A MITEL
PRODUCT
GUIDE

Mitel OpenScape Fault Management

Mitel OpenScape Fault Management V12 Performance Management

User Guide
10/2025

A31003-F30C0-U117-01-7619

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 Preface 5
1.1 Purpose 5
1.2 Audience 5
1.3 Terminology 5
1.4 Organization of this Guide 6
1.5 Conventions Used within this Guide 6

2 Introduction 7
2.1 Performance Management Plugin 7
2.2 Technical Architecture 8

3 Collecting the Data 9
3.1 Installation and Configuration 9
3.1.1 Database 9
3.1.1.1 Using MySQL 10
3.1.2 Agent 11
3.2 Calculation of Performance Values 12
3.2.1 R-Value 12
3.2.2 MOS 12
3.2.3 Jitter & Maximum Inter Arrival Jitter 13
3.2.4 Packet Loss 13
3.2.5 Consecutive Packet Loss 13
3.2.6 Average Round Trip Delay 13
3.2.7 Lost Packets Percent 13
3.3 Performance Management Monitors 13
3.3.1 QDC Monitor 13
3.3.1.1 Trap Monitor 14
3.3.1.2 QDC Export Monitor 14
3.3.2 Call Monitor 14
3.3.3 SLA Call Monitor 15
3.3.4 Topology-based Call Monitor 16
3.4 Trace Manager Integration 17

4 Activating the User Interface 19
4.1 Installation and Configuration 19
4.2 Starting the Web Client 19
4.2.1 CMP 19
4.2.2 OpenScape FM Client 19
4.2.3 Web Client 20
4.2.4 OpenScape FM Landing Page 20
4.3 Licensing 20

5 Configuration of the Monitoring 21
5.1 Displaying Agents 21
5.2 Domains 21
5.3 Groups 22
5.4 Monitored Endpoints 22
5.5 Defining Monitors 23
5.5.1 Managing Monitors 23

5.5.2 Defining Thresholds 25
5.5.3 Defining SLAs 26
5.6 Web Client Configuration 27

6 Displaying Performance Management Results 29
6.1 Overviews 29
6.2 Call Dashboard 30
6.3 Switch/Router Dashboard 31
6.4 Reports 33
6.4.1 Call Report 33
6.4.2 Call Search 34
6.4.3 Cumulative Call Report 34
6.4.4 Cumulative Consecutive Packets Report 35
6.4.5 Consecutive Packets Over Time Report 35
6.4.6 Call Monitor Report 35
6.4.7 SLA Monitor Report 36
6.4.8 Topology Monitor Report 36
6.5 Report Scheduling 36
6.5.1 Templates 37
6.5.2 Execution Plans 37
6.5.3 Report Results 38

7 IP Manager Integration 39
7.1 Dashboard 39
7.2 Networks 39
7.3 Nodes 41

8 Events 43
8.1 Dashboard 43
8.2 Events 43

9 External Software Integration 45
9.1 Trace Manager 45
9.1.1 Trace Manager Preparation 45
9.1.2 Trace Manager Configuration 45
9.1.3 Trace Manager Trouble Shooting 47
9.2 OpenScape DLS 47
9.2.1 DLS Preparation 48
9.2.2 DLS Configuration 48
9.2.3 DLS Endpoints 49
9.2.4 DLS QoS Templates 50
9.3 CSV Export 50

Index 53

1 Preface

This chapter discusses the following aspects:

- Purpose and Audience of this guide
- The terminology used in this guide
- Organization of this guide
- Conventions used in this guide

1.1 Purpose

This user guide describes the Performance Management for OpenScape FM.

1.2 Audience

This guide is written for end users, who want to use the Performance Management for the OpenScape FM. The reader should be familiar with the usage of the OpenScape FM. A detailed description of this program can be found in the *OpenScape FM Desktop User Guide*.

1.3 Terminology

- **OpenScape FM** or **OSFM** stands for OpenScape Fault Management.
- **Server** means the OpenScape FM server. The server on which the OpenScape FM has been installed.
- **Client** means the OpenScape FM client. Generally this is a web browser in which the OpenScape FM has been started by entering an URL.
- **Web Client** stands for the user interface of the Performance Management (see *Chapter 4* to *Chapter 6*).
- **Performance Management** is the short version for OpenScape FM Performance Management.
- **Performance Management Server** stands for the OpenScape FM Server on which the Performance Management Plugin is running.
- **Performance Management Agent** stands for a System Management Agent on which the Performance Management characteristics have been installed.
- **CMP** is the abbreviation for the Unify Common Management Platform.
- **QoS Data**, **QDC Trap**: The QoS (Quality of Service) Data is sent as an SNMP Trap from an endpoint to a Performance Management agent. The trap contains the QoS values for a single call calculated by the sending endpoint. It is send as an QDC trap.

- **Port** means a physical interface of an Ethernet switch to connect a network component.

1.4 Organization of this Guide

This guide is organized as follows:

- *Chapter 2, "Introduction"* contains an introduction about the functions of the Performance Management Plugin.
- *Chapter 3, "Collecting the Data"* contains information about the agents that collect and calculate the Performance Management data.
- *Chapter 4, "Activating the User Interface"* explains the configuration of the Performance Management Web Browser Client.
- *Chapter 5, "Configuration of the Monitoring"* explains how the Performance Management can be configured.
- *Chapter 6, "Displaying Performance Management Results"* describes how the results of the Performance Management monitoring can be displayed.
- *Chapter 7, "IP Manager Integration"* describes how OpenScape FM IP Networks and IP Nodes can be displayed and handled.
- *Chapter 8, "Events"* describes how OpenScape FM Events can be displayed and handled.
- *Chapter 9, "External Software Integration"* describes the integration of external software into the Performance Management Plugin.

1.5 Conventions Used within this Guide

The following font conventions are used within this guide:

Bold Font: Indicates that a word is a new word or an important term.

Example: **Endpoint**.

Bold Computer Font: Indicates data that has to be entered by the user.

Example: **`Java`**.

Computer Font: Indicates computer output (including UNIX prompts) or explicit directory or file names.

Example: `Prompt%.`

Italics: Indicates a reference to another guide or to another chapter within this guide.

Example: *Documentation for the OpenScape FM.*

Italics are also used for emphasis.

Example: *All* users are effected.

2 Introduction

Traditional circuit-switched telecommunication solutions are more and more replaced by IP phones/Voice over IP (VoIP) solutions. VoIP uses another technology which is based on the use of the IP protocol.

Using VoIP allows the handling of data transfer and telecommunication by the same network. Data and telecommunications can now use the same connections. The resulting cost reduction is the prime reason for the implementation of VoIP.

While the same infrastructure is used for data transfer and telecommunications, the technical requirements to generate customer acceptance differ fundamentally.

IP focusses on an optimized transmission of data packages, which is not sufficient for phone calls. Call data has to be transmitted to the receiver in a short time interval, in the given order and with a small deviation in the delivery time.

By using a microphone, the spoken words are converted into electric signals. These signals are digitised and coded based on the selected transmission protocol. If the transmission protocol provides a compression, the speech data will be send to the target system in smaller packages.

The major problems within the IP telephony that trouble the user are: fluctuations in the package transit times, long transit times or losses of packages. The bandwidth needed for phone calls over IP is about 120kbit/s.

The following attributes have a big impact on the quality of IP based phone calls perceived by the users.

- Jitter / fluctuation of the latency
- Average latency
- Package losses
- Transmission bandwidth

It is useful to monitor the quality attributes continuously. This allows the detection of quality problems a soon as possible. Phones from Unify are able to monitor the attributes by themselves. They can be configured to send QDC-SNMP traps with the collected data to a collection centre when a call is finished. The Performance Manager and its agents is such a collection centre.

2.1 Performance Management Plugin

The Performance Management plugin is an extension module for the OpenScape FM. Its purpose is the collection and evaluation of data that is relevant for VoIP performance and quality, also known as Quality of Service (QoS) data. It supports the online evaluation of performance data and generates alarms/events on degradation of the VoIP performance in the monitored network. In addition it provides reporting functions for various performance and QoS data.

The Performance Management helps the network administrator to track down performance problems by correlating QoS data with the network topology. It monitors router interfaces in the network and provides information about the quality of calls which are routed through a particular interface.

2.2 Technical Architecture

The Performance Management uses a two-tier architecture which consists of the plugin representing the OpenScape Performance Management Server and monitoring profiles bundled with a Performance Management Agent.

The Performance Management Agent receives the QoS data from the various monitored VoIP endpoints (VoIP phones), computes additional values (like e.g. the R-Factor) from this data and applies thresholds for online monitoring.

The Performance Management Server receives the raw and computed data from the agent, stores it in an external relational database and provides access to it for the user. It creates reports, displays monitored parameters and generates events when thresholds are exceeded. In addition, it has access to the layer-2/3 information of the network and can determine which network components are involved in a particular call. This allows for the mapping of QoS values to IP nodes and interfaces.

3 Collecting the Data

The Performance Management Agent collects the QDC traps from the various endpoints. Monitors are used to calculate additional management data from the values given in the traps. The trap data and calculated data is collected in the OpenScape FM database.

The values, provided by the traps or calculated by the monitors, are described in *Section 3.2, "Calculation of Performance Values"*.

The different monitors that calculate and monitor the data are described in *Section 3.3, "Performance Management Monitors"*.

Chapter 5 explains how the monitors can be configured and how new monitors can be defined.

One Performance Management Agent is always installed on the same host as the OpenScape FM Server. To e.g. optimize the load distribution in larger networks, additional stand alone agents can be installed (see *Section 3.1, "Installation and Configuration"*).

3.1 Installation and Configuration

The following sections describe the selection of the Performance Management Database (see *Section 3.1.1, "Database"*) and the installation/configuration of the Performance Management Agents (see *Section 3.1.2, "Agent"*).

