3 SysLog

SysLog is an external program which is used to display the System and Security logs.

If the Common Management Platform is installed on several computer systems, the activities of all computer systems can also be forwarded via Syslog. In order to do this, the service must be enabled for each computer system and the IP address of the SysLog server must be configured.

IMPORTANT:

Since the transmission of the System or/and Security log with SysLog does not occur via a secure protocol, no security mechanisms such as authentication or encryption are possible.

SysLog should therefore only be used in secure networks.

If the System or/and Security log is to be transmitted over unsecured networks, it is necessary to also use IPSec for this purpose.

5.1.7.4 How to Display an Audit Log

Display of all logged activities.

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP.

2) Select the desired domain from the **Domain** list in the system bar.

3) Navigate to **Operation & Maintenance** > **Configuration & Monitoring**.

4) Click **Audit Log**.

   A list of all activities logged for the relevant node appears in the work area.
5) Click on the date/ time specification of the activity for which you want to display the details.

   The dialog with the associated activity details opens.
6) Click tabs **General** and **Parameters**.

   This displays the detailed information.
7) Click **Close** to close the activity details window.

5.1.7.5 How to Export a System Log

For externally processing audit logs can be exported and saved as log file.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree click **Logs** > **System**.
3) Select the audit log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the work area.
4) Click **Download**.

   The audit log data is downloaded from the server and saved in an XML file.

5.1.7.6 How to Load a System Log

How you can import exported System log data in the system

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System**.
3) Select the audit log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the work area.
4) Click **Choose audit file**.

   A window with all loadable log files opens.
5) Select the desired log file.
6) Click **Save**.

   The System log data from the selected log file is imported in the system and displayed in the activities list.

5.1.7.7 How to Enable SysLog for the System or/and SecurityLog

Activation of Syslog to transfer the System or/and Security log to an external program.

Prerequisites

Adequate administrative permissions

If Syslog is used in a system configuration with several nodes, it must be activated for each node.

Step by Step

1) On the **Maintenance** navigation tab, click on the **Inventory** navigation menu item.
2) In the navigation tree, click on **Nodes**

   A list of all system nodes and external links available in the entire system is displayed in the work area
3) Click on the name of the system node you want activate SysLog.

   A dialog box with the dashboard of the selected node opens
4) Click on **Show** next to **Actions** -**Show Service Status**

   A list of all components available on the selected application computer appears in the working area.
5) Mark checkbox **Syslog Audit Component** in the component list.
   - The Syslog Audit Component has been stopped, continue with step 7.
   - Otherwise, continue with step 6.
6) Click **Start / Stop** to stop the component.
7) Click **Edit**.

   A window that displays the component's settings opens.
8) Enter the IP address of the desired Syslog server in the **SyslogHost** field.
9) In the active field enter the true value.
10) Click **Save**.
11) Make sure that the **Syslog Audit Component** component is still selected.
12) Click **Start / Stop**.

    The Syslog Audit Component component is started with the new settings.

5.1.7.8 How to Estimate Backup Interval

If you want the log files to be backed up permanently, the backup unit audit log files must be included in the backup concept of Common Management Platform. You should create a scheduled backup for this purpose. To configure an appropriate backup interval for this scheduled backup, you need to previously determine how long it takes until the log file created first is deleted. In order to estimate the backup interval, you will need to know the maximum size of the audit log file (maxFileSize) and the maximum number of log files (maxBackupIndex). These values are predefined.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab, click on the **Inventory** navigation menu item.
2) In the navigation tree, click on **Nodes**

   A list of all system nodes and external links available in the entire system is displayed in the work area
3) Click on the name of the system node you want activate SysLog.

   A dialog box with the dashboard of the selected node opens
4) Click on **Show** next to **Actions** -**Show Services Status**

   A list of all components available on the selected application computer appears in the working area.
5) In the components list look for the **log file audit component** and click on the component's name.

   A window that displays the component's settings opens.
6) Note down the values under maxFileSize and maxBackupIndex, respectively.

   Default values: maxFileSize=4000k , maxBackupIndex=50.
7) Click on **Cancel** to close the window with the component's settings without modification.
8) Calculate the storage space by using the formula:

   Storage space=maxFileSize×maxBackupIndex

   With the above default values, the storage space would be 200 MB (4000000 × 50; max 50 files of 4 MB each).
9) Calculate the maximum number of entries by using the formula:

   Max. number of entries = storage space / 2000

   The size of an entry is approximately 2 KB. With a storage space of 200 MB, this amounts to a maximum of 100000 possible entries in all log files.
10) Estimate how many entries are written per day, e.g. 1000 entries per day.
11) Divide the maximum possible number of entries by the number of entries approximately written per day: 100000/1000=100

    In the example, the maximum possible number of entries is written after 100 days. Subsequently, the log files created first will already be deleted again.

    In the example, the backup interval should therefore be less than 100 days.

5.1.7.9 How to Set Filter for a System Log

The search for specific activities can be defined by search criteria in a filter. Once a filter is selected, only specific activities matching the criteria defined in the selected filter will be displayed. This reduces the total number of activities displayed and makes it easier to find a specific activity or group of activities.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System**.
3) Select the System log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the working area.
4) Click **Advanced**.

   The dialog with the filter settings opens.
5) If you want to filter according to a specific time range or specific user groups,click on the **General** tab and specify the desired filter settings.
6) If you want to filter commands according to certain categories, click the **Category** tab and select the desired category.
7) If you want to filter entries according to successful and/ or faulty entries, click the **Result** tab and mark the desired checkbox.
8) If you want to filter the entries according to a term in the additional information, click the **Additional Info** tab and enter the search item under **Filter information**. You can also enter a term that is only part of the full range of additional information.
9) If you want to filter the entries according to a parameter, click the **Parameters** tab and enter the search term under **Parameter string**. You can also enter a term that is only part of the full range of parameters.
10) Click **Apply**.

    The System log will only display activities that correspond to the filter settings made.

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

5.1.7.10 How to Change a Filter for System or/and Security Log

How to change a filter for System or/and Security Log:

Prerequisites

Adequate administrative permissions

A filter was set, this is indicated in the **Filter** field.

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System** or **Security**.
3) Select the System log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the working area.
4) Click **Advanced**.

   The dialog with the current settings of the applied filter opens.

5) Make your changes to the filter settings.
6) Click **Apply**.

   The audit log will only display activities that correspond to the filter settings made.

5.1.7.11 How to Clear Filter for System Log

How to clear filter for System Logs:

Prerequisites

Adequate administrative permissions

A filter was set, this is indicated in the **Filter** field.

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System**.
3) Select the System log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the working area.
4) Click **Show All**.

   The **Filter** field displays **No filter applied** and the activities list contains all activities again.

5.1.8 VIP Fault Detection and Alarming

The feature is for identifying a number of subscriber or endpoint problem conditions which might occur and can be monitored within the OpenScape Voice server. These types of issues are to be looked for and then logged. For special DNs (Directory Numbers) called VIPs (Very Important Persons), a special processing is done for the purpose of notifying administrators of these conditions. The monitored conditions are the following: registration timeouts/ failures (including digest authentication and multiple prime line registrations with different IPs failures), transaction timeout and configuration failures (subscription/registration).

Properties of the monitored conditions are:

- Registration Timeouts: This kind of failure is identified by the Registration Audit within the OpenScape Voice. This audit runs periodically and identifies when a registration has exceeded it's time to live value. Then the audit automatically performs a de-registration. This de-registration record will then be logged.

  Registration Failures: If a DN attempts to register and fails the Digest Authentication challenge or attempts to register as a Primary line but with a different IP than already registered, then these will be logged as well.
- Transaction Timeout: Within the SIP protocol, many messages sent to the endpoint expect a given response within a certain amount of time. The protocol has built in retry mechanisms, but ultimately a response must be

received or else a timeout occurs. When no response is received, and a timeout occurs, this occurrence will be logged.

- Configuration Failures: There are different features that the device (normally a phone) will use SIP messaging to communicate with the OpenScape Voice server of a particular device setup. An example would be that the phone is part of a Call Pickup Group. If the phone is setup for this particular feature, then a Subscribe will be sent to the OpenScape Voice server. The OpenScape Voice server will then verify this setup and respond with a Notify providing the device with the appropriate information. However, if the OpenScape Voice server cannot verify the feature setup, which normally indicates a configuration issue on either the device or OpenScape Voice server then this condition will be logged.

If a failure condition is registered for a VIP tagged DN, then it will be considered for special handling.

Functional Sequence

Logging means that a TCA (Threshold Crossing Alarm) category will be created for each of the three issues. These categories will have attributes associated with them that will monitor the occurrences for determination of alarming/ clearing and data suppression to avoid flooding and possible performance impacts.

These failures are logged in one specific unique VIP fault file. This log can then be easily monitored for failures. If any of these VIP DN related failures occur, it is imperative to address them expeditiously. In order to bring these problems to the administrator's immediate attention so that corrective action (as necessary) can be taken, an alarm will be issued for any single problem identified using the capabilities of the TCA mechanism.

Other Characteristics

The error conditions logged for VIP and non-VIP DNs are almost 100% the same (excluding the registration attempts of a non-existent DN or endpoint. A non-existent DN cannot be tagged as a VIP).

This feature also applies in part to non subscriber endpoints (gateways, proxies, etc). Transaction timeouts, authentication and certain registration scenarios are logged for non-subscriber endpoints.

5.1.9 Error Conditions for VIP Fault Detection and Alarming

This feature is for identifying a number of subscriber and endpoint problem conditions. Problems identified VIP (Very Important Person) subscribers will be brought to the attention of the administrator immediate so that corrective action (as necessary) can be taken.

The following types of problems are logged:

- Transaction timeouts:

  These errors are logged with log category COM_EXT_TIME_OUT to log file `/log/HiqLogTransactionTimeout.log`
- Configuration, Registration, Authentication & SIP Subscribe errors:

  These errors are logged with log category SUB_PROVISIONING_ERR to log file `/log/HiqLogProvisioning.log`

- De-registrations performed by the registration audit:

  These errors are logged with log category END_POINT_EXPIRED to log file `/log/HiqLogEndPoints.log`

For VIP subscribers, the above 3 log categories errors are concurrently logged with log category VIP_SUBSCRIBER_PROBLEM to log file `/log/HiqLogVIP.log`.

Transaction timeouts, authentication and certain registration scenarios are logged for non-subscriber endpoints (gateways, proxies, etc).

Functional Sequence

There are many errors that get logged, but only some are mentioned.

The transaction timeout indicates network failure and these conditions are logged to bring the network outages to the administrator's attention:

- Transaction timeout
  - Timeout of Invite Server transaction when timer-H is running
  - Timeout of non-Invite client transaction when timer-F is running
  - Timeout of Invite Client transaction when timer-B is running
- Configuration errors
  - Registration problems

    REGISTER message received from non-configured subscriber / endpoint

    REGISTER message received with invalid expiry time

    REGISTER message received with invalid transport type

    REGISTER message received from invalid line appearance

    REGISTER message for line appearance indicates that already registered prime line is non-Keyset

    A REGISTER message from a phantom subscriber attempting to register as the primary line on a device. A keyset device trying to register a

subscriber as its primary line while this subscriber is already registered as the primary line of another keyset device.

  - Registration audits:

    Subscribers that have not re-registered when their registration timer has expired are de-registered when the registration audit runs.
  - Subscription problems

    SUBSCRIBE message received with invalid Group pickup URI access code

    Keyset SUBSCRIBE received from non-Keyset DN

    SUBSCRIBE message received with invalid Feature Toggle access code

    SUBSCRIBE message received for Call Pickup from an unauthorized DN

    SUBSCRIBE with message-waiting event

    MLHG failure response for Toggle Make Busy when user is not part of MLHG
  - Authentication problems

    REGISTER message Digest authentication error for subscribers

    REGISTER / OPTIONS message Digest authentication error for non-subscriber endpoints
- OpenScape Voice Assistant
  - The VIP monitoring attribute is set in the **Attributes** tab of a subscriber's profile.
  - It is possible to filter based on the VIP monitoring attribute from the "Subscribers" list of the OpenScape Voice Assistant.

    When the VIP filter is set to "VIP Yes" - all subscribers having the VIP monitoring attribute will be displayed.

    When the VIP filter is set to "VIP No" - all subscribers NOT having the VIP monitoring attribute will be displayed.

    Since the feature does not apply to profile-only subscribers, profile-only subscribers will NOT be displayed when the filter is set to either "VIP Yes" or "VIP No".

5.1.10 Security Event Logging

The Security Event Logging feature permits OpenScape Voice to record security administration actions and OAM&P (Operation, Administration, Maintenance and Provisioning) activity originated over CLI (Command Line Interface), SNMP (Simple Network Management Protocol), SOAP (Simple Object Access Protocol)/ CLI or SOAP/XML interfaces to OpenScape Voice. It also records OS-level CLI activity.

This feature provides:

- The ability to track down system abusers and hackers that may be involved in system and network intrusions, interruptions, damage and unauthorized configuration changes.

- The ability to investigate recent security-related activity such as the following:
  - Changes to security attributes, services, and access controls such as successful and unsuccessful changes to user IDs and passwords; and successful and unsuccessful login attempts, logouts, or session termination (either local or remote) via the security audit trail.
  - Recent non-security related OAM&P activity via the recent change log This security event log is different from, and is kept completely separate from, the system event log, which logs abnormal runtime activity.

Functional Sequence

- The security audit trail supports logging capabilities:
  - Any action that changes the security attributes and services, access controls, and other configuration parameters of each network element and management system that is part of the OpenScape Voice infrastructure
  - Logins attempts, regardless of their success
  - Logouts or session termination, whether local or remote
  - Critical security administration actions, both successful and unsuccessful, such as actions affecting user IDs, login passwords, IKE (Internet Key Exchange) pre-shared keys for IPsec, and other security-related system characteristics.

    Logging of both OS- and application-level critical security administration activity is performed.
- The recent change log records all OAM&P activity (whether successful or unsuccessful), including:
- – Changes to system resources, system parameters, network elements, and end-user devices
  - Provisioning commands
  - Commands that retrieve customer data
  - Data synchronization commands
  - Data or network element recovery commands

System Specific Information

The security audit trail is based on ANSI T1.276-2003 and Telcordia GR-815-CORE.

The security log files are rotated on a daily basis. Archived security log files for the previous 30 days are retained; files older than 30 days are automatically removed.

Although the active security event log files are not encrypted, they are accessible only to CLI users who have the proper authorization. However, these files can be archived to long-term storage as an encrypted file.

SFTP (using IPsec) is used for the secure transfer of the log file data from OpenScape Voice.

5.1.11 Provisioning and Security Logging

The provisioning and security logging feature provides the ability to log all activities and commands in a log file to assist in detecting hacker and access violations.

Alarm reports are generated according to ITU-T (International Telecommunications Union-Telecommunications) Recommendation X.736, Systems Management: Security Alarm Reporting Function.

Provisioning and security events can be logged using the log control function of OpenScape Voice Assistant, according to ITU-T Recommendation X.735, Systems Management: Log Control Function.

5.1.12 Internal Audits

The internal audits feature provides for an audit process that performs a context scanning operation, first for UCE (Universal Call Engine) contexts and then for each type of signaling manager contexts.

The internal audit mechanism is to clean up memory leaks - specifically, hung call contexts.

System Specific Information

The time interval of internal audits has a recommended, default, and minimum value of 60 minutes, with a maximum value of 1440 minutes. 0 minutes, which indicates that auditing is disabled, is also a valid value.

5.1.13 On-Demand Audit

The On-demand Audit feature provides the capability for administrators to immediately obtain the status of the system resources. Two different times (peak and off-peak) define different timer values between each trunk channel audit.

The default value of the timers are 1 second for peak times and 0.25 seconds for off-peak times.

These times are also configurable, and can be fine-tuned to ensure that the audit cycles through all the resources at least twice a day without taking system time away from call processing.

5.1.14 Overload Handling

The OpenScape Voice utilizes a large number of Linux processes to provide the required call processing, maintenance and administration functions. The operating system schedules these processes using time-slices and priorities. In circumstances when the offered call processing or maintenance and administration load is higher than the available CPU capacity, overload controls are required to restrict and managed the offered traffic.

In normal operation (duplex mode) the rated call processing load can be handled with each node generally running at not more than 50% average CPU load. So when the average CPU consumption is close to 50%, this is a strong

indication that the system is heavily loaded and could enter into overload. In addition, an overload may occur even at lower average CPU percentage depending on various characteristics. The spare CPU capacity is required to allow management operations, and on node failure the surviving node has spare capacity to handle the call load. While the average CPU may be only 50%, CPU usage periodically may go to 100% due to provisioning, periodic health checks, statistics collection etc.

Call processing applications run at higher priority than non-call processing tasks, hence Maintenance and Administration tasks, such as provisioning, can utilize spare CPU capacity while the call processing applications are still allocated sufficient CPU to process the rated load. On a lightly loaded system, provisioning will run faster than on a heavily loaded system. The call processing queues are sized to allow zero message loss through short suspensions, due to other tasks running.

In addition to operating system process scheduling, OpenScape Voice utilizes various mechanisms to protect itself against overload conditions. The logic that applies is that when such a condition is identified some of the new calls or registration attempts will be rejected until the system can handle them without issues. This ensures that existing calls can be serviced properly, and the system does not get destabilized.

The following mechanisms exist:

Response time overload

OSV uses response time as the primary overload indicator. This overload metric is related to call handling. The response time of request/acknowledgement message pairs between the incoming signaling managers and the Universal Call Engine (UCE) lengthens approximately exponentially as the CPU load increases, with the response time starting to increase rapidly at around 70% CPU. An exponential smoothing algorithm is applied to the measured response time taking into account the response time history between the Signaling manager and the UCE.

If the response time forecast exceeds a certain threshold (100 ms) then OSV gets into overload state and starts rejecting calls. OSV will start rejecting 1 out of 2 calls but will reject incrementally more calls based on the overload level. For every increment of the threshold by 50 ms an additional call will be rejected before allowing a call to proceed.

So the following:

- At 100 ms 1 out of 2 calls are rejected
- At 150 ms 2 out of 3 calls are rejected
- At 200 ms 3 out of 4 calls are rejected

and so on

When calls are rejected due to this condition, OSV reports the problem by logging:

"SIP SM is in response time overload. New call request from %s:%d rejected to spare system resources"

or

"CSTA SystemStatus has entered overload. MakeCall Responses are timing out or being rejected"

Registrations are not rejected due to this mechanism. Only new calls made through SIP or CSTA (Make Call, Join Call, etc..). When the new call is rejected with a SIP 503 response message the message includes a warning header:

"SIPSM in overload, new call rejected"

Message Flooding Queue condition

Another mechanism to prevent failures in OSV due to high traffic is the message queue flooding prevention. This mechanism monitors the status of various message queues used in OSV to make sure that the critical process related to the call processing functionality will have enough memory available to queue all new messages arriving to the process.

The sizes of the queues are designed so that the response time overload mechanism will identify an overload condition before the queues are filled and messages are lost. However, there are cases (such as during a peak of registration attempts) where queues are filled despite the existence of the response time overload mechanism. In this case OSV will enter a message queue overload and will start rejecting new calls or generally SIP messages in high overload conditions as well as registration attempts depending on the nature of the overload.

SIP call handling queues overload

For SIP call handling queues overload controls reject messages depending on the number of messages in the input queue and while in overload level 1 there are sublevels of increasing call rejection:

1) Overload level 1
   - sublevel 1 - Q size 2000 - start rejecting 20% of the new calls with 503
   - sublevel 2 - Q size 2200 - start rejecting 40% of new calls with 503
   - sublevel 3 - Q size 2400 - start rejecting 60% of new calls with 503
   - sublevel 4 - Q size 2600 - start rejecting 80% of new calls with 503
   - sublevel 5 - Q size 2800 - start rejecting 100% of new calls with 503

2) Overload level 2 - Q size 3000 - start rejecting 100% of new calls with 503

3) Overload level 3 - Q size 4700 - reject all INVITES with 503 including new and mid call INVITES.

4) Overload level 4 - Q size 6400 - reject all messages except call terminations, responses and ACK's with 503

5) Overload level 5 - Q size 8100 - reject all new calls with 503 and all messages except call terminations, responses and ACK's without responding

6) Overload level 6- Q size 9950 - reject all new calls with 503 and all messages except call terminations, responses and ACK's without responding

When the SIP request is rejected with a SIP 503 message the message includes a warning header:

"SIPSM in overload level xxx"

Additionally, a log is created for all above cases:

"SIP SM is in queue overload (level %d)…"

SIP Registration overload

This is triggered based on the SIP REGISTRAR queue fill percentage or on the XDM queue fill percentage. If XDM queue size exceeds the predefined level (90%), then any incoming REGISTER request is immediately rejected.

If SIP REGISTRAR queue size exceeds predefined levels, then the overload queue level is considered to start rejecting incoming REGISTER requests at an increasing rate.

The SIP REGISTRAR queue has the following overload logic:

1) Overload level 1

- sublevel 1 - Q size 2000 - start rejecting 20% of new registrations with 503
- sublevel 2 - Q size 2200 - start rejecting 40% of new registrations with 503
- sublevel 3 - Q size 2400 - start rejecting 60% of new registrations with 503
- sublevel 4 - Q size 2600 - start rejecting 80% of new registrations with 503
- sublevel 5 - Q size 2800 - reject 100% of new registrations with 503

2) Overload level 2 - Q size 3000 - reject 100% of new registrations with 503
3) Overload level 3 - Q size 4700 - reject 100% of new registrations with 503
4) Overload level 4 - Q size 6400 - reject 100% of new registrations with 503
5) Overload level 5 - Q size 8100 - reject 100% of new registrations without response
6) Overload level 6 - Q size 9950 - reject 100% of new registrations without response

When a SIP Register request is rejected with a SIP 503 message the message includes a warning header:

"Registration in overload Level xxx" or "Registrar detect Xdm is in Overload"

Additionally a log is created:

"SIP Registrar in in queue overload…" or ""Rejecting registration request because of XDM overload…" depending on the situation.

CPU congestion levels

OSV has three congestion levels dependent on total CPU load, typically the thresholds are:

1) Level 1 - Minor - 90% CPU load
2) Level 2 - Major - 95 % CPU load
3) Level 3 - Critical - 98% CPU load

A change in the Congestion level will raise an alarm indicating the change in the congestion level.

The CPU congestion level will impact provisioning actions as explained below.

Overall Congestion Level

Overall Congestion Level is calculated as the maximum level when looking at the CPU Congestion Level and at the level corresponding to Response time overload status. The latter is defined as follows:

1) Congestion Level 1 and 2 = Response time overload > 100 msecs
2) Congestion Level 3 = Response time overload > 150 msecs

The overall congestion level will impact provisioning actions. More specifically:

- New requests through the SOAP API are rejected with an indication that the system is in overload.
- SOAP Mass Provisioning (soapMassProv) cancels import when Congestion Level is greater or equal to 2. A new log is created for this:

  "Soap Mass Provisioning execution canceled due to system congestion"
- SOAP export pauses the execution of the export action above Congestion Level 2. A log is created for this:

  "Soap Export pausing execution due to system congestion" or "System is congested; pausing soapExport on item"

Mitigation

There are various reasons why OSV may enter any of the described conditions but the most obvious one is that the OSV cannot handle the received traffic with the current configuration. Perform the following checks which are a common reason for overloads:

- In a virtualized environment make sure that the configuration of the system is done according to the recommended settings. Make sure that the CPU and memory are properly configured and that OSV does not share CPU resources with other applications that could cause the system to respond poorly.
- Verify that the tracing level is appropriate. By default, OSV systems should be running in 24_7_min (on systems with low traffic 24_7 is also acceptable to get more debug info, if no performance issues are identified). If more traces are enabled, make sure to fall back to 24_7_min and observe if the performance issues are resolved.

  If the system is in 24_7_min and still in overload, after collecting enough traces/logs, switch to 24_7_ext which is a lot lighter and should resolve the issue. Use the traces/logs to open a ticket for investigation
- Check if there is extensive CPU consumption during the overload by any process such as Solid or others or commands such as lsof, RPM etc..

  This could be an indicator that a lot of disk activity is slowing the system down. Make sure that no heavy maintenance or provisioning actions (e.g. Upgrades, FS Backup, DB Backup, SoapExport) are not done during the time of the overload. Always plan such activities during low traffic time windows.

  If the CPU consumption of some processes is not dropping for a long time, even if all relevant actions have finished, then operations should consider restarting the node with the problematic process that is consuming too much CPU

NOTICE:

There is a major drop (it can be as high as ~70%-80%) between 24_7_extern and 24_7_min tracing level depending on the system. Switching from 24_7_min to 24_7 will also induce a performance drop. Initial estimations put this drop in the range of 40%-50% or even higher depending on the underlying system.

In general, there are many cases where the overload occurs due to external (to OSV) reasons:

- There might be a peak of calls more than what the solution was designed for. In this case the solution from OSV side is to drop to traces to a lighter level such as 24_7_ext until the peak of calls has passed. Otherwise by design the OSV will drop some excess calls to protect itself and the established calls (overload mechanism).
- Similarly, there can be a burst of registrations that could cause a registration overload on OSV. The typical response from OSV is to send a 503 with try again later. If this mechanism is not enough, then there should be relevant configuration on the phones to not register all at the same time. Another solution is to use an SBC to limit the amount of registrations that can reach OSV at the same time.

5.1.15 System History Log

The system history log feature provides a log that is used to maintain a history of significant events pertaining to a particular OpenScape Voice installation.

Logging configurations (level, filename, output destination) are controlled by process level through either the GUI, command line interface, or SNMP (Simple Network Management Protocol).

Functional Sequence

The administrator can define a significant event to be any of the following:

- Initial installation
- Patch installations
- Upgrade activities
- Backup and restore activities
- Recent change functions

System Specific Information

Each process in the system generates its own log. The log is formatted as a flat file which can be viewed by using a standard editor and includes the option of being output to the screen or to some other type of viewpoint.

The log entry contains the following:

- Source process
- Date and time of log
- Severity level
- Debugging text (output)

5.1.16 OpenScape Voice Logging

The capability to log OpenScape Voice events is provided and the results are stored on the Public Wiki at http://wiki.dev.global-intra.net/publicwiki/index.php/Main_Page. Each OpenScape Voice log entry contains the following information:

- Log text
- Component
- Application ID
- Priority

- Category
- Possible Reasons
- Workaround
- Traces to Collect

The OpenScape Voice uses special logging APIs to report these events:

- SW-errors
- Data errors
- Communication errors
- Interface errors
- Single endpoint problems
- Security violations
- Performance and Resources
- Inconsistencies detected by audits
- Regular events of interest, such as
- External Communication (File transfers, link establishment)
- Endpoint events
- Maintenance activities
- Major SW events

5.1.17 OpenScape Voice Provisioning Errors Log

Configuration mismatches between OpenScape Voice and phones are captured in OpenScape Voice log-files as provisioning errors. The contents of these log-files, are exported via the OpenScape Voice Assistant GUI in CSV format for off-line processing via Excel or other software by service technicians. The OpenScape Voice threshold crossing alarm mechanism is used for reporting the existence of provisioning errors via the alarm interface.

The application scenario is where an error occurs in OpenScape Voice due to inconsistent configuration between OpenScape Voice and the phone of a user. The error is logged in OpenScape Voice Provisioning Error log. When the rate of log statements exceeds a predefined threshold an alarm is generated in OpenScape Voice. Following the reception of the alarm, the service technician can export the OpenScape Voice log file in a CSV format using Assistant GUI, and process it with an offline application such as Excel. Each log statement includes the OpenScape Voice subscriber directory number and Device IP address that are involved in this configuration conflict as well as a description of the error.

5.1.17.1 How to Download Voice Provisioning Error Log

OpenScape Voice Threshold Crossing Alarm mechanism is used for the reporting of the existence of provisioning errors via the alarm interface. The OpenScape Voice logging subsystem can be configured to generate threshold crossing alarms for various log categories when the number of logging calls within 5 or 15 minutes exceeds a threshold. Threshold Crossing Alarms clear automatically after a time period of intervals without threshold crossings. The default time is 24 hours, but it can be changed per log category to any number between 0 and 1440 minutes, 0 meaning no alarms at all. The log category that

is used for the logging of Provisioning errors is SUB_PROVISIONING_ERR. The following steps show how to download the OSV Provisioning Error Log:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring > OpenScape Voice Logging**.
2) Select the **Switch Name** and set the **Log Category** to SUB-PROVISIONING-ERR.
3) Click **Download**.

5.1.18 Reducing logs size

/log partition in an integrated simplex is possible to become full and as a result some issues may occur, i.e. the media server may stop functioning properly. You can perform the actions below to mitigate this issue.

Media server logging level

The file *mediaserver.mfw.native.log* consumes a significant part of the space in the /log partition. This is due to the fact that the logging level includes both INFO and DEBUG messages.

To decrease the .log file size, edit the *log4cxx.xml* file located under *UC_Installation_Path/mediaserver/application_host/bin/*.

This file describes the logging level that *mediaserver.mfw.native.log* file uses.

In it, check and substitute the **DEBUG** values with **INFO**.

You can also reduce the file size setting of the *mediaserver.mfw.native.log* file to 10 MB instead of 100 MB.

Restart Symphonia for the changes to take effect.

If necessary, remove the very large files *mediaserver.mfw.native.log* and *mediaserver.statistic.native.log*.

You can reduce the number of rotation files created by the default *log4j*.

Reduce the size of the *openscapeuc.log* by modifying the file */enterprise/ HiPathCA/config/common /log4j-webtier.xml*.

Empty *startup.log* file of the webclient if it gets very large, due to errors caused during the time the log partition was full.

6 Serviceability - Tracing, Status Checks, Misc. Tools

These features provide mechanisms to improve serviceability.

6.1 Call Trace

Call Trace allows administrators to display selective call tracing records based on a calling or called Directory Number (DN). It makes use of the real-time trace subsystem, and includes GUIs to provide a subscriber-friendly interface for call tracing and analysis. This tracing can be performed during offline functional testing and to debug live (online) system problems.

The call trace GUI provides the following operating modes:

- Normal mode: The normal mode is intended for use by subscribers and level 1 administrators. Normal-mode subscribers cannot access Real-time Trace functions that may impact call processing or overall system performance.
- Expert mode: The expert mode is intended for use by subscribers and administrators who are specifically trained in the use of Real-time Trace. Expert-mode subscribers have the knowledge to use Real-time Trace in a manner that ensures no impacts to call processing or overall system performance.

Functional Sequence

NOTICE:

Call Trace must be disabled while Continuous Trace is active.

Call Trace consists of two distinct phases:

- Online phase: During this phase, trace data is written from the memory buffer to the ASCII or binary file. This phase must be run on a Linux machine; its purpose is trace registration, activation, and information storage and retrieval. The online traces are captured and retrieved with the call trace GUIs.
- Offline phase: During this phase, the binary files are decoded and the trace data is analyzed. This phase can be run on a Linux machine or Windows PC; the offline tools are used to manage trace merging and filtering as well as interpret trace data.

Other Characteristics

The offline analysis is done with the Trace Manager GUI and the Call Analyzer tools.

6.2 Continuous Trace

Continuous Trace collects the detailed call data needed by field technicians, developers, system testers, and support engineers to efficiently analyze software, network, and configuration problems.

6.2.1 Continuous Trace Overview

Continuous trace runs on the SESAP (Secured Enterprise Service and Administration Platform) server, which is a Windows computer within the customer network that is maintained by customer service.

Functional Sequence

Continuous Trace is started and stopped via scripting. After it is activated, it collects, stores, and indexes trace data, compressing the data as necessary.

When a customer problem is reported, the technician can select trace files using filter criteria such as the telephone number (originating or terminating), IP address, and time of day. The relevant trace files can then be exported via FTP or e-mail for further analysis by customer service or development.

Other Characteristics

Call Trace allows administrators to display selective call tracing records based on a calling or called DN (Directory Number). It also includes GUIs that facilitate such tasks as call tracing and analysis.

Another tool for tracing is the Real-time Trace (RTT), which is a command-oriented tool that is used for general process tracing.

6.2.2 Continuous Tracing Including OpenScape Branch

The OpenScape Voice-Trace Manager is expanded to provide trace collection, analysis and display for OpenScape Branch.