3.1.1 Database

To use the Performance Management an external relational database is needed. This database is not a part of the OpenScape FM installation. It has to be installed and configured separately (currently supported are Oracle, PostgreSQL (Postgres) and MySQL).

Due to licensing laws, the needed JDBC drivers cannot be delivered as a part of the Performance Management installation media. The drivers have to be obtained and installed individually. For example, if MySQL is used, the steps listed in *Section 3.1.1.1* should be considered.

To setup the drivers, only two steps are necessary:

- The driver has to be copied to the directory
  `<InstallationDirectory>/server/lib/user`
- The Startup Service has to be restarted.

The database connection can be configured within the OpenScape FM.

Within the OpenScape FM, the main menu entry **Add-Ons=>Performance Management=>Select or Create Database Connection...** has to be used. In the selection window an already configured database connection can be selected within the pull down menu **Database Connection**.

When a new database connection should be configured, the entry `<New Connection>` can be selected in the same menu. A window will open in which the driver for the database can be chosen. The pull down menu **Driver** lists all database JDBC drivers which were found in the library path of the OpenScape FM and that are supported by the Performance Management.

When a driver is selected, the following page allows the configuration of the database connection values like **Database**, **User** and **Password**. The needed parameters may vary, depending on the selected driver.

To limit the size of the database, the Performance Management data will be deleted automatically when a defined time interval has passed. The default for this is 30 days. The **Storage Duration** can be customized on the page **JDBC** on the main page **Configuration=>PM** within the Web Client.

3.1.1.1 Using MySQL

When MySQL is used for OpenScape FM, the following steps have to be considered:

1. **Database Driver Installation** (this part can be skipped if **MySQL 5.5** is used)

   The database driver (JDBC driver from MariaDB) which is included in the OpenScape FM installation is only supported for MySQL 5.5. If a different MySQL version is used, the corresponding MySQL driver has to be installed manually. This can be done as follows:

   a) Open the download page `http://dev.mysql.com/downloads`

   b) Select the link `MySQL Connectors`

   c) Select the link `Connector/J`

   d) At the combo box **Select Platform**, select `Platform Independent`

   e) Download the archive (available as `zip` or `tar`)

   f) Extract the archive file and locate the driver. Its name is something like `mysql-connector-java-X.X.XX-bin.jar` where `X.X.XX` represents the current version number

   g) Stop the OpenScape FM server process

   h) Copy the driver file `mysql-connector-java-X.X.XX-bin.jar` into the directory `<OPENSCAPE FM INSTALL>/server/lib/external`

   i) **Delete** the file `<OPENSCAPE FM INSTALL>/server/lib/external/mariadb-java-client.jar`. **This step is important**, otherwise the database connection may not work correctly.

   j) Start the OpenScape FM server process

2. **Preparation of the Database**

   The Performance Management Plugin needs a pre-defined database. To create a database in MySQL, perform the following steps:

a) Connect to the local MySQL database server by invoking the `mysql` command line tool. If the tool is not found, maybe the `mysql-client` package is not installed. The client prompts for a password for "`root`" if invoked as stated below. This is **not** the Unix-root user but the MySQL database administrator. The password has to be known. It is usually defined during the MySQL server installation process.

   Command: `mysql -u root -p`

b) Create a database with a name of your choice. The same name has to be configured in the OpenScape FM user interface using the main menu entry **Add-Ons=>Performance Management=>Select or Create Database Connection**.

   Command: `create database pm_database;`

c) Exit the command line client

   Command: `exit;`

3.1.2 Agent

During the installation of the OpenScape FM, the Performance Management plugin and the local Performance Management Agent will automatically be installed on the same host as the OpenScape FM.

Note:
If only the Performance Management should be used, the general System Management can be deactivated (see *System Management User Guide*).

To keep the sending of QDC traps restricted to local networks, further Performance Management Agents can be installed as stand alone agents on any number of systems. These distributed agents monitor the endpoints from which they received at least one trap. They perform the calculations locally.

The endpoints have to be configured to send their QDC traps to the system on which their dedicated agent is running.

The OpenScape FM Server host and the Performance Management Agent hosts have to support the same IP protocol(s). If the OpenScape FM Server host supports IPv4 the Performance Management Agent hosts have to support IPv4. If the OpenScape Server host supports IPv6 the Performance Management Agent hosts have to support IPv6.

In contrast to a Performance Management Agent residing on the OpenScape FM host system, topology based data cannot be monitored by distributed agents.

Only the data that matches the monitoring criteria will be forwarded to the central Performance Management database by using an RMI connection.

Distributed agents can be installed by using the installation file `setup_agent_osfm.exe` which will be provided on the installation media. The installation file installs the general OpenScape System Management Agent (see separate User Guide). During the installation **Performance Management** has to be selected. This will lead to the installation of the special set of Performance Management monitors that define the Performance Management Agent.

The distributed agents will be detected by the OpenScape FM when a discovery for the agent‘s host is performed.

The OpenScape FM that performed the discovery registers itself on the distributed agents. The data that is received/calculated by the agents is exported into the Performance Management database.

Newly installed agents will only receive and calculate the incoming QDC traps. Additional monitors and filters can be created by using the Performance Management Web Client (see *Chapter 5, "Configuration of the Monitoring"*).

3.2 Calculation of Performance Values

The following values are provided by the QDC traps from the monitored endpoints or are calculated by the Performance Management Monitors.

3.2.1 R-Value

In the Performance Management only the impacts on transmission quality resulting from signal transmission can be calculated. The other factors like quality of microphone and speaker, background noise level, etc. cannot be taken into account because they are not known. So only the theoretical R-Value can be computed which is calculated based on:

- codec (if available)
- signal delay
- packet loss

Only the parameters provided by the QDC traps can be used to calculate an R-Value. If the R-Value could not be calculated because some data is missing (e.g. the endpoint has not sent it), the user will be informed about this by an event.

3.2.2 MOS

The Mean Opinion Score (MOS) is the arithmetic average of single valuations and can have values in the interval from 1 (worst value) up to 5 (best value). The MOS is the result of a defined test series, where e.g. a group of persons assess the audio or video quality.

From the R-Value the MOS can be derived using the following mapping.

R-Value	0-50	50-60	60-70	70-80	80-90	90-100
MOS	1.0-2.6	2.6-3.1	3.1-3.6	3.6-4.0	4.0-4.3	4.3-5.0

Table 1 MOS from R-Value

Only the parameters provided by the QDC traps can be used to calculate a MOS value. If, for example, the used codec is not provided, it cannot be taken into account for the calculation.

3.2.3 Jitter & Maximum Inter Arrival Jitter

Jitter describes the variation in the delay of data packets. This is a raw value provided by the communication endpoint.

The Maximum Inter Arrival Jitter is the maximum of the standard RTCP ‚inter arrival jitter' that is sent in the RTCP reports. It is also provided by the communication endpoint.

3.2.4 Packet Loss

The number of dropped packets. This is a raw value provided by the communication endpoint.

3.2.5 Consecutive Packet Loss

The number of packets consecutively lost. This is a raw value provided by the communication endpoint.

3.2.6 Average Round Trip Delay

The average network delay obtained by the RTCP packets from the local station to the remote station plus the same value in the opposite direction. This is a raw value provided by the communication endpoint.

3.2.7 Lost Packets Percent

The percentage of the lost packets in relation to the total number of packets (the sum of good packets, lost packets and discarded packets).

3.3 Performance Management Monitors

The following describes the specific monitor types that are included in the Performance Management Agent. The monitors are used for data acquisition, computation of R-Value and MOS, counting ‚good' and ‚bad' calls and applying thresholds.

3.3.1 QDC Monitor

This monitor consists of two separate monitors.

3.3.1.1 Trap Monitor

The Trap Monitor is responsible for receiving and processing the data from the QDC traps. It calculates R-Value and MOS from the QoS data.

The monitor stores the computed QoS and raw data in the internal database of the Performance Management Agent.

The monitor has the following parameters:

- QoS data
- Number of QoS data records received

For each QoS data a history sample is stored in the QoS parameter of this monitor.

3.3.1.2 QDC Export Monitor

The QDC Export Monitor stores the raw QoS data as well as computed data into the selected database. Examples for raw data are jitter, packet loss and delay. Examples for computed data are R-Value and MOS.

3.3.2 Call Monitor

The Call Monitor evaluates the QoS data for a single call.

It allows the definition of thresholds for the jitter, delay, packet loss, MOS and R-value. These thresholds are applied to the QoS data for calls to or from IP endpoints belonging to a particular endpoint domain and group. The domains and groups are defined by specific filters (MAC addresses, IP address ranges, subscriber numbers, see *Section 5.2* and *Section 5.3*).

The monitor registers itself for the reception of QoS data provided by the Performance Value Calculator Monitor. It has the following structure:

- Call Monitor
  - Parameter Delay
  - Parameter Jitter
  - Parameter Packet Loss
  - Parameter Consecutive Packet Loss
  - Parameter R-Value
  - Parameter MOS

The Call Monitor calculates the average, median, minimum and maximum values for each parameter. The set of calls which is taken into account during the calculation, can be defined in two ways:

Either a number of consecutive calls can be used or a time interval can be defined (see *Section 5.5.1, “Managing Monitors”*).

Thresholds can be defined individually for each parameter (see *Section 5.5.2, “Defining Thresholds”*).

The calculations of average, median, minimum and maximum values use history data. This data is reset when the monitor is restarted. This happens when an agent restart is performed or when the configuration of the monitor is changed.

To reduce the load to the database, the internal aggregated monitor values will only be calculated and stored at a maximum of once every 15 seconds.