This includes:

- Setting up the trace detail on target OpenScape Branch system.
- Starting/restarting the trace.
- Setting up the SFTP interface between the Branch under trace and an external trace receiver server.
- Import of trace data into internal db via a common API (e.g. DIPAZ).
- Integration of data into common analysis and display tools (e.g. FADE).
- Selection and export of raw trace files via a user-friendly application interface (e.g. FADE).

Functional Sequence

The SIP/MGCP traces can be started, stopped or restarted by the OpenScapeBranch Assistant.

The OpenScape Voice-Trace Management has an SFTP server. An SFTP client is used to transfer the files to the Continuous Tracing tool. The SFTP client is running automatically in OpenScape Branch. The SFTP user name

and password must be configured in the OpenScape Branch. After being transferred, the trace file will be deleted.

The file names are:
`<OpenBranchNodeName>_sipmgcp_<yyyymmdd>_<hhmmss>.cap.bz2`,
`<OpenBranchNodeName>_<LogType>_<yyyymmdd>_<hhmmss>.log.bz2`,
`<LogType> = sip|b2b|ms|cdr|pm|sp|rtp|alm|alh|sys|boot|snt|upd`

System Specific Information

The configuration of the log levels is already possible via SOAP. The log level which is set for Continuous Tracing will also be valid for accessing the logs via Assistant or CMP.

The default values for the log levels are:

Log	Default level
SIP Server	Error
B2BUA	Error
Media Server	Error
CDR	Error
Process Manager	Error
Survivability Provider	Error
RTP Proxy	Error
Alarm Manager	Error

6.2.3 Continuous Trace on Maintenance Server

The Continuous Trace tool on the maintenance (mtc) server consists of the three components: RTT (Real-time Trace), DIPAZ (Data Storage Indexing and Compressing) and FADE (Filtering, Analysis and Data Export). RTT and FADE are accessible via different start icons.

The continuous tracing, once activated, is automatically restarted with the current Continuous Trace filter (24_7, 24_7_min, or 24_7_extern) after any OpenScape Voice node startups.

The continuous trace feature is administered per node.

The Continuous Trace tool can be installed with one package (RTT, DIPAZ, FADE). Separate installation of RTT only is possible.

The software for continuous tracing is independent from the hardware and the Windows version.

System Specific Information

The RTP parameter is set to `Srx/PrttReader/ConTraceCompressFiles = 1 (true)by default`, the trace files are zipped at the OpenScape Voice before writing to disk to save space.

Continuous trace and call trace can run in parallel. This option is controlled by RTP parameter `Srx/PrttReader/RunBothCallTraceContTrace`. The

default value is `Srx/PrttReader/RunBothCallTraceContTrace = 1 (true)` meaning the two traces can run in parallel.

The administrator will be informed when trying to run continuous trace and call trace at the same time.

6.3 Call Trace and RTT (Real-time Trace) GUI

This feature realizes a common Graphical User Interface for Real Time Trace and Call Trace. More than one GUI can connect to a single OpenScape Voice. The GUIs can run on a standalone machine or be integrated with a web enabled management system.

Functional Sequence

Applications use the trace APIs to pass message trace and process detailed trace to the Real Time and Call trace sub-system, which writes the trace to a memory buffer. The trace reader reads the buffer and decodes the trace file into a 'Perl' format which will allow efficient analysis on the offline machine. The GUI controls enabling of trace and allows a list of decoded trace files to be displayed. A simple 'file select with transfer' will transfer the decoded files to the off-line machine.Once transferred to the off-line machine the decoded files can be selected for analysis and the results displayed.

When the trace GUI is activated the main window will be displayed. The GUI can be started in normal or expert mode, the process control and filter management tabs are only available in expert mode. The main window will display the content of the connection control tab which will allow the user to connect to an OSV.

The user will need to provide:

- OpenScape Voice host name
- UserId
- Password

System Specific Information

The filter management is only available in expert mode.

Allows full control of all trace filters.

Uses a tree-view to show flag data.

Specific filters to control 'normal' use detail trace flags.

Menu to select a local trace file, or remote trace session data from the connected system.

Some options will be expert mode only.

Other Characteristics

Additional start/stop criteria of the Trace functionality and reconfiguration of the Call Trace Directory structure are implemented. In some more detail, the Call Trace should be able to start based on prefix DN (Directory Number) digits, and the RTT Tracer should be enhanced to also support stop criteria due to specific dialed DN.

The specific feature are the following:

- Trace based on Prefix Directory Number digits.Call Trace is able to start tracing based on the suffix digits of a DN. This capability is enhanced to prefix digits of a DN.
- RTT Trace Stop Criteria functionality includes the dialed DN. Additional stop criteria were requested to stop the RTT Trace and it was decided to include only the Dialed Directory Number. This concept should apply only for SIP calls.
- Call trace stops when file size reaches a certain limit (e.g. 50 MB). The capability to automatically stop the Trace in case such a limit is reached.

6.3.1 RTT (Real-time Trace)

RTT (Real-time Trace) allows administrators to display Call Trace Records during offline functional testing and for debugging live (online) system problems. A combination of Online and Offline tools are used by the Real Time Tracing features.

This feature collects - in real time - all OpenScape Voice data associated with specified signaling messages or applications. It also provides additional capabilities that cannot be performed with the call trace GUIs.

Real-time trace employs the classic tracing methods of commands, pre designed scripts, and ASCII dumps.

Functional Sequence

NOTICE:

Customers and customer service engineers unfamiliar with this tool should contact their next level of support before using it.

Real-time trace consists of two distinct phases:

- Online phase:

  During this phase, trace data is written from the memory buffer to the ASCII or binary file. This phase can be run on a Linux machine or Windows computer; its purpose is trace registration, activation, and information storage and retrieval. The online traces are captured and retrieved either with pre-assigned scripts and flags that must be preset and input into the command line.
- Offline phase:

  During this phase, the binary files are decoded and the trace data is analyzed. This phase must be run on a Linux computer. The offline tools are used to manage trace merging and filtering as well as interpret trace data.

This offline analysis is done with commands input at the command line.

Other Characteristics

Call trace makes use of the real-time trace subsystem to provide selective call tracing based on a calling or called DN (Directory Number). It also includes GUIs that facilitate such tasks as call tracing and analysis.

Continuous trace collects the detailed call data needed to efficiently analyze software, network, and configuration problems.

6.3.2 Real-time Trace Enhancement

RTT (Real-time Trace) is part of the continuous trace tool, consisting of an OpenScape Voice online part and an offline part on a separate maintenance server, allowing administrators to manage Call Trace Recording and Trace File Administration (copy, compression and storage).

RTT is running continuously with the recommended default setting of 24_7_extern flags.

Use of CLI on OSV or RTT GUI running on OSV-TM allow Continuous Tracing to be started or stopped quickly.

Parts of the RTT:

- Online part on OpenScape Voice:

  The online part of RTT consists of the Trace Management server, the Persistent Reader, and the RTT Command Line tools.

  – Trace Management server

    This process provides the interface between the offline Trace Manager, and the internal RTT tools
  – Persistent Reader

    This process stores Continuous Trace data into a set of aged files, and optionally FTP or SFTP the trace data to the maintenance server. These options are controlled from the offline Trace Manager GUI through commands forwarded from the trace management server or via the OSV CLI interface.
  – RTT command line tools

    The existing RTT command line tools are invoked as needed by the trace management Server in response to commands received from the offline Trace Manager GUI.
- Offline part on a maintenance server:

  The Offline part of RTT consists of the Trace Manager GUI, Call Analyzer GUI and a Command Line Interface for the management of Continuous Tracing.

  The Trace Manager GUI is able to provide control of Continuous Tracing on the OpenScape Voice system.

  This control will include the ability to:

  – Start and stop Continuous Tracing on the OpenScape Voice
  – Setup the FTP/SFTP parameters for transferring trace data to the maintenance (MTC) server.
  – Start and stop the FTP/SFTP transfer of trace data to the MTC server.
  – Coordinate Continuous Tracing with Call Trace and RTT trace (when initiated through the GUI)

.

Functional Sequence

RTT is configured by default with a set of trace flags for continuous tracing. It offers commands (SSH connection):

- to start/stop the continuous trace for a given time. If the stop time is set to 0 the trace will run continuously until manually stopped. The administrator may stop the continuous trace at any time.
- to configure trace file copy (IP address, directory name, password, user id) and
- to start/stop trace file copy via FTP/SFTP.

RTT creates trace statements when the continuous trace is started/stopped and when trace flags are changed. These actions can be initiated via the trace GUI or via the RTP CLI menu.

The trace files are always stored locally.

RTT wraps locally stored trace files (deletes oldest file if max number of files is reached, this avoids RTP alarms when disk gets full).

The administrator can invoke these commands via the RTT GUI or CLI.

System Specific Information

RTT compresses the trace files before they are written to the local disk.

If the trace file copy is active all locally stored trace files are copied to the maintenance server via the admin IP address of the OpenScape Voice node and deleted afterwards.

When a non-empty trace file is 5 minutes old, it is closed and copied to the maintenance server.

Other Characteristics

RTT creates a trace statement '"xx trace statements lost" whenever trace statements could not be stored in the local trace file.

6.4 Resource Reports

Srx/Ovl/MonitorQueues and Srx/Ovl/MonitorPrograms are associated with resource reports -- they control the queue and process tracking for the given OSCVoice programs. When the OP_RTT_RES_VAL flag setting for SrxOvlMgr (1 or 2) includes QUEUES then Srx/Ovl/MonitorQueues is applied, when the flag includes CPU then the Srx/Ovl/MonitorPrograms is applied.

2.2.1.12 CPU Usage of CPU CoresPercentage of used CPU since the last trace for each CPU core. Currently up to 12 cores. Maximum is 1000‰, rounded to integer, below 0.5 is zero.Traced every 5 seconds.

Currently the OSV Trace Manager OSVTM analyses OSV signaling traces, stores call and registration related information in a database and provides queries to display callp traffic and graphs with OSV call processing statistics. The goal is to trace resource usages and to display OSV resource usage in OSVTM graphs for CPU, Memory, Disk, Response Time, Message Queues, I/O, Switch Size.

OSV SW processes that know about OSV resource usage should periodically report the usage via trace statement. For simplification and consistency reasons a new resource trace API was implemented. The new resource trace flags has been added to all continuous trace flag sets. The OSVTM trace file parsing process DIPAZ reads the resource usage values and adds averages to the

OSVTM database with a granularity of 1 minute and 15 minutes. In the future a new set of graphs will be implemented in OSVTM that show the 1 and 15 minute values of all traced resources.

6.4.1 List of Resource Traces

Important OSV resource trace flags has been added to all continuous trace flag sets. The resource trace faclity is RTT_RES_VAL with the trace flags CPU, Memory, Queues, IO, Performance and Sizing.

The first column specifies the trace flags predefined for resource tracing, the second column specifies the resource, the third is the value of the resource usage, the fourth specifies the frequency of tracing.

Resource Type	Resource ID	Remarks	How often
CPU	Node CPU	Used CPU percentage since the last trace over all CPU cores. Maximum is 1000‰, rounded to integer, below 0.5 is zero	5 sec
CPU	Process CPU	CPU usage of process, max = 100%	5 sec
Memory	SwapUsed, MemFree, Buffers, Cached	Percentage, rounded to integer	5 sec
Queues	Queue Fill Level	Average message queue fill level percentage of selected processes plus number of sent and received messages and the average time spent in the queue <avg fill percentage>-<sent msgs>-<rec msgs>-<avg latency in micro-sec>	5 sec
IO	eth0 … eth7 bond0 bond1 bond2 bond3	Amout of KiloBytes sent and received since last trace statement per bonding interface. Shown are Rx/Tx-Bytes-Packets-Errors	5 sec
Performance	Response Time	SIP, CSTA response times in msec since last trace statement SIPSM-Samples-Avg-Min-Max-RejectedCalls, LostBeginEvents, LostEndEvents, SampleTimePeriod	10 sec
Sizing	ActiveRegistrations	Number of currently active registrations stored in the local node (memory)	1 min

6.5 Query of Subscriber Transient Operational Status

The feature Query of Subscriber Transient Operational Status provides the capability to determine a subscriber’s transient operational status, which refers to a snapshot of the status of the subscriber at the instant that the request is issued by administration or service personnel.

A subscriber is identified by the associated DN (Directory Number).

Functional Sequence

The administrator enters the subscriber's DN into OpenScape Voice Assistant screen, then receive details about the connections active for that subscriber.

System Specific Information

The following information is displayed in the Transient Status display area:

- Subscriber ID
- Session Number
- Session Status
- Original Called Party DN (for each outgoing session)
- Calling Party DN (for each incoming session)
- Error Messages, if any

If multiple sessions are active, the call session number and the called/ calling party DN are repeated (i.e. listed for each session).

If a SIP subscriber has multiple call sessions active, the status display is limited to the first 5 sessions. If the subscriber has multiple contact bindings, the status is displayed per contact, limited up to 5 sessions.

The status of the call session can be displayed as one of the following:

- Idle
- BLV Active
- Call Setup Outgoing
- Ringing
- Busy Outgoing
- Busy Incoming
- Releasing

Other Characteristics

It is not possible to query the transient status of multiple subscribers simultaneously.

6.5.1 How to Query the Transient Status of a Subscriber

The transient status information is displayed for all registered contacts of the selected subscriber ID: Subscriber ID, Session Number, Session Status, Original Called Party DN (for each outgoing session), Calling Party DN (for each incoming session), Error Messages, if any.

Prerequisites

Adequate administrative permissions

It is only possible to query the transient status of one subscriber but not of multiple subscribers simultaneously.

Step by Step

1) Navigate to **OpenScape Voice** > **Business Groups** > **Members** > **Subscribers**.
2) Tick/select one subscriber. Click **Transient Status**.

   You will get the current status of this subscriber.
3) Establish a call using this same subscriber.
4) Click **Run Again**.

   You will get the latest current status of this subscriber.
5) Click **Close**.

6.6 FADE

The FADE (Filtering, Analysis and Data Export) tool allows for the freezing trace files of a particular time frame, selecting trace files, analyzing selected trace files and exporting selected Trace, Index, PCAP (Positioning Calculation Application Part) and QoS (Quality of Service) files via FTP or e-mail.

The FADE tool can be used by end users and administrators when attempting to locate and analyze trace data for a specific issue, problem or error condition. They will hopefully have specific info about the fault, such as time of occurrence, DNs (Directory Numbers) involved, errors observed, etc. which will be used as filtering criteria.

Functional Sequence

FADE provides a GUI interface to the following functionality:

1) Data Filtering:

   The subscriber may enter any combination of search criteria and the tool will search the stored index data to locate and identify the trace files associated with the requested data.
2) Data Analysis:

   The administrator may access basic analysis tools against the selected data. This may include opening the stored PCAP files with Ethereal (if installed) or initiating the SIP analysis of the raw trace data with the DAT tool (if installed).
3) Data Exporting:

   The administrator may request that the requested trace data be exported to development using e-mail or FTP. Scheduling may be setup to periodically export selected trace data automatically.

System Specific Information

The FADE tool can be instructed to transport selected trace files to another server most likely located at customer service and/or development site by e-mail or FTP/SFTP.

E-mail volume is limited to 4 MB.

FTP transfer rates are possible from 2 Mbit/sec to 400 Mbit/sec. No need for SFTP if using VPN tunnel to SIRA (Secure Infrastructure for Remote Access).

If QoS is wanted, the QoS "performance data" is embedded in the PCAP and the raw trace data files. There are no specific QoS files.

Other Characteristics

The analyzer tools are enhanced to select trace files using the list created by the trace filter for local analysis preferable via remote desktop.

Functions of the trace analyzer are:

- Display summary line for each trace statement in human readable form with time stamp, DN and call ID.
- Sort trace statements by DN, call ID
- Find call data of corresponding call legs
- Show flag irregularities
- Show message flows graphically

The analyzer tools are enhanced to display QoS data from the QoS database or the exported QoS file identified by call ID.

6.7 DIPAZ

The DIPAZ (Data Storage Indexing and Compressing) tool is a Windows service that reads the trace files and creates trace files and PCAP (Positioning Calculation Application Part) files. DIPAZ also deletes trace files before the disk gets full, reads Quality of Service (QoS) data and stores them in a SQLite database.