Within the Performance Management Web Client, the defined Call Monitors are displayed on the page **Call Monitoring** of the main page **Monitoring**. This page can be used to configure or modify monitors. More about this can be found in *Section 5.3, “Groups”*.

3.3.3 SLA Call Monitor

The SLA Call Monitor is responsible for SLA monitoring. In this context, the term SLA has the following meaning:

An SLA defines that a specified percentage of calls within an observation period must fulfill certain quality criteria. If a call does not fulfill the defined criteria, it is counted as a ‚bad‘ call, otherwise it is counted as a ‚good‘ call. The SLA is fulfilled, if ‚X‘ percent of all calls within the observation period are ‚good‘ calls.

The quality criteria to decide if a call is good or bad are the following:

- Maximum Jitter
- Maximum Delay
- Maximum Packet Loss
- Maximum Consecutive Packet Loss
- Minimum R-Value
- Minimum MOS

If at least one of the specified thresholds is exceeded, the call is counted as a ‚bad‘ call. The thresholds themselves are monitored by the Call Monitors described in *Section 3.3.2, “Call Monitor”*. Each Call Monitor keeps track about the good and the bad calls. These counters are used by the SLA Call Monitor to check if an SLA has been violated.

To check this, the SLA Call Monitor reads the counters of the Call Monitors in a configured time interval, e.g. 1 hour. The percentage value of the accumulated good calls from the total number of calls within the time interval defines the SLA value that is marked.

It is possible to define thresholds for this computed value. If the value falls below the threshold (e.g. less than 90% of the calls are good), an alarm event is generated. Reporting functions for the SLAs are also available (see *Section 6.4, “Reports”*).

Thresholds can be defined individually for each parameter (see *Section 5.5.2, “Defining Thresholds”*).

Within the Performance Management Web Client, the defined SLA Call Monitors are displayed on the page **SLA Monitoring** of the main page **Monitoring**. This page can be used to configure or modify monitors. More about this can be found in *Section 5.5.1, "Managing Monitors"*.

3.3.4 Topology-based Call Monitor

Important Note:
Topology-based Call Monitors cannot be used with distributed agents.

The Topology-based Call Monitor correlates the knowledge about the network topology with the received QoS data. It is used to monitor a particular device (e.g. a router) with regard to QoS data. To achieve this, the Topology-based Call Monitor collects data about all calls which are routed over specific interfaces of the device. By this it can provide data about jitter, packet loss, delay etc. for a particular interface and makes it easier to find out bottle necks or problems in the network (e.g. a router which is frequently routing calls with high packet loss).

The calculation which calls are routed over a specific interface or device is performed based on the current knowledge of the network within the OpenScape Fault Management. The underlying information used for this purpose are the routing tables and Layer 2 specific information which are retrieved via SNMP.

The routing can only be processed when the IP address of the target can be mapped to the MAC of the receiving endpoint. This information can be gained by evaluating ARP caches, MIB II interface entries or QoS data send by the receiver. If the mapping is not known when the QoS data is received, it will not be used for the topological evaluation.

The monitoring collects QoS data for all calls where the defined routers are a part of the communication path. Information about the collected data is available for each interface and the router itself.

Topology-based Call Monitors have the same structure as the call monitor described in *Section 3.3.2*, but in contrast to this, they are applied to IP nodes in the network topology and not to endpoint groups.

The following data is collected or calculated by the Topology-based Call Monitors:

- Parameter: Delay
- Parameter: Jitter
- Parameter: Packet Loss
- Parameter: Consecutive Packet Loss
- Parameter: R-Value
- Parameter: MOS

The Topology-based Call Monitor calculates the average, median, minimum and maximum of the performance values for calls going through a particular interface or router. It is possible to define a number of calls or a time interval that should be used to calculate the performance values (jitter, delay, packet loss, MOS value, R-Value).

Thresholds can be defined individually for each parameter (see *Section 5.5.2, "Defining Thresholds"*).

The calculations of average, median, minimum and maximum values use history data. This data is reset when the monitor is restarted. This happens when an agent restart is performed or when the configuration of the monitor is changed.

To reduce the load to the database, the internal aggregated monitor values will only be calculated and stored at a maximum of once every 15 seconds.

Within the Performance Management Web Client, the defined Topology-based Call Monitors are displayed on the page **Topology-based Monitoring** of the main page **Monitoring**. This page can be used to configure or modify monitors. More about this can be found in *Section 5.5, “Defining Monitors”*.

3.4 Trace Manager Integration

The Performance Management usually receives the endpoint information through QDC/QoS traps sent by the phones.

For OpenScape Voice systems that do not send QDC/QoS traps and that are monitored by a Trace Manager, the Performance Management provides an alternative. The Performance Management can be configured to collect the data for the respective endpoints directly from the Trace Manager itself.

To use the Trace Manager data within the OpenScape Fault Management and Performance Management, the connection to the Trace Manager has to be configured. *Section 9.1.2, “Trace Manager Configuration”* describes the necessary steps to connect the Performance Management to a Trace Manager.

The data collected from the Trace Manager is displayed in the same fashion as the data collected through traps. Endpoints detected by either method are shown in the same lists.

4 Activating the User Interface

The Web Client provides the major part of the Performance Management‘s user interface. From here the agents can be configured, search criteria and SLAs can be defined, and reports can be generated.

This chapter handles the installation and configuration of the OpenScape Performance Management Web Client.

The following chapters describe the user interface of the Performance Management. *Chapter 5, “Configuration of the Monitoring”* explains how monitored objects can be selected, how the data collection can be configured and how SLAs can be managed. The following *Chapter 6, “Displaying Performance Management Results”* shows how the results of the monitoring can be reported.

4.1 Installation and Configuration

The installation and configuration of the needed Apache Tomcat Server and the Web Client installation will automatically be performed during the installation of the OpenScape FM Server.

4.2 Starting the Web Client

There are four methods to start the Web Cient:

4.2.1 CMP

The Performance Management Web Client can be started by pressing the button **Performance Management** within the Unify Common Management Platform (CMP). The login for the CMP will be used to connect to the Performance Management (auto login).

4.2.2 OpenScape FM Client

The client can also be started from within an OpenScape FM Client by selecting the main menu entry **Add-Ons=>Performance Management=>Open PM Client** (auto login).

Note:
If this action generates an error message about "DataTypes", the browser cache should be cleared, the Performance Management tab should be closed and the entry should be invoked again.

The Performance Management Server that should be used can also be selected from within the OpenScape FM by using the main menu entry **Add-Ons=>Performance Management=>Configure Web Server**.

This opens a window in which the host and port can be selected and whether HTTPS should be used to connect.

4.2.3 Web Client

The Web Client can be started from a web browser by entering the URL ,`https://<server>:3080/PMWebGui`. In this connection string `<server>` stands for the hostname or IP address of the OpenScape FM Server on which the Performance Management plugin is running. `3080` is the default connection port. It has to be substituted respectively if another port has been configured.

This method opens the login page of the Performance Management web client.

4.2.4 OpenScape FM Landing Page

The Web Client can be started by entering the URL for the OpenScape FM Landing Page `https://<server>:3043` and selecting the button **Performance Management** on this page. Again `<server>` stands for the hostname or IP address of the OpenScape FM Server on which the Performance Management plugin is running.

4.3 Licensing

The Performance Management Plugin uses the general licensing mechanism of the OpenScape FM. The available licensing methods are explained in the *OpenScape FM Desktop User Guide*.

If no valid Performance Management License is available on the OpenScape FM Server, connection attempts of the Web Client will be refused and an appropriate error message will be displayed.

If insufficient endpoints are licensed, no further endpoints will be displayed.

5 Configuration of the Monitoring

This chapter handles the configuration of the OpenScape Performance Management environment within the Performance Management Web Client.

Mostly the Performance Management Web Client displays lists of objects.

The user interface consists of a number of **main pages** (like e.g. Reporting or Monitoring) that are selected by clicking the respective button on the top of the window. Each of the main pages consists of a number of **pages**, that can be selected by clicking the respective entry on the left of the main page.

Generally within these lists entries can be deleted, reconfigured or newly created by using the buttons **Delete...**, **Modify...** or **Add...** in the upper right corner of the client table. To delete or reconfigure entries, the respective entry has to be marked in the respective checkbox.

Detailed information about list entries is often displayed in a separate window that is opened when an individual entry is clicked.

On most lists the upper part of the page consists of a search area. By using this area, the list can be reduced to display only those entries that match the search criteria. The list will consist of all entries that contain the entered search string as a substring.

5.1 Displaying Agents

Performance Management Agents (see *Chapter 3*) are responsible for the collection of the QoS data send by the monitored endpoints. They are discovered automatically by the OpenScape FM.

The list of the Performance Management Agents known by the OpenScape FM is displayed on the page **Agents** within the main page **PM=>Summary**.

Within this list each line represents one agent. The columns display the name of the agent (Column: **Label**), its location (Column: **Hostname**) and its current status (Column: **Status**).

Among other data, the detailed information shows the field **Agent UUID** which contains the ID that is used for the agent within the OpenScape FM. The lower part of the information window lists the monitors that are running on the agent and their current status.

5.2 Domains

Domains are used to restrict and order the data received by the Performance Management Agents.

Sets of endpoints that have similar characteristics (e.g. same SLA, same assigned technician, same technology, same location) can be assigned to one Domain or Domain/Group combination (see *Section 5.3*). A special set of rules (e.g. monitored parameters, thresholds, SLAs) can then be configured for the set.

Every Domain belongs to exactly one Performance Management Agent, but an agent can have any number of Domains. At least one Domain must exist for an agent. Therefor the last Domain of an agent cannot be deleted.

For each agent that is discovered by the OpenScape FM one default Domain is automatically created. This domain is labeled with the name of the host on which the agent is running. By default it accepts data from all QDC traps that are send to the agent.

The known Domains are displayed and configured on the page **Domains** within the main page **PM=>Endpoints**.

Each Domain has an identifying name (Column: **Label**), a **Description** and one **Agent** to which it belongs.

In addition filter criteria can be defined that restricts the QDC traps handled by the Domain to only those that match the criteria.

The filters are assigned within the panel **Pattern** within the detailed information window of a selected Domain.

The button **Add** and the button **X** can be used to add or remove individual filters.

Filters can be applied to the **IP_ADDRESS**, **MAC_ADDRESS** or **SUBSCRIBER_NUMBER** of the endpoint that sends a QDC trap. The filter lines are connected with the OR-Operator, which means that the filter matches when one of the assigned criteria matches.

The search is always a partial string search. For example, the string '`139.2.51.125`' applies to the search string ‘`139.2.`'.

The filters can be used to e.g. create separate Domains for individual groups of endpoints.

Most lists displayed in the Performance Management Web Client only display entries that belong to one Domain. The Domain that is currently shown can be selected with the pull down menu **Domain** at the top of the page.

5.3 Groups

Groups are used to restrict and order the data even more detailed as with the Domains.

Each Group is assigned to exactly one Domain but any number of Groups can be defined for each Domain.

The known Groups for the selected Domain are displayed and configured on the page **Groups** within the main page **PM=>Endpoints**.

The configuration is identical to the configuration of Domains. The same filter criteria can be assigned, and the criteria are connected with the OR operator.

If a Group is assigned to a Domain, the filter criteria of the Group AND the filter criteria of the Domain have to match. If e.g. a Domain filters for ‚A or B‘ and a Group filters for ‚C or D‘, the combination will filter for ‚(A or B) and (C or D)‘ where A, B, C and D stand for the selected filter criteria.

Different Groups can be used to e.g. create virtual sub networks of endpoints within a single Domain.

5.4 Monitored Endpoints

Endpoints are the objects that are monitored by the OpenScape Performance Management. Generally these are VoIP phones.

Endpoints are not added manually.

Endpoints have to be configured to send their QDC traps to a Performance Management Agent. When such a trap is received, the Performance Management will check whether the endpoint is already known by the system. If not, a respective endpoint will be created and added to the OpenScape FM database as an endpoint of the receiving agent.

By default, the Performance Management Agents listen for QDC traps on the ports 162 and 12010. The ports can be reconfigured with the argument `port` in the file `QdcMonitor.xml` in the directory `<agent_install_dir>\ssma\conf\PerformanceManagement`.

The list of known endpoints for a selected Domain is displayed on the page **Endpoints** of the main page **PM=>Endpoints**.

Endpoints can be deleted from the database as usual by checking the respective table entry and pressing the button **Delete** on the upper right corner. This will remove the collected QoS data for the endpoint from the database.

A deleted endpoint will be added again, if a new QDC trap is received from the endpoint.

To prevent the addition of unwanted endpoints, respective filters have to be created for the Domain (see *Section 5.2*) and/or Group (see *Section 5.3*).

By pressing the button **CSV**, the displayed Endpoint list can be exported into a file as a Comma-Separated Values list (see *Section 9.3*).

For Endpoints that are also shown within a DLS Endpoints list (see *Section 9.2.3*), their DLS configuration can be started from this page by pressing the button **Data Collection**.

5.5 Defining Monitors

The lists of the defined **Call Monitors** (see *Section 3.3.2*), **SLA Call Monitors** (see *Section 3.3.3*) and **Topology-based Call Monitors** (see *Section 3.3.4*) can be found respectively on the pages **Call Monitoring**, **SLA Call Monitoring** and **Topology-based Monitoring** of the main page **PM=>Monitoring**.

The handling of these three monitor types is very similar as far as their configuration is concerned.

Each list contains all monitors of the respective type that have been defined for the selected domain (see *Section 5.2*). Each line within the table represents one monitor and displays the **Label**, the assigned **Agent** and **Endpoint Group** (see *Section 5.3*) and the current **Status** of the monitor.

5.5.1 Managing Monitors

New monitors of the currently displayed type can be created by pressing the button **Add...** in the upper right of the page.

Important Note:
Topology-based Call Monitors (see *Section 3.3.4*) cannot be created for distributed agents.

Already existing monitors can be modified or deleted by checking the check box of the respective monitor and pressing the button **Modify...** or **Delete...** in the upper right of the page.

Monitors can be duplicated to allow the easy creation of multiple, similar monitors. If the button „**Duplicate..**“ is clicked, a dialog comes up where the configuration of the duplicated monitor can be edited before it is saved. It is a good practice to configure at least a new, meaningful name for the new monitor. After clicking the „Save“ button, a copy of the previously selected monitor is created.

The button **Report...** can be used to create a report for a selected monitor. The search criteria and report parameters that can be selected are the same as for general reports of the respective monitor type (see *Section 6.4*) but the results are also restricted to the data of the selected monitor.

The two functions *Add* and *Modify* open a similar configuration window which contains a number of common fields for all three monitor types:

- **Label**: This is the identifying name of the monitor and has to be unique.
- **Domain**: The domain which holds the objects which should be watched by the monitor. This field cannot be modified.
- **PM Agent**: The agent on which the monitor should be performed.
- **Trap Target**: The trap target configuration for the RAQMON traps send by the monitor. In case of SLA Call Monitors, a trap will be send to the configured destination when the call data is insufficient to fulfill the SLA. In the case of Call Monitors and Topology-based Call Monitors a RAQMON trap will always be send to the configured destination.
  The trap target configuration is handled on a popup window that is displayed when the button **Configure** is clicked. If no trap target is defined, or the traps are disabled, the string **<disabled>** will be shown in the field.
- **Endpoint Group**: Here a defined endpoint group can be selected to further reduce the objects which should be watched by the monitor.

The following fields differ between the monitor types:

Call Monitor:

- **Calculation Period**: There are two options to choose for „Calculation Period“: „Single Call“ or „Calculation Over Last:“ (value, minutes, …). In the first case, the configured thresholds are applied to each QoS data record (SNMP Trap from endpoint) individually. If a threshold is exceeded, the generated events includes the subscriber number and IP address of the related endpoint. If the configuration period is configured for the last N values, minutes or hours, the thresholds are applied to a set of collected QoS data records and are compared with average, minimum, maximum or median, depending on the configuration. Therefore, the generated event does not refer to a single call or endpoint in this case.
- **Monitored Parameters**: This panel contains a list of the possible parameters that could be monitored. Only the parameters selected in this panel will be added to the database. Individual thresholds can be added to the parameters (see *Section 5.5.2*).

Call Monitoring Templates

To make the creation of multiple call monitors with the same thresholds easier, templates can be used. After creation of a new call monitor template with the desired thresholds, this template can be assigned to a monitor in the create- or modify-dialog. By this way, the same threshold configuration can easily be assigned to multiple monitors. Subsequently changes of an existing template affects all monitors which have the template assigned.

SLA Monitor:

- **Observation Interval**: The length of the time interval that is used to check the fulfillment of SLAs.
- **Condition**, **Threshold**: A condition and thresholds can be defined to configure an SLA and its fulfillment rules (see *Section 5.5.3*).

Topology-based Monitor:

- **Calculation Period**: This field is either filled with a number of values or with a time interval. Either a fixed number of the last QDC traps or all traps within a defined time interval before the current trap are used to calculate aggregated QoS data like the average jitter.
- **Switches/Routers**: A comma separated list of the switches/routers that should be watched by the monitor.
- **Monitored Parameters**: This panel contains a list of the possible parameters that could be monitored. Only the parameters selected in this panel will be added to the database. Individual thresholds can be added to individual parameters (see *Section 5.5.2*).

The currently configured monitors will then be running on the agent, and the parameters that are selected for the monitors will be added to the database.

Monitors can be deleted by checking the check box of the respective monitor and pressing the button **Delete...** in the upper right of the page.

If a monitor is added, deleted or modified, the configuration file of the affected agent will be changed. The agent will then be restarted to activate the changes.

5.5.2 Defining Thresholds

For Call Monitors and Topology-based Monitors, threshold rules can be defined for individual monitored parameters. These threshold rules define a status for a monitored parameter depending on its value.

Defining such thresholds makes it possible to monitor individual parameters like e.g, MOS, Jitter or AverageRoundTripDelay for individual calls.

When the value of a monitored parameter changes, the threshold rules will be checked. When, according to the rules, the status of a parameter changes, an event will be created in the OpenScape FM event browser.

The list of the **Monitored Parameters** can be seen in the respective panel on the detailed information page of an individual monitor. The button **Edit** on the right side of each parameter opens the threshold definition for the respective parameter.

New rules can be added by pressing the button **Add**. Existing rules can be deleted by pressing the button **X** on the right side of the respective rule.

Each rule consists of:

- **Status**: The status that is assigned to the parameter, if the rule matches.
- **Value**: The value that is compared to the **Threshold**. This could be the value of the parameter within the **last** trap. Or it can be the **min**imum, **max**imum, **average** or **median** of the parameter during a defined **Calculation Period** (see *Section 5.5.1*).
- **Relational Operator**: Defines the relation that must be matched by the rule.
- **Threshold**: The value against which the check is performed.

The rules will be checked in the order in which they appear within the configuration window. The first rule that matches, defines the status of the parameter.

5.5.3 Defining SLAs

SLA Monitors check whether incoming calls fulfill the SLA requirements and whether enough calls fulfill the requirements for the SLA to hold.

Both criteria can be configured individually for each SLA monitor on the detailed information page of the respective monitor.

The requirements that have to be fulfilled by the individual calls are configured on the tab **Condition to hold the SLA**.