DIPAZ is a Windows Service that will be started automatically on Windows startup and runs continuously on the Windows PC. DIPAZ will constantly monitor the raw trace file directory, looking for new raw trace files being uploaded via FTP/SFTP from the OpenScape Voice Persistent Reader or FTP/SFTP scripts.

The DIPAZ process has no user interface.

Functional Sequence

When a new raw trace file is detected, DIPAZ will:

1) Parse the binary trace data and extract key info such as DNs, call-ids, and error info.
2) Create a PCAP file for all external messages
3) Compress the file using GZIP
4) Parse the phone and/ or QoS file/database and store extracted QoS info in SQLite database indexed by call-ID

System Specific Information

The continuous trace software DIPAZ is hardware and Windows (XP, 2003 and 2008) version independent. There is no dependency on service packs, 32/64 bit and drivers.

When the file size reaches 20 MB or the end of the day is reached the index file is closed and a new index file is opened.

Once the trace file is successfully parsed it is compressed, saved to disk and the original trace file is deleted.

The trace files are stored in a directory tree by day / hour / node ID.

The index file is stored directly in the day directory.

Because trace file compression is executed by default on the OpenScape Voice, DIPAZ needs to uncompress the trace files before the indexing.

6.8 Quasi Real-Time Network Health Visuals

This feature introduces quasi-real-time charts for a set of Key Performance Indicators (KPI). The charts enable administrators to identify service affecting network conditions via Quasi-real-time performance visuals and to localize them to repairable network elements. Diagnosis and repair may be escalated, depending on the nature of the condition. The main intent is to enable administrators to take proactive steps that previously could only be made by reactive escalations, due to the tools available and expertise required.

The visuals provide indications for the following:

- Network Interface Health
- Call Pattern Health
- SIP Signaling Health
- SIP-Q Signaling Health
- CSTA Signaling Health
- MGCP Signaling Health
- PRI Signaling Health
- Quality of Service (QoS) of voice (RTP stream)

Functional Sequence

The "DIPAZ" function will write or create entries from trace data into an SQL table that are read on a 2.5 minute refresh interval, or on demand for a manual charting request, by the "FADE" function to populate the charts.

Upon Login to the OSV-TM, the administrator sees the "Calls" graph.

The administrator has the option to choose how often a refresh occurs. The refresh timer option should be 30 seconds, 1 minute, 2.5, 5, 10 and 15 minutes. The administrator can turn on/off Auto Refresh.

The administrator can cycle thru all available graphs based on a selected time interval.

The administrator is able to traverse between the screens using tab navigation, per CMP "look-and-feel" requirements.The X-axis of the KPI charts shall be time of day, adjustable between 30 minutes and 24 hours. User shall be able to zoom in on particular time of day.

The Y-axis of the KPI charts is auto adjust to fit the scale of the measurement.

Where more than one KPI is shown, color shall be used to distinguish between the KPIs.

System Specific Information

The quasi-real-time charts for the following Key Performance Indicator are introduced:

- Stable (Active) Calls
- New Call Attempts
- Answer Seizure Ratio (ASR)
- Ineffective Call Attempts
- Ineffective Machine Attempts
- Active Registrations
- New Registration Attempts
- Registration Change Ratio
- Ineffective Registration Attempts
- Voice, i.e., Real time Protocol (RTP) Transmit Packets
- RTP Received Packets
- RTP Packet Loss
- RTP Packet Latency
- RTP Packet Jitter
- RTP Duplicate Packet
- Post dial delay
- Subscribe
- Notify
- Option

Other Characteristics

Help text is displayed when the curser hovers on an (x,y) coordinate. The following information is displayed:

- Name of line plotted
- Date and time
- Value

6.8.1 Chart to Database Mapping: CALLS

The chart identifies the KPIs and relevant SQL database items. The complete list comprises the charts: Calls, Registrations, Performance, Call Timings and SIP Messaging (Non-Call).

Chart Name: CALLS

KPI Name	Algorithm	Corresponding DB Mapping
Stable (Active) Calls	Σ call Where call > answer_time, but < end_time Expressed as an absolute. Summed over a minute interval.	interval.stablecalls
New Call Attempts	1/2. Σ SIP_Invites Expressed as an absolute. Summed over a minute interval.	interval.total

KPI Name	Algorithm	Corresponding DB Mapping
Answer Seizure Ratio (ASR)	100. Σ SIP_Answered / Σ SIP_Invites Expressed as an absolute. Summed over a minute interval.	interval.Answered / interval.Total
Ineffective Call Attempts	100. Σ (SIP_Abandoned +SIP_ErroredCalls) / Σ SIP_Invites Expressed as a %. Summed over a minute interval. Where: • SIP_Abandoned: calls abandoned by A party before ringing. • SIP_ErroredCalls: calls refused for any reason	interval.IneffectiveCalls / interval.Total
Ineffective Machine Attempts	100. Σ SIP_ErroredCalls / Σ SIP_Invites Expressed as a %. Summed over a minute interval. SIP_ErroredCalls: calls refused for any reason	interval.ErroredCalls / interval.Total

6.8.2 Chart to Database Mapping: REGISTRATIONS

The chart identifies the KPIs and relevant SQL database items. The complete list comprises the charts: Calls, Registrations, Performance, Call Timings and SIP Messaging (Non-Call).

Chart Name: REGISTRATIONS

KPI Name	Algorithm	Corresponding DB Mapping
Active Registrations	Σ endpoint Where endpoint > last_register, but < next_register_due Expressed as an absolute. Summed over a minute interval.	interval.RegisteredLines

KPI Name	Algorithm	Corresponding DB Mapping
New Registration Attempts	Σ SIP_Register Expressed as an absolute. Summed over a minute interval.	interval.Registers
Registration Change Ratio	100.(KPI: Active Registrations @ t-KPI: Active Registrations @ t-1) /KPI: Active Registrations @ t Expressed as a %, where t is time in minutes.	interval.DeltaRegisteredLines
Ineffective Registration Attempts	100. Σ Registration_Failures / Σ SIP_Register Expressed as a %. Summed over a minute interval.	interval.RegisterErrors / interval.Registers

6.8.3 Chart to Database Mapping: PERFORMANCE

The chart identifies the KPIs and relevant SQL database items. The complete list comprises the charts: Calls, Registrations, Performance, Call Timings and SIP Messaging (Non-Call).

Chart Name: PERFORMANCE

KPI Name	Algorithm	Corresponding DB Mapping
Stable (Active) Calls	Σ call Where call > answer_time, but < end_time Expressed as an absolute. Summed over a minute interval.	interval.stablecalls
RTP Received Packets	RTP_Received_Packets, as reported by OpenScape SBC, phone or per call basis. Expressed as an absolute for each call, at the end of the call.	PerfData.PacketsRcv

KPI Name	Algorithm	Corresponding DB Mapping
RTP Transmit Packets	RTP_Transmit_Packets, as reported by OpenScape SBC, phone or per call basis. Expressed as an absolute for each call, at the end of the call.	PerfData.PacketsSent
RTP Packet Loss	RTP_Packets_Lost, as reported by OpenScape SBC, phone or per call basis. Expressed as an absolute for each call, at the end of the call.	PerfData.Lost
RTP Packet Latency	RTP_Packets_Latent, as reported by OpenScape SBC, phone or per call basis. Expressed as an absolute for each call, at the end of the call.	PerfData.Delayl
RTP Packet Jitter	RTP_Packets_Jitter, as reported by OpenScape SBC, phone or per call basis. Expressed as an absolute for each call, at the end of the call.	PerfData.Jitter
RTP Duplicate Packet	RTP_Duplicate_Packets, as reported by OpenScape SBC, phone or per call basis. Expressed as an absolute for each call, at the end of the call.	PerfData.Duplicate

6.8.4 Chart to Database Mapping: CALL TIMINGS

The chart identifies the KPIs and relevant SQL database items. The complete list comprises the charts: Calls, Registrations, Performance, Call Timings and SIP Messaging (Non-Call).

Chart Name: CALL TIMINGS

KPI Name	Algorithm	Corresponding DB Mapping
Stable (Active) Calls	Σ call Where call > answer_time, but < end_time Expressed as an absolute. Summed over a minute interval.	interval.stablecalls
New Call Attempts	1/2 Σ SIP_Invites Expressed as an absolute. Summed over a minute interval.	interval.total
Post dial Delay	Incoming_SIP_Invite_Time - SIP_Ringing_Time Expressed as an absolute for each call, at Ringing Time.	calltimes.StartTime - calltimes.RingStart
Call Hold Time	SIP_Answer_Time - SIP_End_Time Expressed as an absolute for each call, at the end of the call.	calltimes.Answer - calltimes.EndTime
Processor Time	Outgoing_SIP_Invite_Time - Incoming_SIP_Invite_Time Expressed as an absolute for each call.	calltimes.InviteDelta

6.8.5 Chart to Database Mapping: SIP MESSAGING (NON-CALL)

The chart identifies the KPIs and relevant SQL database items. The complete list comprises the charts: Calls, Registrations, Performance, Call Timings and SIP Messaging (Non-Call).

Chart Name: SIP MESSAGING (NON-CALL)

KPI Name	Algorithm	Corresponding DB Mapping
Subscribe (Sent)	Σ SIP_Subscribe Expressed as an absolute. Summed over a minute interval.	interval.Subscribe

KPI Name	Algorithm	Corresponding DB Mapping
Notify (Sent)	Σ SIP_Notify Expressed as an absolute. Summed over a minute interval.	Interval.Notifies
Options (Sent)	Σ SIP_Options Expressed as an absolute. Summed over a minute interval.	interval.Options
Subscribe Time (Sent)	Response_To_SIP_Subscribe_Time - SIP_Subscribe_Time Expressed as an absolute for each call.	noncalltimes.SubscribeResponse
Notify Time (Sent)	Response_To_SIP_Notify_Time - SIP_Notify_Time Expressed as an absolute for each call.	noncalltimes.NotifyResponse
Options Time (Sent)	Response_To_SIP_Options_Time - SIP_Options_Time Expressed as an absolute for each call.	noncalltimes.OptionsResponse

6.9 Simulate Dialing

This feature is used to simulate dialing in order to verify whether a certain destination's (Subscriber Id or else) call can be translated to an endpoint.

The Simulate Dialing feature provides a diagnostic tool that allows users to input originating (i.e. calling party) and terminating (i.e. called party) translation information to the tool. The subscriber then submits the translation request, the tool performs a translation based on the input provided and returns a success or failure indication along with the destination and routing results or an error message. The results will also provide the tables accessed and the pertinent data from each table.

Given a phone number and using the numbering plan the following topics are checked.

- To which number the call is routed?
- Is dialing available?

6.9.1 How to Simulate a Dial

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate **OpenScape Voice** > **Administration** > **Tools** > **Simulate Dial**.

   The **Simulate Dialing** dialog opens.

2) Select in the field **Originator´s Subscriber ID** (optional parameter) for the originating (calling party) number:

   - Enter a Subscriber ID or click Subscriber ID selection button "**...**".

     The **Select Subscriber** dialog opens.

     Select a Subscriber ID from the list and click **OK**

     NOTICE:

     This parameter is optional because there can be call scenarios where the call is coming from a Gateway or proxy.

3) Select in the field **Originator's Details**:

- Enter a **Numbering Plan** (optional parameter) or click the corresponding selection button "**...**".

  The Numbering Plan List dialog opens, providing a list of NPs.

  NOTICE:

  When a subscriber is selected, the NP of the selected subscriber is set but the user can change this NP for test purposes.

- Enter a **Routing Area** (optional parameter): Click the corresponding selection button "**...**".

  The Select Routing Area for Subscriber dialog opens, providing a list of Routing Areas.

  Select a Routing Area from the list and click **Accept Selection.**

  NOTICE:

  When a subscriber is selected, the Routing Area of the selected subscriber is set but the user can then change this routing area for test purposes.

- Enter a **Class of Service** (optional parameter) by clicking the corresponding selection button "**...**".

  The Select Class of Service for Subscriber dialog opens, providing a list of COSs.

  Select a Class of Service from the list and click **Accept Selection**.

  NOTICE:

  When a subscriber is selected, the COS of the selected subscriber is set but the user can change this COS for test purposes.

- Enter a Calling Location (optional parameter) by clicking the corresponding selection button "**...**".

  The Calling Location dialog opens, providing a list of Calling Locations.

  Select a Calling Location from the list and click **Accept Selection**.

  NOTICE:

  When a subscriber is selected, the Calling Location of the selected subscriber is set but the user can change this Calling Location for test purposes.

- Select the Originator´s Bearer Capability (optional parameter) by selecting a value from the corresponding dropdown list. This parameter

specifies the bearer capability associated with the incoming call to be taken into account during translation.

NOTICE: Possible selections: Unassigned, Speech, Audio, Data64KB, Rate Adapted, 64KB Preferred.

NOTICE: Default: "Unassigned".

- Select the Originator´s Signaling Type (optional parameter) by selecting a value from the corresponding dropdown list. This parameter specifies the signaling type associated with the incoming call to be taken into account during translation.

NOTICE: Possible selections: Unassigned, Sip, Sipt.

NOTICE: Default: "Unassigned".

4) In the field **Destination Data**:

- In the **Dialed Digits** field, enter the number to be dialed including including the prefix digits, if any. This is a mandatory parameter.
- Select **Nature of Address** (optional parameter) in the **Destination Data** area by selecting a value from the corresponding dropdown list. This parameter specifies the Nature of Address of the called party.

NOTICE: Possible selections: Unknown, Subscriber, National, International, No DN, Test, L0, L1, L2, Extension, Calling Loc, Code-Index}.

NOTICE: Default: "Unknown".

5) Click **Simulate** to start the digit translation. The Assistant receives a translation reply message from the switch and displays the message in the Result textbox once the translation is done. If the translation is unsuccessful, the message describes the error encountered.

If the translation is successful, the typical output data has the following syntax:

NPA, Digits, NOA, Destination Type and Destination ID, Route Data, and DB Table accessed.

Example

```
***Translation Not Successful***

Input: Originating Number = 302101001003 Dialed Digits

3021011001003, Numbering Plan ID = 5, Nature Of Address =
Intl

Output:*** Unsuccessful Translation. Code does not exist
for this numbering plan.
```

6.10 Database Architecture

OpenScape Voice uses a shared-nothing database from SolidTech. Data changes are made to the primary database and automatically replicated to the secondary database.

6.10.1 How to Check for the Active Database

The only way to find out the active DB is to use the command described below.

Prerequisites

Adequate administrative permissions

Step by Step

1) Login as user `srx`.
2) Run `RtpSolid -l`.
3) You will get an information like this:

Server	C-S Conn.	HSB State	ClmonState	Interface
grd403n2	CONNECTED	SECONDARY ACTIVE	----	127.0.0.1
grd403n1	CONNECTED	PRIMARY ACTIVE	UP	grd403n1_cip0

In that example PRIMARY ACTIVE in grd403n1 indicates that SolidTech is Primary Active on node1.

6.11 Cluster Interconnection

This feature is used to display the Cluster Interconnection configuration parameters defined in the `node.cfg` file.

The feature Cluster Interconnection will remove the need for an expensive optical fibre link between two sites for survivability. Instead a layer 3 IP connection can be used. Two IP connection scenarios are supported:

- Cluster foundation over Ethernet
- Cluster foundation over IP

Depending on the interconnection type the displayed data will be different:

Cluster interconnection over Ethernet (L2 scenario):

- Interconnection type
- Node 1: Primary IP
- Node 1: Logical IP
- Node 2: Primary IP
- Node 2: Logical IP
- Netmask
- Network
- Broadcast

Cluster interconnection over IP (L3 scenario:)

- Interconnection type
- Cluster Interconnect Control
- Cluster Interconnect Data
- Node 1: IP address
- Node 1: Netmask
- Node 1: Network
- Node 1: Broadcast
- Node 2: IP address
- Node 2: Netmask
- Node 2: Network
- Node 2: Broadcast
- Node2: Gateway

The feature is meaningful only in cluster deployment scenarios. In case of cluster absence (single node scenario) the displayed data will depict the configuration of the single existing node.