In this tab, new conditions can be added by pressing the button **Add**. Existing conditions can be deleted by pressing the button **X** on the right side of the respective conditions.

Each condition consists of:

- **Value**: The value that is compared to the **Threshold**. This is the value of the parameter within the current trap.
- **Relational Operator**: Defines the relation that must be matched by the condition.
- **Threshold**: The value against which the check is performed.

The pull down menu on the tab defines, whether only one or all conditions must be met to fulfill the SLA for a single call. If the requirements are not fulfilled for an individual call, a RAQMON trap is send if configured (see *Section 5.5.1*).

The tab **SLA Threshold** is used to configure the status for the SLA itself. Whenever an **Observation Interval** ends, the conditions on this page are checked.

Each condition consists of:

- **Status**: The status that is assigned to the SLA.
- **Relational Operator**: Defines the relation that must be matched by the condition.
- **Threshold**: The percentage value against which the check is performed.

All checks are made against the percentage of the calls that were good calls.

The conditions will be checked in the order in which they appear within the configuration tab. The first condition that matches defines the status of the SLA.

5.6 Web Client Configuration

The main page **Configuration** can be used to configure the web client.

The page Preferences offers a selection menu to define the local **Timezone**.

On the page **JDBC** the database that should be used for the Performance Management data and for the creation of reports can be selected. The pull down menu **New Database JDBC Connection** contains the possible database choices. The menu only contains entries for connections that have been previously configured in the OpenScape FM (see *Section 3.1.1, “Database”*). The page can also be used to define, how long the data should be stored in the database.

The field **Storage Duration [Days]** defines the duration for which Performance Management data is stored in the database. Once a day a database check is performed that deletes Performance Management data which is older then the defined value. To secure ‚old‘ Performance Management data without straining the database, regular database backups should be performed.

6 Displaying Performance Management Results

The OpenScape FM provides a number of overviews and reports that can be used to visualize the Performance Management data collected within the Plugin.

- Overviews (see *Section 6.1*) provide a first impression about the state of the monitored endpoints. Overviews are generated by the ControlCenter Plugin (see *Control Centre Plugin User Guide*).
- The Call Dashboard (see *Section 6.2*) can be used to get an overview about the QoS data of the last 100 monitored calls.
- The Switch/Router Dashboard (see *Section 6.3*) displays performance data over time of monitored switches, routers or any other systems that support the MIB II Interface Table.
- Reports (see *Section 6.4*) provide a more detailed insight and can be used to automatically collect and store the data over time. They are created by the Report Manager Plugin. More about the Report Manager itself can be found in the separate Report Manager Plugin documentation. Scheduled Performance Management reports can be displayed within the OpenScape FM by selecting the main menu entry **Add-Ons=>Performance Management=>Report Schedule**.
- Reports are generated as PDF output. They can either be generated manually or scheduled for automatic generation (see *Section 6.5*). Automatically generated reports can be saved in the file system of the OpenScape FM Server or be send via email. More than one email recipient can be defined by separating them with a comma or space character.

6.1 Overviews

If the ControlCenter plugin has been initialized within the OpenScape FM, a number of ControlCenter overviews is provided within the OpenScape Performance Management. These overviews can be used to identify critical elements within the VoiP network at a single glance.

All overviews can be displayed within the Web Client by using the page **Monitors** within the main page **PM=>Summary**. This page lists the available overviews and the status of the worst member within the individual overviews. By clicking an overview within the list, the respective list of monitors will be opened.

Within the OpenScape FM these overviews can be displayed by using the main menu entry **Add-Ons=>Performance Management=>Control Center - Overview**.

The following overviews are provided:

- A list of the Call Monitors with the highest average jitter.
- A list of the Call Monitors with the highest average packet loss.
- A list of the Call Monitors with the highest average round trip delay.
- A list of the Call Monitors with the lowest average MOS.
- A list of the Call Monitors with the lowest average RValue.
- A list of the SLA Monitors with the lowest service level.

- A list of the Topology Monitors with the highest average jitter.
- A list of the Topology Monitors with the highest average packet loss.
- A list of the Topology Monitors with the highest average round trip delay.
- A list of the Topology Monitors with the lowest average MOS.
- A list of the Topology Monitors with the lowest average RValue.

More about the ControlCenter itself can be found in the respective user guide.

6.2 Call Dashboard

The Call Dashboard provides an overview about the performance data of the last 100 calls for which QoS trap information was received by the Trap Monitor (see *Section 3.3.1.1*) and calculated by the Call Monitor (see *Section 3.3.2*).

In addition performance graphs provide an overview about the average performance values for the last calls over time.

The overview is frequently refreshed and displays all calls for the selected **PM Domain**.

The Call Dashboard is displayed on the page **Call Dashboard** within the main page **PM=>Summary**.

Call List:

The list displayed within the Call Dashboard shows the last 100 calls for which QoS traps have been received for the currently selected **PM Domain**.

Each entry displays the following data: the *Subscriber Number*, the *Start* and *End* time of the call, the *IP Address* of the endpoint that started the call, the *Remote IP* of the endpoint that received the call, and the performance data of the respective call (*Delay*, *Max. Jitter*, *Lost Packets*, *MOS*).

Above the list, threshold values for the four performance values can be defined. Entries within the list that exceed a threshold are displayed in red.

Call Details:

Additional information about a specific call can be displayed by selecting the call from the list and using the tab **Call Details** within the window that opens after the selection. The tab displays the data that was included in the QoS trap which was received for the call.

Call Ping:

For a selected call, Pings can be performed to the IP nodes that define the start point and end point of the call.

This can be done by using the tab **Ping** within the window that opens when a call is selected from the list.

Pressing the button **Ping** performs two Pings from the OpenScape FM Server to the start and end point of the selected call. By default ICMP Pings are used, but other methods can be configured within the OpenScape FM IP Manager Plugin.

Call Layer-2-Path:

The Layer-2-Path between the start and end point of a call can be displayed by using the tab **Layer-2-Path** within the window that opens when a call is selected from the list.

The button **Layer-2-Path** starts a path search within the Layer-2 Manager Plugin of the OpenScape FM and displays its result within a window.

Call Performance Graphs:

The graphs at the top of the Call Dashboard show the performance values of the calls for the current **PM Domain** over time. This can be further restricted to displayed only the data of one selected **Endpoint Group**.

Depending on the selection menu **Average**, the graphs display the average values per *Minute* for the last hour, per for the last day, per for the last Week or per for the last three months. If no average is selected, the individual results will be displayed as received. The displayed data can be refreshed manually with the button **Reload** or automatically if an according value is selected from the selection menu **Reload**. The time of the last refresh is displayed to the right of the **Reload** button.

6.3 Switch/Router Dashboard

The Performance Management Plugin can be configured to monitor the performance parameters of individual devices that support the MIB II Interface Table (e.g. Switches, Routers, Servers). Such devices are named *Interface Devices* in the following.

The monitoring is handled by an Interface Performance Management Monitor named `PerformanceManagement=>InternetPerformance` that is automatically installed and configured within the Performance Management Agent (see *Section 5.1*) to which the currently selected **PM Domain** is assigned.

The individual devices that should be monitored have to be manually added by a user. These devices are then automatically added to the target list of the Monitor.

The Monitor collects the performance management data, calculates averages over defined time intervals and provides the data for the Performance Management Plugin.

On the Switch/Router Dashboard the monitored devices are listed. The collected data can be displayed as a graph over time, or within the Detail Information for an interface.

The page **Switch/Router Dashboard** within the main page **PM=>Summary** displays the list of monitored interface devices. Here monitoring targets can be added, reconfigured or deleted. The collected results are also displayed on this page.

Displaying the Results:

If the column **Show Charts** is marked for interface devices, the performance graphs (*Utilization*, *Throughput*, *Error Rate*) are displayed at the top of the page. Depending on the selection menu **Average**, the graphs display the average values per *Minute* for the last hour, per for the last day, per for the last Week or per for the last three months. If no average is selected, the individual results will be displayed. The displayed data can be refreshed manually with the button **Reload** or automatically if an according value is selected from the selection menu **Reload**. The time of the last refresh is displayed to the right of the **Reload** button.

Searching Interface Devices:

Searches can be performed for the currently selected **PM Domain**. The **Search Area**, located above the list, can be used to restrict the displayed devices to those that contain the search string (case insensitive) within the selected column. Pressing **Show All** disables a search filter.

Devices are selected by checking the respective list entry on the left hand side of the row.

Interface Device Details:

Clicking a device within the device list opens an information window for the interface device. The information window contains five tabs.

- **Performance Info**: This tab displays the last **Utilization**, **Throughput** and **Error Rate** values for the clicked device. It also displays the three respective graphs with the average values over time for each interface.
- **Details**: This tab shows the **Label**, the **IP Address** and **Fully Qualified Hostname** of the device. It also shows the current **Status** of the device, the time of the **Last Status Change** and the **Status Polling Interval**.
- **Status Explanations**: This tab explains the reason of the device‘s current status. It also shows the objects and events that concern the status.
- **Network Interfaces**: This tab contains a list of the device‘s interfaces.
- **Child Objects**: This tab contains a list of the child objects of the device object.

Adding Interface Devices:

Using the button **Add** opens a window in which the IP address or hostname of an interface device and the affected PM Agent can be entered. The second tab of the window is used to enter the SNMP configuration to connect to the MIBII of the interface device. When the button **Ok** is pressed, the device will be added to the list of monitored devices and to the target list of the respective Monitor. The Performance Management Agent to which the Monitor has been assigned will then be restarted. This may take some time and a manual reload of the list is necessary to see the effect.

Configuring Interface Devices:

Using the button **Configure** opens a window in which the configuration parameters of the selected device are displayed and in which they can be modified. Within the window the **SNMP Configuration** for the interface device can be defined.
The SNMP Configuration is performed for the respective IP node within the OpenScape FM (see *IP Manager Plugin User Guide*).

Removing Interface Devices:

Using the button **Delete** removes the selected device from the list of monitored interface devices (after a confirmation). It also automatically removes the device from the target list of the respective Monitor. This means that the Performance Management Agent to which the Monitor has been assigned will be restarted and the data collected for the deleted device will be lost.

Interface Device Ping:

Using the button **Ping** performs a Ping from the OpenScape FM Server to the selected device. By default ICMP Pings are used, but other methods can be configured within the OpenScape FM IP Manager Plugin.

6.4 Reports

Reports are used to display the data, collected by the various monitors.

This section explains the various reports and how they are started manually. *Section 6.5* describes how reports can be generated automatically.

The following subsections describe the available reports. The reports can be selected using the respective report entry within the menu **Report Generation** on the main page **PM=>Reporting**.

The upper part of all report pages consists of a search area in which the data, that should be displayed in the report can be restricted.

The search can be restricted to the **Current Domain**, or performed using **All Domains**

If **All Domains** is selected, the search will be performed across all domains to which the current user has the respective access rights.

If the search is restricted to the **Current Domain**, the search can additionally be restricted to a single **Endpoint Group**.

The panels **Start of Call** or **End of Call** can be used to define time intervals in which the calls must have been started or ended to be used for the report.

The checkbox **true-to-scale Time Axis** can be marked to display the time on a linear axis. If the box is not marked, the records will still be ordered by time, but they will be represented with an equal distance between the records.

With the checkbox **tabular view only** the method for the display of values can be modified. If this checkbox is marked, the graphical representation of values will be removed from the report and replaced by a table containing the respective data.

Entries within the fields restrict to the objects to those that have the input as a substring.

All reports are created manually by selecting the output format (**PDF**) and pressing the button **Generate**.

The application will then determine the size of the output. If this would be to large or to time consuming, a warning will be displayed. A more restricting search filter will then be necessary for the successful generation of a report.

6.4.1 Call Report

The Call Report visualizes the performance of individual calls. It contains charts for the following QoS parameters:

- Jitter
- Average Round Trip Delay
- Package Loss
- R-Value
- MOS Factor

The chart shows the measured values on the y-axis and the time on the x-axis.

Call reports can be configured and started on the page **Report Generation=>Call** of the main page **PM=>Reporting**.

6.4.2 Call Search

Call Searches are used to find all calls for which QoS data exists and which match the selected search criteria.

If the button **Search...** is pressed, a list that includes all matching calls will be displayed on the page. Detailed data about a call can then be displayed by clicking on the respective list entry.

If the button **Report...** is pressed, a Call Report (see *Section 6.4.1*) will be generated that only includes the calls that were selected within the displayed list.

Call Searches can be configured and started on the page **Call Search** of the main page **PM=>Reporting**.

By pressing the button **CSV**, the results of a Call Search can be exported into a file as a Comma-Separated Values list (see *Section 9.3*).

6.4.3 Cumulative Call Report

The Cumulative Call Report cumulates values from multiple calls of one or multiple distinct endpoints.

The accumulation is performed by combining QoS data in a given time interval for all involved calls. The average, median, minimum and maximum values are calculated, based on the QoS data.

The report contains charts for the following QoS parameter values:

- Jitter
- Average Round Time Delay
- Packet Loss
- R-Value
- MOS Factor

The chart shows the measured values on the y-axis and the time on the x-axis.

Beside the search parameters common for most reports, an additional **Report Parameter** can be selected in the menu **Period**. This selection defines the time interval that is used to calculate the values.

Cumulative Call reports can be configured and started on the page **Report Generation=>Cumulative Call** of the main page **PM=>Reporting**.

6.4.4 Cumulative Consecutive Packets Report

The Cumulative Consecutive Packets Report shows the number of consecutive lost/good packets for calls. The endpoints provide information for 1 up to 10, or more than 10 consecutive lost/good packets. This information is displayed within the report.

In the included charts the x-axis gives the information on how many packets in percent have been received or lost consecutively, the y-axis shows how many times the number of packets have been received or lost.

Beside the search parameters common for most reports, an additional **Report Parameter** can be selected with the checkbox **Extended Version**. If this checkbox is **not** marked, the report contains the aggregated information about all endpoints that match the search criteria. If the checkbox is marked, in addition the information is displayed individually for each matching endpoint.

Cumulative Consecutive Packets reports can be configured and started on the page **Report Generation=>Cumulative Consecutive Packets** on the main page **PM=>Reporting**.

6.4.5 Consecutive Packets Over Time Report

The Consecutive Packets Over Time report shows the progress of consecutive lost/good packets over time. It is similar to the Cumulative Call Report (see *Section 6.4.4*) but with added information about the changes over time.

This report represents the QoS data for the selected calls in a 3D-chart with three axes. The x-axis shows the timestamp of the measured data, the y-axis shows the number of consecutive packets, and the z-axis shows the number of occurrences in percent for the cumulative packets for the given timestamp.

Beside the search parameters common for most reports, two additional **Report Parameter** can be selected:

If the checkbox **Extended Version** is **not** marked, the report contains the aggregated information about all endpoints that match the search criteria. If the checkbox is marked, in addition the information is displayed individually for each matching endpoint.

The menu **Period** defines the length of the time intervals that are used to calculate the values.

Consecutive Packets Over Time reports can be configured and started on the page **Report Generation=>Consecutive Packets Over Time** of the main page **PM=>Reporting**.

6.4.6 Call Monitor Report

The Call Monitor Report displays the data collected by the Call Monitor described in *Section 3.3.2*.

The report shows the QoS data of an endpoint domain/group over time.

Besides the search parameters common for most reports, additional **Report Parameters** can be selected within the checkbox list **Monitored Parameters**. The list contains the parameters that are collected by the monitor. Only the parameters that are marked will be displayed in the report.

The charts show the measured values on the y-axis and the time on the x-axis.

Call Monitor reports can be configured and started on the page **Report Generation=>Call Monitor** of the main page **PM=>Reporting**.

6.4.7 SLA Monitor Report

The SLA Monitor Report displays the data collected by the SLA Call Monitor described in *Section 3.3.3*.

The report shows the computed SLA values (degree of fulfillment in percent) over time.

The charts show the measured values on the y-axis and the time on the x-axis.

SLA Monitor reports can be configured and started on the page **Report Generation=>SLA Monitor** of the main page **PM=>Reporting**.

6.4.8 Topology Monitor Report

The Topology Monitor Report displays the data collected by the Topology-based Call Monitor described in *Section 3.3.4*.

The report shows the QoS data for specific interfaces and IP nodes over time.

Besides the search parameters common for most reports, additional **Report Parameters** can be selected within the checkbox list **Monitored Parameters**. The list contains the parameters that are collected by the monitor. Only the parameters that are marked will be displayed in the report.

The charts show the measured values on the y-axis and the time on the x-axis.

Topology Monitor reports can be configured and started on the page **Report Generation=>Topology Monitor** of the main page **PM=>Reporting**.

6.5 Report Scheduling

The previous chapters describe how the various reports can be configured and started manually.

In many cases reports should be generated automatically in regular time intervals. These can be used to keep track of the QoS data over time. Since the reports can be send as emails, scheduled reports can also be used to keep track of the performance status when no direct access to the Performance Management is possible.

The configuration of the scheduling of reports is a two step process:

First the search criteria and the reports that should be generated have to be selected (see *Section 6.5.1*).

Then an execution plan has to be created (see *Section 6.5.2*). This plan defines, when and how often the report chosen in the first step should be generated.

6.5.1 Templates

Templates are the combination of a selected report and the search parameters defined for the report. This combination defines the data that should be displayed within reports that are created automatically.

Templates are created by selecting one of the reports described in *Section 6.4* from the menu **Report Generation** within the main page **PM=>Reporting**.

The panel **Template** can be used to store a template with the currently defined search criteria.

A unique **Name** has to be assigned to the template. This name will be used to reference the template in selection lists and within the generated outputs.

To send the generated outputs as emails, the checkbox **Send as e-mail** has to be marked and a sender and recipient have to be defined. More than one email recipient can be defined by separating them with a comma or space character. The SMTP configuration in the OpenScape FM Server is used to define the mail server (see *OpenScape FM Desktop User Guide*).

If the checkbox **Store as file** is marked, the output will be stored on the OpenScape FM Server. The output file is saved in the directory `<OpenScape FM Install Dir>/export/generatedReports`. The name of the file begins with the string ‚Scheduled', followed by the name of the schedule and the date and time of the creation.

The button **Store Template** will save the template itself for further use.

The page **Report Scheduling=>Templates** on the main page **PM=>Reporting** displays a list of all defined templates. Here the button **Delete...** can be used to remove selected templates.

6.5.2 Execution Plans

Execution Plans define the time at which stored templates are to be executed.

New Execution Plans can be created by selecting a template on the page **Report Scheduling=>Templates** of the main page **PM=>Reporting** and pressing the button **Report Scheduling...** on either the list page or in the detailed information window.

The button opens a configuration window in which an identifying name (**Description**) can be added to the schedule.

It can also be selected whether the plan should create a single report (**Single Execution**) or if the report should be created in regular intervals (**Multiple Execution**).

In both cases a **Start** date has to be entered. In the latter case also an **End** date and a time interval (**Period**, **Multiplier**) can be entered. The field **Multiplier** defines multiples of the selected interval. If e.g. ‚Daily' and ‚3' are entered, the report will be created every three days.

If no **End** date is entered, the respective report will be created indefinitely using the defined time interval.

The button **Save** stores the Execution Plan.