6.11.1 How to Display the Cluster Interconnection Configuration

Step by Step

1) Navigate to the **OpenScape Voice** > **Administration** > **General Settings** > **Cluster Interconnection** dialog to display the cluster interconnection parameters.
2) Checks the configured data and verify whether there is a misconfiguration.
3) Start the NPCE tool and change the configuration.
4) Refresh the Cluster Interconnection dialog and verify the cluster interconnection parameters displayed.

   The Assistant will only display the values defined by the NCPE tool, based on the enriched `RTPparameters.conf` file.

6.12 System Health Check

The System Health Check feature uses an on-board Test Call Generator on each OpenScape Voice node that tests the call processing and registration capabilities of the node. In addition to the two main TCGs each TCG has a backup TCG on the other node.

The System Health Check feature is an automatic system-wide feature that is enabled by default.

6.12.1 Test Call Generator

Test Call Generator is a on board SIP UA (User Agent) to generate test calls that allow automatically detecting the failure of OpenScape Voice to process calls. The Test Call Generator will serve as a SIP endpoint (registrations and originating calls) and as a SIP keyset (registrations and terminating calls).

Functional Sequence

The on-board test call generator is deployed on each OpenScape Voice node. The TCG periodically register a subscriber and generates a test call to the primary SIP Signaling Manager on its own node. The registration pass through SIP Registrar and XDM. The call processing messages for the test call will pass through TTUD, SIP SM and UCE, completing the loop.

As long as the loop is completed in a timely fashion and without errors, the registration and call processing components of that node are declared to be functional.

As soon as the loop is not completed, recovery actions are undertaken, such as getting the survivable branch offices in survivable mode, generating alarms for the administrator, restarting processes.

If a failure to process calls is detected, the following corrective actions are proceeded:

1) Alarm to the Assistant/Fault Management.
2) Force proxies into survivable mode by stop answering OPTIONS messages..
3) Restart processes to attempt to recover them (SIP Registrar, SIP SM, TTUD, UCE as needed).

Other Characteristics

TCG uses endpoints and subscribers created with a special numbering plan. They are created when the system is installed.

6.12.2 Test Cycles of the Test Call Generator

In normal operation, each TCG (Test Call Generator) runs a TCG Test Cycle in defined intervals.

Each test cycle contains 5 main parts:

1) Registration as SIP Trunking endpoint with the SIP registrar on the node.
2) Registration as a SIP keyset with the SIP registrar on the node.
3) Test call to the SIP server on the node.
4) Un-registration as a SIP keyset from the SIP registrar on the node.
5) Un-registration as a SIP Trunking endpoint from the SIP Registrar on the node.The outcome of a test cycle determines the health level of the system and with each health level specific recovery measures need to be taken.

Functional Sequence

The outcome of a test cycle determines the health level of the system and with each health level specific recovery measures need to be taken.There will be three health levels of recovery measures in erroneous cases:

1) Not Run

This is the state in which the TCG is when it is started or when it is turned off. There are scenarios listed in which the TCG returns to this state in case of provisioning error condition.

2) Overload

When the test call is unsuccessful because of an overload condition, indicated by the receipt of a response message containing a warning header

including the warn-text `Overload`, no immediate recovery measures are taken.

However, the total time that the Test Call Generator is in overload level is measured. If the Test Call Generator stays in this level for more than half an hour, an additional alarm is issued. The Warning header is present in both Registration and Call Processing overload.

3) **Not OK**

When the Test Call Generator cannot complete a pre-defined amount of test cycles, an individual process may be restarted based on where the failure precisely is expected to have occurred.

The interval for the TCG test cycles is defined via an RTP variable. The default value is 64 seconds. This parameter is configurable between the minimum value of 32 seconds and the maximum of 300 seconds. The value is in seconds. If the administrator configures a value outside this range, the TCG falls back to the last valid value and restores this value in the RTP parameter.

6.12.3 How to Activate Test Call Generator

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP.
2) Navigate to **OpenScape Voice** > **Administration** > **Tools** > **Test Call Generator**.

   The window **System Health Check** appears in the work area.
3) Select the tab **Status**.
4) Mark the checkboxes **Activate** for the Test Call Generators 1 and 2.
5) Click **OK**.

6.12.4 How to Configure Test Call Generator

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP.
2) Navigate to **OpenScape Voice** > **Administration** > **Tools** > **Test Call Generator**.

   The window **System Health Check** appears in the work area.
3) Select the tab **Configuration**.

   A dialog opens, which displays all available configurable parameters.

4) Select in the field **Key Layout**:

   - **Show BG in Assistant**

     In most cases not necessary to modify. This can only be administered by service.
   - **Allow Forced Survivable Mode for Proxies**

     If OSV is one node (simplex) or in failover (duplex with one node down), and TCG goes into status 'Not OK', then **Allow Forced Survivable Mode for Proxies** means all proxies are forced to survivable mode.
   - Select the **Office Code**. Default value is 999999999.

5) Select in the field **Test Cycle**:

   - Select the **Interval**. Default value is 64.
   - Select the **Failure Threshold**. Default value is 3.
   - Select the **Success Threshold**. Default value is 2.

6) Select in the field **Test Call Generator 1**:

   - Select the **Keyset Directory Number**. Default value is 999999991.
   - Select the **Primary Listen Port**. Default value is 54325.
   - Select the **Backup Listen Port**. Default value is 54326.
   - Select the **Endpoint Name**. Default value is EP_TCG1.
   - Select the **Primary Listen Port**. Default value is 54327.
   - Select the **Backup Listen Port**. Default value is 54328.

   IMPORTANT:

   Don’t change the port numbers.

   ---

7) Select in the field **Test Call Generator 2**:

   - Select the **Keyset Directory Number**. Default value is 999999992.
   - Select the **Primary Listen Port**. Default value is 54325.
   - Select the **Backup Listen Port**. Default value is 54326.
   - Select the **Endpoint Name**. Default value is EP_TCG2.
   - Select the **Primary Listen Port**. Default value is 54327.
   - Select the **Backup Listen Port**. Default value is 54328.

   IMPORTANT:

   Don’t change the port numbers.

   ---

8) Click **OK**.

6.12.5 OSV Tracing Administration in OSV Assistant

The OSV Tracing Administration function previously located on the OSVTM server is now moved to the OSV Assistant. A new GUI for Continuous Trace Control is added under the menu tree Administration - Tools. On the new GUI the OSV Cluster name is shown as well as one refresh button. Both switching nodes are also represented on the GUI display. In the case of a simplex configuration, the second node display information is hidden.

Each column on the display has the following information:

Node Status (Active or Not Active)

Tracing Information: Filter (24/7 extern or 24/7 normal or 24/7 min; see below for description of Trace Levels); Start / Stop buttons; Status (Active, Not Active); Detail field (with status messages from the node).

Description of Trace Levels:

24/7extern: Enables a subset of trace facilities and flags for ccm and ttudProc.

24/7 normal: Enables a subset of trace facilities and flags for sip, sipRegistrar, uce, cstasm, ccm and ttudProc.

24/7 min: Enables a smaller set of 24/7 trace facilities and flags for sip, sipRegistrar, uce, cstasm, ccm and ttudProc.

File Export Information: Name/IP Address of trace file receiver/server (OSVTM); Directory of trace files on OSVTM; Login Username (of SFTP); Login Password (of SFTP); Start / Stop buttons; Status (Active, Not Active); Detail field (with status messages from the node).

Note: node 1 and node 2 of the OSV Cluster are administrated independently. Configuration of a node can only be changed when the node is active in state 4 (the key being that the SOAP interface is available).

6.12.5.1 How to Start OSV Tracing

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP.

2) Navigate to **OpenScape Voice** > **Administration** > **Tools** > **Continuous Tracing**.

The window **OpenScape Voice Tracing Administration** window appears in the work area.

3) The OSV **Cluster Name** is shown along with the node 1 information on the left side of the display and node 2 information on the right hand side of the display.

4) **Tracings Settings and Status**: Filter: Select 24/7 extern, 24/7 normal or 24/7 min.

5) **Host Information - Data File Export**:

On the Continuous Trace Data File Export Control section, enter the corresponding values for the OSV-TM server

a) **Name or IP Address**: *OSV-TM server IP address (nnn.nnn.nnn.nnn format)*

b) **Directory:** *OSV-TM system name (i.e., SYS1)*

c) **Login Username for Export Host**: *tracedata*

d) **Login Password for Export Host**: *OSV-TM FTP account password.* Note: The same account and password are used by SFTP.

6) Click on the **Start** button.

7) The **Link Status** should display "Active".

8) The **Refresh** button will update the transfer status showing the number of files that have been transferred.

   When the Continuous Trace Data File Export is activated, an SFTP session will be established, and all continuous trace data files will be transferred to the OSV-TM server (Export Host) for offline processing.

   Trace Files are transferred from oldest to newest and are deleted from the OpenScape Voice server after a successful transfer.

6.12.5.2 How to Stop OSV Tracing

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP.
2) Navigate to **OpenScape Voice** > **Administration** > **Tools** > **Continuous Tracing**.

   The window **OpenScape Voice Tracing Administration** window appears in the work area.
3) The OSV Cluster name is shown along with the node 1 information on the left side of the display and node 2 information on the right hand side of the display.
4) Click on the appropriate **Stop**button (for each node) in the Tracing Settings and Status section of the screen to terminate the tracing.
5) Click on the appropriate **Stop**button (for each node) in the Host Information - Data File Export section of the screen to terminate the exporting of trace data.

6.13 State of a Node

A node can be in one of four states: 1 - 4 at any time. With command `srxctrl` the state is changeable, changes are written in logs to check and subsystems of nodes can be forced started or stopped.

Functional Sequence

The script `srxctrl` changes the state of a node. The different states stand for:

- State 1

  The node is not part of the cluster and no application(s) is/are running on the node.

  NOTICE:

  State 1 is historical and is not achievable via `srxctrl`.

- State 2

  The clustering software is running on this node and the node is part of the cluster.

- State 3

  All the necessary databases are running on the node.
- State 4

  RTP platform and OpenScape Voice applications are running on the node.

6.13.1 How to Start / Stop a Node

Prerequisites

Adequate administrative permissions

Step by Step

1) Login as `root`.

2) To force stop of the subsystems listed, run `srxctrl -Q <mmgr,snort,xcm,oplog,oprtt>|all` from `/unisphere/srx3000/srx/startup/srxctrl`.

- The argument 'all' will stop all subsystems. This option is mutually exclusive to any other option.

  NOTICE:

  This option applies to the local node only.
- Subsystem mmgr

  The Maintenance Manager (mmgr) serves for activating and controlling OpenScape Voice maintenance jobs – for example, to back up and restore files.
- Subsystem snort

  Snort is a open source network intrusion detection and prevention system (NIDS/NIPS) capable of performing real-time traffic analysis and packet logging on IP networks.
- Subsystem xcm

  Xcm is cross channel monitor.
- Subsystem oplog

  OPLOG OpenScape Voice software uses this component to store non-alarmed events in different log files. Logged events are counted and may generate threshold crossing alarms if too many log events are reported within 5 or 15 minutes.
- Subsystem oprtt

  Oprtt will allow RTT (Real Time Trace) to continue tracing.

3) To force start of the subsystems listed, run `srxctrl -S <mmgr,snort,xcm,oplog,oprtt>|all` [srxctrl_log_file [rtp_log_file]] from `/unisphere/srx3000/srx/startup/srxctrl`.

- The arguments, see step 2 will start one or all subsystems.

  NOTICE:

  This option applies to the local node only.

6.13.2 How to Change the State of a Node

Note: 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.
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.

Prerequisites

Adequate administrative permissions

Step by Step

1) Login as `root`.
2) To change the state of a node, run `srxctrl node_state node_state` [srxctrl_log_file [rtp_log_file]] from `/unisphere/srx3000/srx/startup/srxctrl`.
   - Example:

     To bring the local node to state 4

     (and optionally: using log file names `/tmp/srx_ctrl` and `/tmp/rtp_start`):

     Run `srxctrl 4 0 /tmp/srx_ctrl /tmp/rtp_start`

NOTICE:

If a node_state is used then a second node_state has also to be used.

The first node_state relates to the local node. The second node state relates to the remote node.

Zero (i.e. 0) is accepted as a parameter for a state of a node and means no change to the state of that node.

NOTICE:

More information: Run `srxctrl -h`

6.14 Traffic Measurement

OpenScape Voice provides different traffic measurements that are collected and recorded as CSV files by the OMM (Operational Measurements Manager). The files may then be downloaded through SFTP to any platform associated with the

collection of performance data. The files may be transferred in either binary or ASCII format.

The following types of traffic measurement data are collected:

- Event-based traffic measurements:

  These measurements are cumulative, and are driven by specific event occurrences such as successful calls, call failures, and any kind of state transition. This type of traffic data is measured for each business group.
- Usage-based traffic measurements:

  These measurements are based on the cumulative duration of a specified event or condition. This type of traffic data is measured for each Business Group (BG).

The traffic measurements are available in OpenScape Voice for:

- BGs
- Hunt groups
- CAC (Call Admission Control)
- SIP endpoints
- Dynamic licensing
- Basic Traffic Tool

IMPORTANT:

OMM measurements data is stored in shared memory until it is written in the .oms files at the specified time intervals. If the switch leaves the state 4 4 by any operation like reboot, image revert, snapshot revert or srxctrl, all data that has not been written to the files will be lost.

6.14.1 OMM (Operational Measurements Manager)

Traffic Measurements (TM) are responsible for reporting increment counters for call events, and an API exists with the Operational Measurements Manager (OMM) to communicate this information. This functionality primarily resides in the Routing and Translation Manager (RTM) and Retailer and Subscriber System (RSS). The OMM in the OpenScape Voice system is responsible for the collection, generation, and maintenance of these performance counters or indicators.

6.14.1.1 OMM (Operational Measurements Manager) Configuration Data

The OMM in the OpenScape Voice system is responsible for the collection, generation, and maintenance of these performance counters or indicators according its configuration data.

For example, the following properties can be modified by setting RTP system parameters:

- the retention period
- the retention period in days

Table 1: Traffic Measurements configuration parameters. Default settings are indicated in bold

Parameter	Description
5 Min Ret Period	Interaction: Read/WriteThis parameter specifies the 5 minute Retention Period in days.Possible values are:1 – 31 daysDefault: **7**
15 Min Ret Period	Interaction: Read/WriteThis parameter specifies the 15 minute Retention Period in days.Possible values are:1 – 31 daysDefault: **7**
30 Min Ret Period	Interaction: Read/WriteThis parameter specifies the 30 minute Retention Period in days.Possible values are:1 – 31 daysDefault: **7**
Hourly Ret Period	Interaction: Read/WriteThis parameter specifies the Hourly Retention Period in days.Possible values are:1 – 31 daysDefault: **7**
Daily Ret Period	Interaction: Read/WriteThis parameter specifies the Daily Retention Period in days.Possible values are:1 – 31 daysDefault: **7**

6.14.1.2 OMM (Operational Measurements Manager) Measurement Settings

The OMM in the OpenScape Voice system is responsible for the collection, generation, and maintenance of these performance counters or indicators according its measurements setting data.

For example, the following properties can be modified by setting RTP system parameters:

- OMM Index
- Measurement Group Name
- Retention flag and period in days

Table 2: OMM Measurement parameters.

Parameter	Description
OMM Index	Interaction: Read Only This parameter specifies an unique, non-reusable index assigned when a TM OMM entry is created.

Parameter	Description
Measurement Group Name	Interaction: Read Only This parameter specifies the name of the TM Measurement group. The maximum length is 63 characters.NOTES:• This object cannot be modified.• The following measurement groups are the only ones possible with the OpenScape Voice system:– Business Groups (5)– MLHG (7)– CAC Group (8)– ENUMSERVER_GROUP (9)– SIP Endpoint Group (10)– Dynamic Licensing Group (12)– OSMO Licensing Group (14)– List All (99)
5 Minute Retention Flag	Interaction: Read/Write This parameter specifies whether the OMM 5-minute Traffic Measurement associated with this group member is turned on or turned off.Possible values are:• Enabled (1)• Disabled (2)
15 Minute Retention Flag	Interaction: Read/Write This parameter specifies whether the OMM 15-minute Traffic Measurement associated with this group member is turned on or turned off.Possible values are:• Enabled (1)• Disabled (2)
30 Minute Retention Flag	Interaction: Read/WriteThis parameter specifies whether the OMM 30-minute Traffic Measurement associated with this group member is turned on or turned off.Possible values are:• Enabled (1)• Disabled (2)
Hourly Retention Flag	Interaction: Read/WriteThis parameter specifies whether the OMM Hourly Traffic Measurement associated with this group member is turned on or turned off.Possible values are:• Enabled (1)• Disabled (2)
Daily Retention Flag	Interaction: Read/WriteThis parameter specifies whether the OMM Daily Traffic Measurement associated with this group member is turned on or turned off.Possible values are:• Enabled (1)• Disabled (2)

6.14.1.3 CLI (Command Line Interface)

The purpose of the Element Management Command Line Interface (CLI) is to supply a command line interface to use for the provisioning and configuration of the OpenScape Voice system.

NOTICE:

If you are familiar with CLI ignore chapters CLI (Command Line Interface) and How to Open CLI (Command Line Interface) Session.

The CLI is accessible in two manners: either locally (using a local console) or remotely (using the SSH Secure Shell) which requires an Ethernet or LAN connection. There are two modes of operation for the CLI:

- CLI Menu Mode
- CLI Expert Mode

Functional Sequence

CLI Menu Mode:

The CLI Menu mode is active by default. The entries in the upper area (options 1 - 5) of the main menu provide access to RTP-specific management functions.

The Application-level Management option (6) opens a second set of provisioning menus that house a vast collection of implemented OpenScape Voice options comprising of all aspects of the OpenScape Voice's provisioning.

The entries in the lower area (options 93 -99) are concerned with the internal functionality of the CLI.

System Specific Information

Because the CLI is accessible using a local console for local access or a SSH Secure Shell interface (requires an Ethernet or LAN connection) for remote access, this section explains how to start the CLI from both possibilities. There is no difference in functionality or capability whether the local console or remote access is used to connect to the CLI. The only difference between the two connections is when connected remotely by way of the Secure Shell interface, users can scroll up and down to see the history of their actions (for example, prior menu selections, choices). Using local access does not allow the history to be viewed.

6.14.1.4 How to Open a CLI (Command Line Interface) Session

The CLI Menu Mode is active by default. It provides menu choices for OpenScape Voice operations. The menu-driven CLI is based on the RTP (Resilient Telco Platform) CLI menus.

Prerequisites

Adequate administrative permissions

Step by Step

1) Start a (remote) shell.

2) Enter `su - srx` to switch to the srx user. Press ENTER.

3) Enter `startCli` to start the Command Line Interface. Press ENTER.

4) Enter user name `sysad`. Press ENTER.

5) When prompted for a password, type it and press ENTER.

NOTICE:

Upon initial entry into the CLI, you may be asked to set the password

IMPORTANT:

As a security measure, it is recommended that you change the default password (option 97) after the initial login.

CLI Menu Mode is started and ready for choosing a submenu.

6.14.1.5 How to Display OMM Configuration Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report Settings** > **General**
2) Check for the logging frequencies in the **Retention Periods** area.

Related tasks

How to Configure General Report Settings on page 356

6.14.1.6 How to Display OMM (Operational Measurements Manager) Measurement Settings

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report Settings**
2) Navigating in the tabs you can see the settings for each statistic type.

Related tasks

How to Configure Call Statistics Reports on page 357
How to Configure Hunt Group Statistics Settings on page 357
How to Configure CAC Group Statistics Reports on page 358
How to Configure Dynamic License Statistics Reports

6.14.2 Statistics Reports

For different statistical reasons OpenScape Voice generates reports for all BGs (Business Groups) or for a selected, specific BG.

The Report Settings dialog allows the subscriber to specify the settings (for all BGs) for the following types of statistics reports:

General settings (for all BGs)

Call Statistics - generic settings for Call Statistics

Hunt Group Statistics - generic settings for Hunt Group Statistics

CAC Group Statistics - generic settings for CAC Group Statistics

License Statistics

6.14.2.1 How to Configure General Report Settings

The Report dialog allows you to specify the settings (for all BGs) for the following types of statistics reports: General settings (for all BGs), Call Statistics - generic settings for Call Statistics, Hunt Group Statistics - generic settings for Hunt Group Statistics, CAC Group Statistics - generic settings for CAC Group Statistics, Dynamic License Statistics.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report** > **General**
2) Mark the check box **Enable logging** to enable/disable the logging feature on the switch in the **Logging** area.
3) Select for the different logging frequencies a retention period between 1 and 31 days in the **Retention Periods** area.

   For every logging frequency you can specify the number of days, the switch will retain the generated files on the switch. For example, if you specify 5 days for the 15 minute data, then the switch will be keeping only those 15 minute files that are not more than 5 days old.
4) Click **Save**.

Related tasks

How to Display OMM Configuration Data on page 355

6.14.2.2 How to Configure Call Statistics Reports

These settings take effect only on the collection of Call Statistics for a Business Group. You can enable the collection of this data for every Business Group separately via the Call Statistics screen in the Business Group Center.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report** > **Call Statistics**
2) Select a logging frequency type **Every ...** in the **Data Logging Frequency** area. Values are: 5, 15, 30 minutes, every hour, every day.

   NOTICE:

   Use the check boxes to enable or disable the frequency types for the collection of Business Group Call Statistics. You can specify any combination of frequency types

3) Click **Save**.

   NOTICE:

   The Basic call statistics display the daily call statistics of the same day, depending on the Start and End Time configured by the user in **Statistics > Call**

Related tasks

How to Display OMM (Operational Measurements Manager) Measurement Settings on page 355

6.14.2.3 How to Configure Hunt Group Statistics Settings

These settings take effect only on the collection of Traffic Measurement Data of Hunt Groups. You can enable the collection of this data for every Hunt Group separately via the Edit-screen of Hunt Group.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report** > **Hunt Group Statistics**

2) Select a logging frequency type **Every ...** in the **Data Logging Frequency** area. Values are: 5, 15, 30 minutes, every hour, every day.

NOTICE:

Use the check boxes to enable or disable the frequency types for the collection of Hunt Group Statistics. You can specify any combination of frequency types.

3) Click **Save**.

Related concepts

Hunt Group Traffic Measurement on page 365

Related tasks

How to Display OMM (Operational Measurements Manager) Measurement Settings on page 355

6.14.2.4 How to Configure CAC Group Statistics Reports

These settings take effect only on the collection of statistics for CAC Groups.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report** > **CAC Groups Statistics**
2) Select a logging frequency type **Every ...** in the **Data Logging Frequency** area. Values are: 5, 15, 30 minutes, every hour, every day.

NOTICE:

Use the check boxes to enable or disable the frequency types for the collection of CAC Group Statistics. You can specify any combination of frequency types.

3) Click **Save**.

Related concepts

CAC (Call Admission Control) Traffic Measurements on page 362

Related tasks

How to Display OMM (Operational Measurements Manager) Measurement Settings on page 355

6.14.2.5 How to Activate License Logging

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Administration** > **General Settings** > **Report** > **Licenses Statistics**
2) Use the checkbox to enable or disable the collection of License Statistics:
   - Dynamic License every 5 minutes
   - Basic License every 5 minutes
   - Essential License every 5 minutes
   - OpenScape Mobile License every 5 minutes
   - Encryption License every 5 minutes
   - Unify Phone License every 5 minutes
3) Click **Save**.

6.14.3 Basic Traffic Tool

The Basic Traffic Tool is a performance monitoring tool that helps analyze performance data for the OpenScape Voice. The application has two software components: server and client.

The server collects data into a file in a defined time frame. It runs under a cron job.

The client, a Windows based JAVA application, generates graphical and numerical displays representing the data collected from the CSV file.

Functional Sequence

An administrator opens an SFTP shell and manually transfers the file to the computer where the client is installed.

Graphical and numerical data is visible on separate screens:

- Graphical data

  The following data appears in graphical form, each on a separate screen:

  – Number of SIP calls over a selected period
  – Number of SIP calls for the current day
  – Busy hour call attempts over a selected period
  – Busy hour call attempts for the current day

  The graphical output is based on data the system collects every 15 minutes. The user can print the output from any of the screens.
- Numerical data

  In addition to the graphical data, the following data appears in numeric form each on a separate screen:

  – Statistical data for selected period
  – Statistical data for today

  Numerical data is displayed for the following fields:

  – Number of calls within the specified time period
  – Number of incoming calls within the specified time period
  – Number of outgoing calls within the specified time period
  – Unsuccessful call attempts within the specified time period
  – Busy hour call attempts within the specified time period

The user can:

- Copy and paste the data in another file.
- Print the tab sheet that provides the numerical output.

Other Characteristics

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.

Another traffic measurement tool, the BG (Business Group) Traffic Measurements feature provides counts of several types of OpenScape Voice activity on a per-BG basis.

6.14.4 BG (Business Group) Traffic Measurement

The BG (Business Group) Traffic Measurements feature provides counts of several types of OpenScape Voice activity on a per-Business Group basis. The administrator can use these measurements to monitor the company's calling patterns and usage at a high level, or can analyze them in greater detail if desired.

The administrator can activate or deactivate this feature for the BG.

Functional Sequence

The BG measurement data is delivered to OpenScape Voice Assistant. The administrator can access the measurements and monitor the company's calling patterns by simply performing a visual inspection of the reported data.

System Specific Information

Administrators can perform additional analysis of measurement data to determine:

- The percentage of calls placed outside the business group
- The business group calling features that are under- or overused.

The OpenScape Voice system provides traffic measurements that are collected and recorded as CSV files by the OMM (Operational Measurements Manager). The files may then be downloaded through SFTP to any Telco platform concerned with the collection of performance data. The files may be transferred in either binary or ASCII format.

Other Characteristics

Table 3: The traffic measurements available for each business group

Measurement	Description
Originating calls	The number of successful (connected) and unsuccessful (Busy, Not Answered, ...) calls originating from Subscribers - not Endpoints - in the BG. BG internal calls and calls leaving the BG are counted. Originating Calls = Intragroup Calls + Public Net Calls + Private Net Calls + Feature Calls + XXX

Measurement	Description
Terminating calls	The number of successful and unsuccessful calls intended to terminate on Subscribers or Endpoints in the BG. Terminating Calls = Intergroup Calls + DID Calls
Intragroup calls	The number of successful and unsuccessful BG internal calls from Subscribers or Endpoints to Subscribers or Endpoints in the BG.
Feature use	The number of times the system's treatment of a call is affected by feature treatment. The count is incremented each time a feature related function is performed in lieu of, or in addition to, a normal call processing function.
Feature activation	The number of times the system responds to requests to allow a feature's function. This count is best exemplified by existing station call forwarding—all calls activation counts.
Feature deactivation	The number of times the system responds to requests to deny or end a feature's function.
Private Net Calls	The number of successful and unsuccessful calls routed via a PAC* set to "Off-net Access". **NOTICE:** The Prefix Access Code in the NP where the subscriber or endpoint is located (not Common Numbering Plan or Global NP
Public Net Calls	The number of successful and unsuccessful calls routed via a PAC* set to "On-net Access" or ’’Extension Dialing’’. **NOTICE:** The Prefix Access Code in the NP where the subscriber or endpoint is located (not Common Numbering Plan or Global NP
DID calls	The number of successful and unsuccessful calls intended to terminate on Subscribers or Endpoints in the BG and coming from an EP located in the E.164 Numbering Plan (Global Numbering Plan).
Attendant Calls Completed, Attendant Calls Busy	Event counts and overflow measurements on Attendant Calls Completed and Attendant Calls Busy. This is the number of calls to the attendant and overflows.

Another performance monitoring tool is the basic traffic tool that is used to view snapshots of the traffic for incoming SIP calls to OpenScape Voice.

6.14.4.1 How to Display Call Statistics Reports

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Business Group**.
   The window **List Business Groups** is displayed.
2) Select a Business Group from the dropdown list Available Business Groups.
3) Navigate to **Statistics** > **Call Statistics**.
   The window **Call Statistics** is displayed.
4) Click **Enable Metrics** if not enabled to get reports.
   The window **Call Statistics** displays the following report types:
   - - Date
   - - Calls Report
   - - Custom Calls Report
   - - Enhanced Services Report
5) Click **View Report** below the desired report type.
   The detailed information on the statistic results summary is displayed.

6.14.5 CAC (Call Admission Control) Traffic Measurements

OpenScape Voice provides CAC (Call Admission Control) Traffic Measurements. These Traffic Measurements are collected via a CAC measurement group in the OMM (Operational Measurements Manager).

The CAC measurements are stored in a log file for post-processing. Although OpenScape Voice does not offer a mechanism to read these measurements in real time, OpenScape Voice Assistant allows the administrator to view the information in the stored log files in a table format.

Functional Sequence

The following measurements are collected for all provisioned CAC Policies and Group-to-Group CAC Policies:

- CAC Policy ID
- CAC Policy name
- CAC Group name
- Number of offered calls
- Number of blocked calls
- Maximum number of calls
- Maximum bandwidth
- Number of offered voice calls
- Number of blocked voice calls
- Number of offered video calls
- Number of blocked video calls
- Maximum value for the counter

System Specific Information

The CAC measurements are stored in a log file for post-processing. One file is created for every collection interval that contains all the CAC data for that interval. Although OpenScape Voice does not offer a mechanism to read these measurements in real time, OpenScape Voice Assistant allows the administrator to view the information in the stored log files in a table format.

Table 4: This traffic measurements are collected for each provisioned CAC Group

CAC Policy ID	The CAC Policy ID is used as the unique identifier for the counters. If there are two CAC Policy IDs associated with the same CAC Group, two counters are used, one for each CAC Policy ID. For Group-to-Group CAC Policies, the CAC Group name in the reports must have the following format: *Group 1, -> Group 2*, where CAC Group1 and CAC Group2 are the names of the two CAC Groups.
CAC Policy Name	The CAC Policy name is used to provide a user friendly identifier of each CAC POLICY. For Group-To-Group CAC Policies, the CAC Group name included in the reports must have the following format: "Group1 <-> Group2", where CAC Group1 and CAC Group2 are the names of the two CAC Groups.
CAC Group Name	This represents the group of endpoints being served by the bandwidth-limited link which needs to be monitored. A CAC Group is the entity to which the CAC Policies are applied. Groups are defined based on one of the following parameters: • Subnet (up to 64 subnets may be used) • IP address (up to 64 IP addresses may be used) • DN (Directory Number): this can be a DN prefix (for example, 1561555*) or the DN of a single user (for example, 15615550110). Up to 64 DNs (with wildcards support) may be used

Number of Offered Calls	This counter is incremented each time the OpenScape Voice attempts to route a call over the access link associated with a CAC Group. A call that is successfully completed over multiple access links (for example, a call between two branch locations) is counted as an offered call in both the originating and terminating CAC Groups. However, if the call is blocked due to bandwidth limitations on the originating access link, only the offered calls counter of the originating CAC Group is incremented; the offered calls counter of the terminating CAC Group is not incremented. In the same way, if the call is blocked due to bandwidth limitations on the terminating access link, only the offered calls counter of the terminating CAC Group is incremented; the offered calls counter of the originating CAC Group is not incremented. This counter shall only be incremented if the call being established requires the Concurrent Number Of Calls counter for the CAC Policy to be incremented as well. This means, for instance, that the Offered Calls counter is only incremented by 1 in scenarios where the call is forked to multiple destinations in the same CAC group (for example, keysets with multiple line appearances, simultaneous ringing multiple contacts, and the like).
Number of Blocked Calls	This counter is incremented each time the OpenScape Voice attempts to route a call over the access link associated with a CAC Group but the call is denied or rerouted due to the CAC limitations imposed by the associated CAC Policy. Notice that a “blocked call” in this context may have been successfully completed by rerouting through an alternate route, for example, through the local PSTN (Public Switched Telephone Network) gateway.
Maximum number of calls	This counter represents the maximum number of calls.
Maximum bandwidth	This counter represents the maximum amount of available bandwidth.
Number of offered voice calls	This counter represents the number of offered voice calls.
Number of blocked voice calls	This counter represents the number of blocked voice calls.
Number of offered video calls	This counter represents the number of offered video calls.
Number of blocked video calls	This counter represents the number of blocked video calls.

Maximum value for the counter	This counter represents the maximum value of the counter.