The output is generated in PDF format. The checkbox **Public Report** defines whether the output should be visible to all users or only to the user that created the execution plan.

The list of all currently active Execution Plans, and their next planned execution time, can be seen on the page **Report Scheduling=>Execution Plan** of the main page **PM=>Reporting**. The button **Delete...** can be used to remove no longer needed plans.

6.5.3 Report Results

The page **Report Scheduling=>Report Files** on the main page **PM=>Reporting** can be used to handle the output of the execution plans.

The page contains a list that shows the report results that are accessible for the current user.

This page also displays the CSV files, that were saved on the Server system because they exceed the defined size (see *Section 9.3*).

Selected files can be removed from the file system of the OpenScape FM Server host (**Delete**), displayed in a PDF viewer (**Show**) or copied from the OpenScape FM Server to the system on which the OpenScape FM Client is running (**Download**).

The public files are stored on the OpenScape FM Server system within the folder:

```
<OpenScape FM Installation>\client\public\export\generatedReports
```

The private files are also stored on the OpenScape FM Server system, but in directories that are accessible only by the user which has adequate access rights, usually by the creator of the execution plan:

```
<OpenScape FM Installation>\client\user\<UserName>\export\generatedReports
```

7 IP Manager Integration

IP Networks and Nodes of the OpenScape FM are displayed within the Performance Management Plugin to provide an easy access to these important objects. More about IP Networks and IP Nodes can be found in the *IP Manager Plugin User Guide*.

The IP Manager data of the OpenScape FM is displayed within three pages of the main page **IP Manager**:

- The page **Dashboard** provides a Control Center Overview about the current status of IP Manager objects (see *Section 7.1*).
- The page **Networks** displays information about networks known by the OpenScape FM (see *Section 7.2*).
- The page **Nodes** displays information about IP nodes known by the OpenScape FM (see *Section 7.3*).

7.1 Dashboard

The page **Dashboard** within the main page **IP Manager** provides an overview about the current state of IP nodes, interfaces, routers and switches known by the OpenScape FM.

The displayed page corresponds to the contents of the respective Control Center Overview of the IP Manager Plugin within the OpenScape FM (see *OpenScape FM IP Manager User Guide*). If the individual panels are reconfigured within the OpenScape FM or if new panels are assigned to the overview, these changes will also be displayed in the Performance Management Plugin.

Within the plugin itself, the dashboard cannot be changed and the display is not interactive.

By default the OpenScape FM displays the following panels:

- The Status distribution of the IP events received within individual days as a bar chart.
- The last 10 IP Nodes that changed to Status *Critical* as a list.
- The last 10 IP Interfaces that changed to Status *Critical* as a list.
- The last 10 Switches that changed to a Status other than *Normal* as a list.
- The last 10 Routers that changed to a Status other than *Normal* as a list.

7.2 Networks

The page **Networks** within the main page **IP-Manager** displays the list of networks from the OpenScape FM to which the Performance Management Plugin is attached (see *OpenScape FM Desktop User Guide*).

This page can be used to see the networks, network details, and to handle the networks. All actions performed on this page are directly performed within the OpenScape FM itself.

The page displays a list of all networks that would be displayed for the current user within an OpenScape FM Client.

Searching Networks:

Within the upper part of the page, the **Search Area** can be used to restrict the displayed networks to only those that contain the search string (case insensitive) within the selected column. Pressing **Show All** disables a search filter.

Networks are selected by checking the respective list entry on the left hand side of the row.

Network Details:

Clicking a network within the network list opens an information window for the network. The information window contains four tabs.

- **Details**: This tab shows the **Label**, the **IP Address** and network **Mask** of the network. It also shows whether the **Auto Discovery** is enabled, the current **Status** of the network, and the time of the **Last Status Change**.
- **Status Explanations**: This tab explains the reason of the network‘s current status. It also shows the objects and events that effect the status.
- **Child Objects**: This tab contains a list of the child objects of the network object.
- **IP Nodes**: This tab contains a list of the IP nodes that are located within the network.

Adding Networks:

Using the button **Add** opens a window in which the parameters for an additional network can be entered. This network will be created within the OpenScape FM database when the button **Ok** is pressed. The following parameters have to be defined:

- **Network Address**, **Network Mask**: These base parameters define the address range of the network.
- **Network Name**: The label used for the network.
- **Auto Discovery**: The selected method determines, whether the network will be (additionally) analyzed using the ARP Cache discovery and whether found IP nodes will be added to the network or not.
- **Start Address Scan**: If this is marked, an additional dialogue allows the definition of an IP address range to be scanned. Every single IP address in the defined range will be analyzed and found nodes will be added.
- **Delete Empty Network Automatically**: If this is marked, the network container will automatically be deleted, when the last IP node of the network is deleted.

Configuring Networks:

Using the button **Edit** opens a window in which the network parameters of the selected network are displayed and in which they can be modified. The parameters are the same as described above (*Adding Networks*).

Deleting Networks:

Using the button **Delete** removes the selected networks and the nodes within these networks from the OpenScape FM database after a confirmation.

Acknowledging Networks:

Using the button **Ack. Events** acknowledges all events within the OpenScape FM database that are assigned to one of the nodes within the selected network.

Show Network Nodes:

Using the button **Show IP Nodes** displays a list of the IP Nodes that are located within the selected network. This corresponds to a node list restricted to the selected network (see *Section 7.3*).

7.3 Nodes

The page **Nodes** within the main page **IP-Manager** displays the list of IP nodes from the OpenScape FM to which the Performance Management Plugin is attached (see *OpenScape FM Desktop User Guide*).

This page can be used to see the IP nodes, IP node details, and to handle the IP nodes. All actions performed on this page are directly performed within the OpenScape FM itself.

The page displays a list of all IP nodes that would be displayed for the current user within an OpenScape FM Client.

Searching IP Nodes:

Within the upper part of the page, the **Search Area** can be used to restrict the displayed IP nodes to only those that contain the search string (case insensitive) within the selected column. Pressing **Show All** disables a search filter.

The search can additionally be restricted to only those IP nodes that are located within a selected network.

IP nodes are selected by checking the respective list entry on the left hand side of the row.

IP Node Details:

Clicking an IP node within the IP node list opens an information window for the IP node. The information window contains four tabs.

- **Details**: This tab shows the **Label**, the **IP Address** and network **Fully Qualified Hostname** of the IP node. It also shows the current **Status** of the network, the time of the **Last Status Change**. and the **Status Polling Interval**.
- **Status Explanations**: This tab explains the reason of the IP node‘s current status. It also shows the objects and events that effect the status.
- **Network Interfaces**: This tab contains a list of the IP node‘s interfaces.
- **Child Objects**: This tab contains a list of the child objects of the IP node object.

Adding IP Nodes:

Using the button **Add** opens a window in which the IP address or hostname of an additional network can be entered. This IP node will be created within the OpenScape FM database when the button **Ok** is pressed.

Adding SubComponents to IP Nodes:

Using the button **New** opens a window in which a Web Server or SNMP Agent can be defined. The new server or agent will be added as a subcomponent to the selected IP node when the button **Ok** is pressed.

Configuring IP Nodes:

Using the button **Configure** opens a window in which the IP node parameters of the selected node are displayed and in which they can be modified. Within the window the **Polling Intervals**, **SNMP Configuration** and **Maintenance Intervals** for the IP node can be defined (see *IP Manager Plugin User Guide*).

Deleting IP Nodes:

Using the button **Delete** removes the selected IP nodes from the OpenScape FM database after a confirmation.

Acknowledging IP Nodes:

Using the button **Ack. Events** acknowledges all events within the OpenScape FM database that are assigned to one of the selected IP nodes.

IP Nodes Ping:

Using the button **Ping** performs a Ping from the OpenScape FM Server to the selected nodes. By default ICMP Pings are used, but other methods can be configured within the OpenScape FM IP Manager Plugin.

8 Events

The OpenScape FM events are displayed within the Performance Management Plugin to provide an easy access to this important OpenScape FM data.

The OpenScape FM event data is displayed within two pages of the main page **Events**:

- The page **Dashboard** provides a Control Center Overview about the current OpenScape FM events (see *Section 8.1*).
- The page **Events** displays the data from the OpenScape FM Event Browser (see *Section 8.2*).

8.1 Dashboard

The page **Dashboard** within the main page **Events** provides an overview about the current OpenScape FM events.

The displayed page corresponds to the contents of the respective Control Center Overview of the Event Browser within the OpenScape FM (see *OpenScape FM Desktop User Guide*). If the individual panels are reconfigured within the OpenScape FM or if new panels are assigned to the overview, these changes will also be displayed in the Performance Management Plugin.

Within the plugin itself, the dashboard cannot be changed and the display is not interactive.

By default the OpenScape FM displays the following panels:

- The Status distribution of the current events as a pie chart.
- The Status distribution of the events received within individual days as a bar charts.
- The IP Nodes with the most events that are of Status *Critical* and still unacknowledged as a list.
- The IP Nodes with the most unacknowledged events as a list.
- The last 10 events that were not of Status *Normal* as a list.

8.2 Events

The page **Events** within the main page **Events** displays the list of events from the OpenScape FM to which the Performance Management Plugin is attached (see *OpenScape FM Desktop User Guide*).

This page can be used to see the events, event details, and to handle the events. All actions performed on this page are directly performed within the OpenScape FM itself.

When the page is opened or reloaded it displays a list of all events that would be displayed for the current user within an OpenScape FM Client.

Searching Events:

Within the upper part of the page, the **Search Area** can be used to restrict the displayed events to only those that contain the search string (case insensitive) within the selected column. Pressing **Show All** disables a search filter.

Events are selected by checking the respective list entry on the left hand side of the row.