Other Characteristics

Traffic Measurements are collected and recorded by the OMM in the form of CSV files that can be found at `/global/user/oms/SRX3000-yyyymmddThhmm00/cac15.oms`. Using SFTP these files may be downloaded to any Telco platform concerned with the collection of performance data. The files may be transferred in either binary or ASCII format.

Each record is in CSV format and contains the following information:

```
2022-15-06T15:30:00.0
1,CAC_POLICY_NAME_1,CAC_NAME_1,50,32,3,40000,1,2,3,4
2,CAC_POLICY_NAME_2,CAC_NAME_2,32,10,2,30000,2,1,4,3
3,CAC_POLICY_NAME_3,CAC_NAME_3,1,4,5,32000,2,0,3,1
;;;END OF FILE
```

The CLI and the OpenScape Voice Assistant support the administration of the CAC group's scheduling in OMM. This includes setting the Logging Interval and the Retention Period for the measurements. This data can be invaluable to the network planner in evaluating the performance of the network and finding remedies for observed problems.

Related tasks

How to Configure CAC Group Statistics Reports on page 358

6.14.6 Hunt Group Traffic Measurement

The Hunt Group Traffic Measurements feature provides counts of Hunt Group and queuing activity on a per-Hunt Group basis. The administrator can use these measurements to monitor the company's calling patterns and usage at a high level, or can analyze them in greater detail if desired.

The administrator specifies whether to maintain traffic statistics for a particular Hunt Group and the interval in which to collect them.

Functional Sequence

The Hunt Group measurement data is delivered to OpenScape Voice Assistant. The administrator can access the Hunt Groups measurements and monitor the Hunt Group by periodically performing a visual inspection of the reported data.

System Specific Information

Administrator can perform additional analysis of this data to determine:

- The average time a HNG member spends on outgoing calls.
- The number of calls that are not initially able to be connected to a Hunt Group member, and instead are overflowed or queued.
- The number of calls that are unable to queue for a Hunt Group member because the queue is full.

- The number of callers who hang up before speaking to a Hunt Group member.

Table 5: The traffic measurements available for each hunt group.

Measurement	Description
Incoming calls	The number of incoming calls that attempt to terminate to the hunt group.
Outgoing calls	The number of outgoing calls originated by hunt group members.
Overflow calls	The number of incoming calls that are initially unable to connect to a hunt group member because no hunt group member is available.
Hunt Group usage	The total usage (in seconds) for calls incoming to and outgoing from the hunt group. For incoming calls, the usage measurement begins when the call is answered by a hunt group member. For outgoing calls, the usage measurement begins when the called party answers the call.
Queue attempts	When a queue is associated with the hunt group, the number of attempts to place a call in queue. It records both successful and unsuccessful attempts.
Queue usage	When a queue is associated with the hunt group, the total usage (in seconds) for all calls in queue.
Queue overflow	When a queue is associated with the hunt group, the number of attempts queue a call that failed because the queue was full.
Queue abandons	When a queue is associated with the hunt group, the number of queued calls abandoned by the originator before being connected to a hunt group member.
Other Requirements	• When Night Service is active, do not peg any MLHG counter. • All counters should be pegged for all hunt algorithms. • Each routing attempt to an MLHG (and to multiple MLHGs) should peg the appropriate counters.

Other Characteristics

Each record in the files is in CSV format, and contains fields for the hunt group ID, the hunt group Pilot DN, the associated BG Name (blank if there is no BG assigned to the item), and then the measurements.

ResetTime is a field that takes a timestamp value whenever OMM process restarts unexpectedly for example, a process crash or restart. It provides the time and day information on a OMM report that shows when statistics were started to be collected (due to this unexpected restart). Otherwise this field in normal situations remains an empty string.

The record fields of the OMS files appear as follows:

Time stamp,

PilotDN 1, BGName, IncomingCalls, OutgoingCalls, OverflowCalls, MLHGUsage,

QueueAttempts, QueueAbandons, QueueOverflows, QueueUsage, ResetTimePilotDN 2, BGName, IncomingCalls, OutgoingCalls, OverflowCalls, MLHGUsage,

QueueAttempts, QueueAbandons, QueueOverflows, QueueUsage,

ResetTime

Related tasks

How to Configure Hunt Group Statistics Settings on page 357

6.14.6.1 How to Display Hunt Group Statistic Results

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **OpenScape Voice** > **Business Group**.
   The window **List Business Groups** is displayed.
2) Select a Business Group from the dropdown list **Available Business Groups**.
3) Navigate to **Statistics** > **Hunt Group Statistics**.
   The dialog **Hunt Group Statistics** is displayed, showing the Pilot IDs of the HNGs (Hunt Groups) configured for this BG.
4) Select a **Pilot ID** of the HNG.
   The dialog **Hunt Group Statistics** is displayed, showing the detailed statistic results summary for the selected HNG.

6.14.6.2 How to Enable Hunt Group Statistics of a Specific Hunt Group

DN (Directory Number) administrators and BG (Business Group) administrators can access this function to enable or disable traffic measurements for HNGs (Hunt Groups) associated with the BGs assigned in the user's BG Access list.

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP and activate the **OpenScape Voice** tab.
2) Navigate to **Business Group**.
3) Select the adequate switch from the list of **Available Switches**.
4) Select the adequate BG from the list of **Available Business Groups**.
5) Navigate to **Teams** > **Hunt Groups**.
   The dialog **Hunt Groups** is displayed.
6) Select a HNG from the list.
   If the list is empty, you must create a new Hunt Group first.

7) Click **Edit**.

   The dialog **Hunt Group** for the selected BG is displayed.

8) Click on the tab **Advanced**.

9) Navigate to the area **Settings**.

10) Enable the check box **Collect traffic measurement data**.

The following features are activated:

- Collection of traffic measurement data
- Display of Hunt Group Statistics

6.14.7 Traffic Measurements for Dynamic Licensing

Dynamic Licenses control the number of concurrent registered subscribers. Each registered subscriber reserves a single license, independently of the number of the clients, registered and associated with this particular subscriber/ primary Directory Number (DN) (multi contact scenario).

Subscribers are allowed to register SIP clients, such as the usual SIP phones, soft-clients, and so on. Each registered subscriber reserves a single Dynamic License independently of the number of clients that have been registered to this particular prime DN (subscriber). This is also applicable to DNs registered through Session Border Controller (SBCs).

For keysets, of the prime line cannot register, the registration requests of the secondary lines are also rejected. OpenScape Voice never reserves a license for secondary and phantom lines.

Traffic measurements are collected and recorded by the Operational Measurements Manager (OMM) in the form of CSV files. Using FTP (actually SFTP) these files may be downloaded to any Telco platform concerned with the collection of performance data. The files may be transferred in either binary or ASCII format.

Functional Sequence

The measurements are written into files. One file is created for every collection interval that contains all the Dynamic License data for that interval. The file names indicate that the data is for Dynamic License and have a timestamp indicating the time and interval length for the collected data.The file naming is consistent with the existing OMM file naming for other measurement groups, such as Multiline Hunt Group (MLHG) and Call Admission Control (CAC) data.

Logging for Dynamic License is done using Time Base Logging. For each interval, OMM logs Dynamic License measurement data in the softswitch in the file path: `/global/user/oms/.`

Under this path, a time-based folder is created and inside this the Dynamic License log files are written.

System Specific Information

License Manager maintains the following internal counters for Dynamic Licenses:

Counters	Description
Dynamic licenses assigned to the system	This number can change only by the installation of new licensing files
Current usage of Dynamic licenses	This number is volatile, changing whenever a SIP client registers or expires.
The maximum usage of Dynamic licenses over the last 24h period	This number holds the maximum value of the current usage counter that has been reported during this period.
Customer violations	This is a counter, holding the number of usage violations.
Customer violation limit	This is the number of usage violations the system allows, before activating the enforcement. This should be a hard coded value of 10 as the Regular Licensing File (RLF) has no field for that today.

For information on how to Monitor Dynamic License please refer to Licensing Administration > How to Monitor Dynamic Licensing.

6.14.8 SIP EP (Endpoint) Traffic Measurements

SNMP Performance Measurement reporting enhancements are required to support third party Network Operations Centers. These enhancements allow the SIP message exchange to be monitored between the **OpenScape Voice**, **OpenScape Branch** and a SIP endpoint such as a gateway or VoIP service provider. Monitoring such message exchanges can lead to detection of network problems and speed up trouble isolation and resolution, by reducing the need to capture message traces and reducing escalations. SIPSM supports SIP Endpoint (SIP EP) counters that are the same as the set of system wide SIPSM counts.

The SIPSM interfaces with the Operational Measurements Manager (OMM) shared memory and is always considered enabled for pegging the SIP EP statistics regardless of whether or not the OMM has been scheduled for one or more intervals. This allows the Simple Network Management Protocol (SNMP) to access the SIP EP statistics even when the OMM has not been enabled for producing SIP EP measurement files. SIPSM is always enabled to peg all the nonsubscriber SIP EP counters.

Functional Sequence

The measurements are written into files. One file is created for every collection interval that contains all the SIP EP data for that interval. The filenames indicate that the data is for SIP EP and have a timestamp indicating the time and interval length for the collected data. The file naming is consistent with the existing OMM file naming for other measurement groups, such as Trunk Group and Primary Rate Interface (PRI) data.

Logging for SIP EP is done using Time Base Logging. For each interval, OMM logs Electronic Number Mapping (ENUM) measurement data in the softswitch in a file path.

Under this path, a time-based folder is created and inside this the SIP EP log files are written.

System Specific Information

The table below displays the system specific information in the SIP EP printing format order.

Table 6: System Specific Information for SIP EP (Endpoint) Traffic Measurements

Message	Description
eNumRegisterRcvd	Number of Register messages received
eNumInviteRcvd	Number of Invite messages received
eNumTryingRcvd	Number of Trying messages received
eNumRingingRcvd	Number of Ringing messages received
eNum200ForInfoRcvd	Number of 200 OK messages received for Info messages
eNumInfoRcvd	Number of Info messages received
eNumReferRcvd	Number of Refer messages received
eNum200ForSubscribeRcvd	Number of 200 OK messages received for Subscribe messages
eNumSubscribeRcvd	Number of Subscribe messages received
eNum200ForNotifyRcvd	Number of 200 OK messages received for Notify messages
eNumNotifyRcvd	Number of Notify messages received
eNum202AcceptedRcvd	Number of 202 Accepted messages received
eNumMultipleChoicesRcvd	Number of Multiple Choices messages received
eNum4XX6XXForReferRcvd	Number of 4XX6XX messages received for Refer messages
eNum4XX6XXForNotifyRcvd	Number of 4XX6XX messages received for Notify messages
eNum4XX6XXForSubscribeRcvd	Number of 4XX6XX messages received for Subscribe messages
eNum200ForInviteRcvd	Number of 200 OK messages received for Invite messages
eNumAckForInviteRcvd	Number of ACK messages received for Invite messages
eNumAckForErrorRcvd	Number of ACK messages received for Error messages
eNumAckForCancelRcvd	Number of ACK messages received for Cancel messages
eNumByeRcvd	Number of Bye messages received
eNum200ForByeRcvd	Number of 200 OK messages received for Bye messages
eNumCancelRcvd	Number of Cancel messages received
eNum200ForCancelRcvd	Number of 200 OK messages received for Cancel messages
eNumErrorRcvd	Number of Error messages received
eNum487Rcvd	Number of 487 messages received
eNum301Rcvd	Number of 301 messages received
eNum302Rcvd	Number of 302 messages received

Message	Description
eNumPrackRcvd	Number of Prack messages received
eNum200ForPrackRcvd	Number of 200 OK messages received for Prack messages
eNumUpdateRcvd	Number of Update messages received
eNum200ForUpdateRcvd	Number of 200 OK messages received for Update messages
eNumSessionProgressRcvd	Number of Session Progress messages received
eNumOther1xxRcvd	Number of Other 1xx messages received
eNumOther2xxRcvd	Number of Other 2xx messages received
eNumOther3xxRcvd	Number of Other 3xx messages received
eNumOther4xxRcvd	Number of Other 4xx messages received
eNumOther5xxRcvd	Number of Other 5xx messages received
eNumOther6xxRcvd	Number of Other 6xx messages received
eNumUnsupportedMethod	Number of Unsupported Method messages
eNum200ForRegSent	Number of 200 OK messages sent for Registration messages
eNumInviteSent	Number of Invite messages sent
eNumTryingSent	Number of Trying messages sent
eNumRingingSent	Number of Ringing messages sent
eNum200ForInfoSent	Number of 200 OK messages sent for Info messages
eNumInfoSent	Number of Info messages sent
eNumReferSent	Number of Refer messages sent
eNum200ForSubscribeSent	Number of 200 OK messages sent for Subscribe messages
eNumSubscribeSent	Number of Subscribe messages sent
eNum200ForNotifySent	Number of 200 OK messages sent for Notify messages
eNumNotifySent	Number of Notify messages sent
eNum202AcceptedSent	Number of 202 Accepted messages sent
eNum4XX6XXForReferSent	Number of 4XX6XX messages sent for Refer messages
eNum4XX6XXForNotifySent	Number of 4XX6XX messages sent for Notify messages
eNum4XX6XXForSubscribeSent	Number of 4XX6XX messages sent for Subscribe messages
eNum200ForInviteSent	Number of 200OK messages sent for Invite messages
eNumAckForInviteSent	Number of ACK messages sent for Invite messages
eNumAckForErrSent	Number of ACK messages sent for Error messages
eNumAckForCancelSent	Number of ACK messages sent for Cancel messages
eNumAckFor3xxSent	Number of ACK messages sent for 3xx messages
eNumByeSent	Number of Bye messages sent
eNum200ForByeSent	Number of 200 OK messages sent for Bye messages
eNumCancelSent	Number of Cancel messages sent
eNum200ForCancelSent	Number of 200 OK messages sent for Cancel messages

Message	Description
eNumErrorSent	Number of Error messages sent
eNum487Sent	Number of 487 messages sent
eNumPrackSent	Number of Prack messages sent
eNum200ForPrackSent	Number of 200 OK messages sent for Prack messages
eNumUpdateSent	Number of Update messages sent
eNum200ForUpdateSent	Number of 200 OK messages sent for Update messages
eNumSessionProgressSent	Number of Session Progress messages sent
eNumOther1xxSent	Number of Other 1xx messages sent
eNumOther2xxSent	Number of Other 2xx messages sent
eNumOther3xxSent	Number of Other 3xx messages sent
eNumOther4xxSent	Number of Other 4xx messages sent
eNumOther5xxSent	Number of Other 5xx messages sent
eNumOther6xxSent	Number of Other 6xx messages sent
eNumMaxCounters	Number of Max Counters

The following are the realtime statistics that are kept on a per-Endpoint basis:

- Number of Incoming Seizures (incoming INVITE)
- Number of Outgoing Seizures (outgoing INVITE)
- Number of Incoming Answers (incoming 200 OKs)
- Number of Outgoing Answers (outgoing 200 OKs)
- Number of Abandoned Calls (incoming/outgoing CANCELs)
- Number of 3xx's received (redirections)
- Number of 4xx's received
- Number of 5xx's received
- Number of 6xx's received
- Number of 4xx's sent
- Number of 5xx's sent
- Number of 6xx's sent

The following counters are added at the end of the usSrxSipConfigStatisticsData object:

- 183 - Number of 183 messages (Session Progress) Sent and Received
- 1xx - Number of 1xx messages Sent and Received
- 2xx - Number of 2xx messages Sent and Received
- 3xx - Number of 3xx messages Sent and Received
- 4xx - Number of 4xx messages Sent and Received
- 5xx - Number of 5xx messages Sent and Received
- 6xx - Number of 6xx messages Sent and Received
- NoSupport - Number of unsupported messages received
- PRACK - Number of PRACK messages sent and received
- UPDATE - Number of Update messages sent and received
- 200 OK for PRACK - Number of 200 OK messages Sent and Received for PRACK Messages

- 200 OK for UPDATE - Number of 200 OK messages Sent and Received for UPDATE Messages

The following measurements as a Subset of Breakout Gateway Control Function are available per system:

- SIP Request Received from Unknown Host
- SIP Requests Sent to EndPoint - Failure
- Non-Invite and Non Ack Requests Received

The following measurements are available per system to be found in `hiqFeatLic.mib`:

- Assigned Dynamic Licenses
- Maximum usage of Dynamic Licenses
- Customer violation limit
- Customer violation counter

6.14.8.1 How to Access SIP Counter

Prerequisites

Adequate administrative permissions

Step by Step

1) Open main menu CLI.

2) Navigate to **Application-level management** > **Signaling Management** > **SIP Management** > **SIP Performance Management** > **Get Performance Counters**.

6.14.8.2 How to Display SIP Performance Counters

Prerequisites

Adequate administrative permissions

Step by Step

1) Open main menu CLI.

2) Navigate to **Application-level management** > **Signaling Management** > **SIP Management** > **SIP Performance Management**.

3) Enter `1` at the selection prompt.

Expert Mode Command Syntax: `sipConfiggetPerformanceCounters`

6.14.8.3 How to Display SIP EP (Endpoint) Statistics

Prerequisites

Adequate administrative permissions

Step by Step

1) Open main menu CLI.
2) Navigate to **Application-level management** > **Signaling Management** > **SIP Management** > **SIP Performance Management**.
3) Enter `1` at the selection prompt.

   Expert Mode Command Syntax: `sipConfiggetPerformanceCounters`

6.14.8.4 How to Monitor SIP Performance

Prerequisites

Adequate administrative permissions

Step by Step

1) Open main menu CLI.
2) Navigate to **Application-level management** > **Signaling Management** > **SIP Management**.
3) Enter `2` at the selection prompt.

The menu SIP Performance Management is displayed.

6.15 Remote Restart

The Remote Restart feature provides the remotely performed restart and recovery of a node with the capability to manage individual processes that run on the different nodes of the predefined clusters.

6.16 Smart Services Delivery Platform

The SSDP (Smart Services Delivery Platform) is a remote service of Unify and will complement the existing SIRA (Secured Infrastructure for Remote Access) Platform.

The SSDP offers a number of advantages for customers and service staff.

- Simple and fast installation with seamless integration in customer networks.
- Maximum security standard based on the usage of state-of-the-art encryption (AES, HTTPS and SSL-VPN) for all transferred data.
- Data transfer via broadband connection supports rapid processing of remote service activities and helps to minimize downtimes.
- Value-added services and further products to be supported will make the SSDP a significant element of the remote service platform in the future.
- In the OpenScape Voice (OSV) Solution a Service Plugin is installed on the server where the Common Management Platform is running. This Service Plugin connects to the central SSDP Enterprise Server. All other servers in the solution (if any) are managed remotely by the Enterprise Server via a connection in the customer LAN. The Enterprise Server retrieves information

about the other devices in the solution from the SNMP interface of the Common Management Platform.

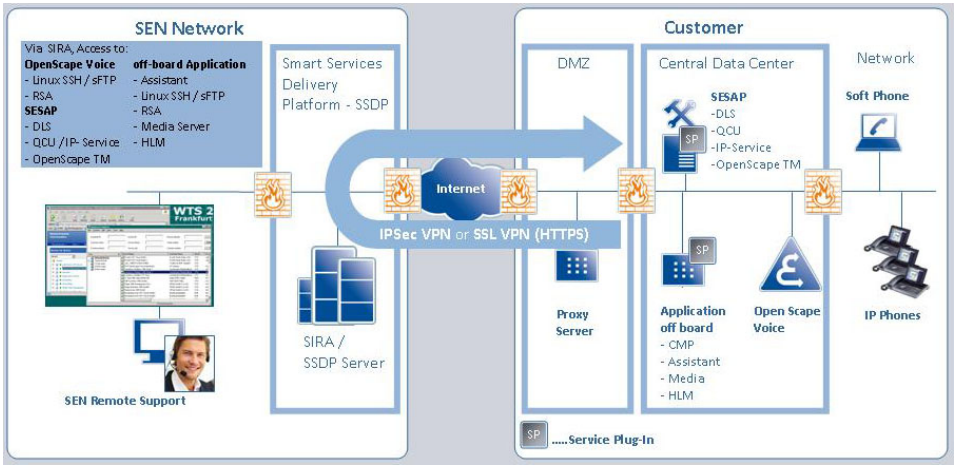

Figure 2: SSDP Architecture - Overview: Standard Duplex

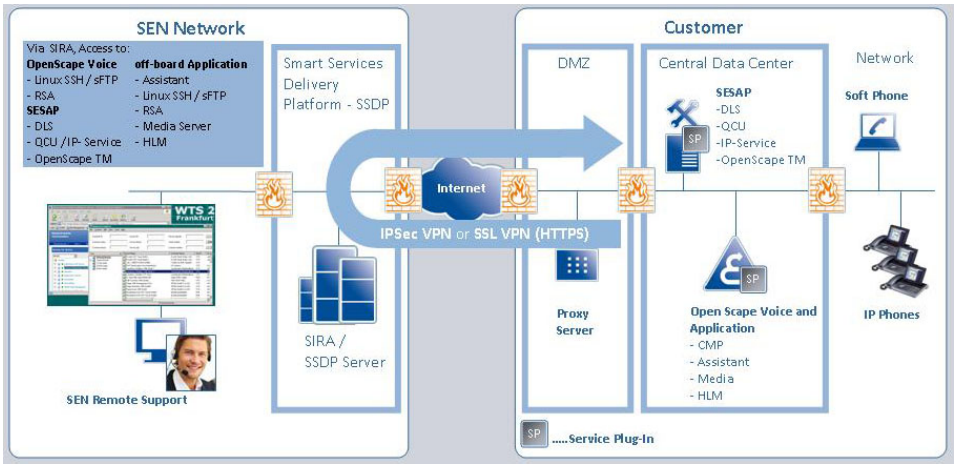

Figure 3: SSDP Architecture - Overview : Integrated Simplex

6.16.1 Smart Services Delivery Platform

SSDP Service Plugin is a product extension for additional services, such as remote access, software management and inventory, to be used by service technicians and partners. For this reason SSDP Service Plugin provides an interface for integration with the supported products.

A proxy server must be configured so you can have access out of the private network of the Customer to the internet.

The proxy server can either be configured in the relative area

Configuration > **CMP** > **General** > **Proxy Servers**

or within the configuration of the SSDP Enterprise Server.

Service Plugin shall always be installed along with CMP and will remain in a "Deactivated" state until the Administrator User explicitly activates it. In order to activate the plugin the User must specify a "Partner ID". After the plugin activation, the CMP Administrator shall be able to configure the Service Plugin

connection parameters (Identification, Proxy and Policy server) as well as modify the "Partner ID" if required.

The SSDP pop up window can be accessed when you navigate **Configuration** > **CMP** > **SSDP.**

Within the pop up window you have the following options:

1) You can see the Partner ID value of SSDP Service Plugin and its possible states:

- **Not Activated (red)**: The SSDP is installed but has not been activated. No SSDP funtionality is availiable

  Activated (green): The SSDP is installed and has been explicitly activated.
- **Not Running(red)**: The SSDP Service Plugin web service does not respond to requests.

  Running (green): The SSDP Service Plugin web service does respond to requests.
- **Not Connected(red)**: The SSDP Service Plugin cannot connect to the Enterprise Server.

  Connected (green): The SSDP Service Plugin can connect to the Enterprise Server.

2) You can **Download Log File** which contains troubleshooting information.

The Log file can be downloaded as long as the SSDP Service Plugin is activated

---

NOTICE:

Depending on the settings of your browser, either a dialog allowing you to select the download location is displayed or the file is directly downloaded in the browser's designated "Downloads" folder.

---

3) You can **Configure** the Partner ID value and activate or deactivate the SSDP Service Plugin

4) You can **Restart** the SDDP Service Plugin

5) You can **Configure** the following:

- Device Identification
- Proxy Server
- Policy Server
- SNMP Profiles

6.16.2 How to activate/deactivate SSDP and configure Partner ID

The partner ID is an attribute required by SSDP as soon as hosted SSDP support for service partners is provided. This means that the service partners get access to the SSDP infrastructure and use it to provide remote service for their customers. You must set the partner ID on a device before activating the SSDP Service Plugin so it can register itself with this ID at the Enterprise Server and will be assigned to the correct service partner.

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's permission level allows the configuration of SSDP.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Smart Services Delivery Platform**.

   The SSDP pop up window opens
3) Click on **Configure** button in Control section under Activation and Partner ID
4) **Set partner Id** of the Agent and click on **Change Partner ID** or if the Device is not activated click on **Activate Partner ID**

   The Partner ID value must satisfy the following restrictions:

   a) Maximum length 30 characters
   b) Allowed characters A-Z, a-z, 0-9, _ (underscore)
   c) Default Partner ID value is "Unify"
5) Click on **Deactivate** if you want to deactivate the device.

6.16.3 How to Configure SSDP Device Indentification

Device Identification is of the Agent Device is stored in the Enterprise Server. How to configure SSDP Device Information:

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's permission level allows the configuration of SSDP.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Smart Services Delivery Platform**.

   The SSDP pop up window opens
3) Click on **Configure** button in Configuration section under Device Identification

   The Device Identification page opens

   The first time the Device Identification page is accessed it has the default values in the relative fields.
4) Enter the **Name** (mandatory) of the Agent.

   Other fields in Indentification section have default values and are read only:

   a) **Model**: The Agent Device model

      Serial: The MAC address of the Agent Device

5) Click on **Save**.

   a) The Device Identification data is stored on the Enterprise Server and can be retrieved from there by the Device Agent

---

NOTICE:

If there is no connection established between Application Server and Enterprise Server no customer information data can be retrieved

---

6.16.4 How to Configure SSDP Enterprise Proxy Server

How to configure SSDP Enterprise Proxy Server.

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's permission level allows the creation of Proxy Server.
3) The Admin User's permission level allows the configuration of SSDP.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Smart Services Delivery Platform**.

   The SSDP pop up window opens
3) Click on **Configure** button in Configuration section under Proxy Server

   The Enterprise Proxy Servers page opens
4) In the navigation tree, click on **Smart Services Delivery Platform**

   You have the option to either **Enable the auto -configuration** or **Enable the HTTPS/SOCKS proxies**
5) **Enable auto -configuration** and enter in **URL** field the `*.pac` file you can find in your Automatic configuration address of your LAN settings in your browser (e.g IE: **Tools** > **Internet Options** > **Connections** > **LAN settings**)
6) Click on **Configure** to enter **User Name** (mandatory) and **Password** for the corresponding types of servers.

   You have determined how the Agent will communicate with an Enterprise server through a proxy server.
7) Click on **Save**.

   a) The Enterprise proxy server is configured successfully .
8) If you choose to Enable HTTP/SOCKS proxies tick the type of proxy you will enable.

9) Choose a Proxy Server from the list of proxies in the **Host** field or **Add** a new Proxy Server with the following attributes:

   - **Name (mandatory)**

     Name of the proxy serverUser ID of the user. :
   - **Host (mandatory)**

     Specify the IP address of your proxy server.
   - **Port (mandatory)**

     Specify the used port (e.g. port 80 for HTTP)
   - **Use authentication**

     If the proxy needs authentication, mark this checkbox and specify the appropriate User name and Password.

10) Click on **Save**.

    a) The proxy is saved successfully

11) Click on **Save**.

    a) The Enterprise proxy server is configured successfully .

6.16.5 How to configure SSDP Policy Server settings

The Policy Server is very important for security purposes.Policy Server provides a browser-based application that you can use to configure policies and permissions for devices.

Prerequisites

1) The Admin User has successfully logged-in the CMP.
2) The Admin User's permission level allows the configuration of SSDP.
3) A Policy Server is configured for the Agent Device

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Smart Services Delivery Platform**.

   The SSDP pop up window opens
3) Click on **Configure** button in Configuration section under Policy Server The policy servers window opens
4) If you want to use the Policy Server tick the **Enable connection** box
5) In the **Host** field enter the Policy Server IP and in the **Port** field the Policy Server Port.

   IMPORTANT:

   You must always make sure you enter a valid Policy Server IP

   ---

6) Tick the **Enable** box if you want to enable the SSL protocol for the communication between Agent and Policy Server, then select the SSL encryption level (**Strength**): 40, 128, or 168.

7) Choose the correct Proxy Server from the **Select** pull down menu for connecting to the Policy Server
8) Click on **Save**.

   SSDP plugin will restart and new settings will be active.

6.16.6 How to Add SNMP Profiles

CMP provides the ability to the User Administrator to configure profiles within SSDP plugin for discovering and collecting data from SNMP-enabled devices. How to Add an SNMP profile:

Prerequisites

1) The Admin User has successfully logged-in the CMP.
2) The Admin User's permission level allows the configuration of SSDP.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Smart Services Delivery Platform**.

   The SSDP pop up window opens
3) Click on **Configure** button in Configuration section under SNMP profiles

   A list of all added SNMP profiles appears
4) Click on **Add...** to configure a new SNMP profile

   Mandatory fields for adding a SNMP profile are **bold**.

   At least one Device must also be added for the profile to be successfully stored
5) In the **Profile** tab fill in the following fields:
   - **Name** (**mandatory**)
   - **Read Community**, default value is `public`
   - **Write Community**, default value is `admin`
   - **Version**, select the SNMP version you are using 1 or 2
   - **Port (mandatory)**, enter the port number for the Agent to use for SNMP broadcast and listening
   - **Timeout (mandatory)**, enter the number of seconds that the SNMP driver should wait for a response while discovering or collecting data from SNMP devices
   - **Retries**(mandatory), enter the number of times the SNMP driver should attempt to discover or collect data from an SNMP device
6) Click on the **Devices** tab
7) Click on **Add**
8) Define the IP address range by entering the **Start** IP adrress and the **Stop** IP address
9) Click **OK**
10) Choose the Device from the list

11) Click on **Save**.

SNMP profile is saved

6.17 TLS Communication with SOAP Server

6.17.1 How to create custom Certificates for TLS Connection with SOAP Server

How to create custom certificates used for the TLS connection of the OSV Assistant & SOAP Server:

Prerequisites

Adequate administrative permissions

root access to Application Server

In a Server where OSV has been installed, proceed with the following steps:

Step by Step

1) Log in to Application Server.

2) Create a key pair and provide a password to protect it.

You can create a key by typing :

openssl genrsa -out osvkeystore.key -des3 2048

NOTICE:

This command will generate an RSA private key which is 2048 bits long.

---

3) Obfuscate the password and store it in file.

4) Create a certificate signing request (CSR):

openssl req -new -days 3650 -key osvkeystore.key -out osvkeystore.csr

---

NOTICE:

This command will create a csr file which will be later used in order to be signed from a Certificate Authority.

---

5) Sign the CSR with the Certificate Authority (CA) of an OSV through the root.pem and create the certificate (cert):

openssl x509 -req -days 365 -in osvkeystore.csr -signkey osvkeystore.key -CA /usr/local/ssl/certs/root.pem -out osvkeystore.cert –CAcreateserial

---

NOTICE:

This command will sign the csr file using the x509 protocol with the Certificate Authority of the OSV which is the root.pem file existing in /usr/local/ssl/certs folder.

---

6) Store the signed certificate and the corresponding key in a PKCS#12 keystore protected with the obfuscated password.

   openssl pkcs12 -name osvkeystore -export -in osvkeystore.cert -inkey osvkeystore.key -out osvkeystore.p12

   NOTICE:

   This command will create the keystore in PKCS#12 format.The output file will be a .p12 file.

7) Store the CA in a PKCS#12 trustore protected with the obfuscated password.

   Use the following command to create the trustore:

   NOTICE:

   Use keytool to create the trustore from the public key on root.pem of an osv.

   /opt/ibm/java-x86_64-60/jre/bin/keytool -import -alias osvtrustore -file /usr/local/ssl/certs/root.pem -keystore osvtrustore.jks

   NOTICE:

   osvkeystore.p12 and osvtrustore.jks should be transfered in the server that hosts OSV Assistant in the $SYMPHONIA_HOME/common/conf/axis_soap_tls path. The files should have 640 permissions (chmod 640 *) & should be root owned although belonging to sym group (chown root:sym *).

   NOTICE:

   A properties file exists in $SYMPHONIA_HOME/assistant_ssl named symphonia-client-config.properties. In this file give the password of the keystore and trustore that you have created previously as well as the path where keystore and trustore exist.

8) Restart the Framework Container and choose to add a switch checking the TLS Connection.

Index

H

I

J

L

N

O

P

R

S

T

U