Event Details:

Clicking an event within the event list opens an information window for the event. The information window contains five tabs.

- **Info** shows base information: the event‘s **Description**, the creation **Date**, the event‘s **Category** and **Source**, by whom and when the event was **Acknowledged**, and the **Status** of the event. The event can also be acknowledged on this tab.
- **Event Details** shows the event **Attributes** and their **Values**.
- **Annotation** shows the Annotation of the event. The Annotation can also be changed and saved on this tab.
- **Parent Event** shows the event to which the current event correlates.
- **Related Events** shows the events that are correlated to the current event.

Deleting Events:

Using the button **Delete** removes the selected events from the OpenScape FM database after a confirmation.

Acknowledging Events:

Using the button **Acknowledge** acknowledges the selected events within the OpenScape FM database.

Annotating Events:

Using the button **Annotate** opens a window in which a comment for the event can be created or modified. If an Annotation has been assigned to an event, this will be marked within the list by a speech bubble in the column **Ack**.

9 External Software Integration

This chapter handles the integration of Unify software into the Performance Management Plugin and the export of data as CSV files.

The following sections describe the integration of the Trace Manager (see *Section 9.1*) and the OpenScape DLS (see *Section 9.2*) as well as the export of data into CSV files (see *Section 9.3*).

9.1 Trace Manager

The Performance Management Plugin can be configured to use Trace Manager information as an additional source for QoS data. The collected data will be displayed as usual within the plugin.

How a Trace Manager is prepared to deliver data to the plugin and how the plugin itself has to be configured is described in the following subsections.

9.1.1 Trace Manager Preparation

Remote Access

The QoS data is collected by an OpenScape FM System Management agent. This agent can be installed locally on the Trace Manager or on a separate system. If the agent is installed on a separate system (e.g. the internal agent of the OpenScape FM server is used), the Trace Manager has to be configured to allow remote access.

For this, the file "`trustedIP.txt`" has to be located (standard location `C:\MTC\Config`) and the IP address of the machine where the System Management agent is running has to be added. If the internal agent of the OpenScape FM server is used, the address of the OpenScape FM server has to be added.

SQL Query

The System Management agent executes three SQL queries to request the QoS data and information about the related IP phones. The needed queries are predefined in the Trace Manager.

9.1.2 Trace Manager Configuration

The page **Trace Manager** on the main page **Configuration=>PM** is used for the configuration of the Trace Manager integration within the plugin. The page contains a list of the already configured Trace Manager connections.

Pressing the button **Add** or **Modify** opens the Trace Manager configuration window to create a new Trace Manger connection or to reconfigure a selected connection. Clicking a list entry activates the modification of the respective entry.

The button **Delete** removes a selected Trace Manager connection. Removing a connection stops the collection of data from this source. Already collected data will not be removed from the plugin.

The configuration window contains the following fields:

- **Status**: (read-only, only visible while modifying) The status of the object that represents the connection within the OpenScape FM. This gives an indication whether the connection has any problems.
- **PM Agent**: The IP address of the agent which should perform the Trace Manager queries.
- **Label**: An arbitrary name for this Trace Manager.
- **Trace Manager**: The IP address of the Trace Manager.
- **Port**: Port of the web interface of the Trace Manager, usually 28081.
- **System**: The Trace Manager system (productive system) that should be queried.
- **Query Name**: The name of the Trace Manager SQL query for the table "`PerfData`". The pre-defined query within the Trace Manager is "`QoS PerfData`".
- **CallID Query Name**: The name of the Trace Manager SQL query for the table "`CallId`". The pre-defined query within the Trace Manager is "`QoS CallID-PerfData`".
- **Call Association Query Name**: The name of the Trace Manager SQL query for the table "`CallAssociations`". The pre-defined query within the Trace Manager is "`QoS CallAssociations-PerfData`".
- **Limit**: The number of imported data sets will be limited to this number.
- **Import data since**: This date is used only for the first query. In all subsequent queries, only the data since the last query will be fetched. If not specified, the data of the last 24h is imported (default behavior of Trace Manager).
- **Accept Filter (Regular Expression)**: A regular expression that defines a positive filter on the local Subscriber Number. Only records that match the filter are evaluated.
- **Ignore Filter (Regular Expression)**: A regular expression that defines a negative filter on the local subscriber number. Only records that do not match the filter are evaluated.

If neither an Accept Filter nor an Ignore Filter is defined, all records are accepted.

If an Accept filter but no Ignore filter is defined, only records that match the Accept filter are accepted.

If an Ignore Filter but no Accept Filter is defined, all records that do not match the Ignore Filter will be accepted.

If both an Ignore Filter and an Accept Filter are defined, only records that match the Accept Filter but do not match the Ignore Filter will be accepted.

Important Note:
The Ignore Filter has a higher priority than the Accept Filter. Data records that match both filters are ignored. It is particularly important not to define contradictory filters.

After pressing the **Save** button, the Trace Manager monitor will be created or reconfigured on the selected agent/domain. This may take some time. All data sets beginning with the date configured in **Import data since** will be retrieved. After this, the Trace Manager monitor retrieves the data since the last import in five minutes intervals.

Note:
When a larger number of endpoints are to be monitored, Performance Management queries to the Trace Manager might take significant time. In this case, it is suggested to use "`Daily`" as the selected DB Partition. *Section 7.24.4 of the OpenScape Voice V7, Trace Manager, Service Documentation* contains information how to change the DB Partition.

9.1.3 Trace Manager Trouble Shooting

Connection to Trace Manager Fails

If the status of a Monitor is not "*Normal*", its symbol can be clicked to open the configuration window.

Within the window, the field "**Message**" contains the URLs that are used to query the Trace Manager.

To check if they are working, the URLs can be opened in a browser. The result should be JSON text.

If no JSON text is displayed, the file "`trustedIP.txt`" on the Trace Manager should be checked for the required IP addresses.

If the queries are working but the results are empty, it should be checked whether the Trace Manager tables "`PerfData`", "`CallID`" and "`CallAssociations`" actually contain data for the relevant time interval.

Connection to Trace Manager Works, but no Data is Written into the Database

It has to be ensured that the monitors "`PathFinder=>Path Finder Monitor`", "`QdcMonitor=>Export Monitor`" and "`QdcMonitor=>Trap Monitor`", located within the container "`Internal System Management=>PerformanceManagement`" within the OpenScape FM navigation tree, are set to "*managed*".

Monitors can be set to the state "*managed*", by selecting the entry "**Edit=>Manage**" from the context menu of the respective monitor symbol.

If the menu item "**Manage**" is not available, the entry "**Server=>Administration=>License Manager=>License Information**" from the main menu bar should be invoked. If the menu item "**Manage**" is still unavailable, it should be checked if the status of the Performance Management License is "*OK*".

9.2 OpenScape DLS

The Performance Management Plugin can be configured to display OpenScape DLS Endpoint information as additional data. The data will be displayed within the plugin.

In addition, the DLS Endpoint configuration can be displayed and reconfigured from within the plugin.

How the OpenScape FM and the plugin have to be prepared to display DLS data within the plugin and how the data can be accessed is described in the following subsections.

9.2.1 DLS Preparation

A user account that should be used by the Performance Management Plugin has to be created within the OpenScape DLS.

It has to be a DLS API user that has the role `DLS-API`.

9.2.2 DLS Configuration

The DLS Configuration consists of two parts. One within the Performance Manager Plugin and one within the OpenScape FM.

DLS Configuration within the Plugin:

The page **DLS Configuration** on the main page **Configuration=>PM** is used for the configuration of the OpenScape DLS integration within the plugin. The page contains a list of the already configured OpenScape DLS connections.

Pressing the button **Add** or **Modify** opens the OpenScape DLS configuration window to create a new OpenScape DLS connection or to reconfigure a selected connection. Clicking a list entry activates the modification of the respective entry.

The button **Delete** removes the selected OpenScape DLS connections.

The configuration window contains the following fields:

- **Status**: (read-only, only visible while modifying) The status of the object that represents the connection within the OpenScape FM. This gives an indication whether the connection has any problems.
- **DLS Name**: The label that will be used to represent the connection.
- **Host**: The IP address or hostname of the machine on which the OpenScape DLS is running.
- **Port**: The port number over which the connection to the OpenScape DLS should be established. This corresponds to the web port of the DLS.
- **HTTPS**: This defines whether an HTTP or HTTPS connection should be used. For an HTTPS connection the respective certificate has to be confirmed within the OpenScape FM (see below).
- **Username**, **Password**: The account and its password that should be used for the connection to the OpenScape DLS.

After pressing the **Save** button, the plugin adds the connection and tries to connect to the OpenScape DLS using the OpenScape FM. Usually this will initially fail since the connection also has to be configured within the OpenScape FM.

DLS Configuration within the OpenScape FM:

Within the OpenScape FM the DLS machine has to be added as an IP node.

During the automatic discovery for the node, the OpenScape DLS web port should be detected and a respective symbol should appear on the submap of the IP node (e.g. an HTTPS symbol with the label `HTTPS 10444`).

Using the entry **Configure** from the context menu of this symbol opens the configuration window.

On the tab **HTTP Connection Parameter** the **HTTP Login** and **HTTP Password** for the connection to the Web Portal have to be entered.

If the OpenScape DLS server uses a self-signed SSL certificate, this has to be accepted before an HTTPS connection can be established. The certificate is displayed and can be accepted on the tab **Certificate**, or via the entry **Administration=>SSL Certificates** from the main menu **Server**.

When the connection to the Web Portal is configured, a symbol representing the connection should appear in the container:
`Root=>System=>Server=>DLS Manager`

The entry **Configure** from the context menu of this symbol opens a window in which the **Login** and **Password** that should be used for the connection to the OpenScape DLS can be entered.

9.2.3 DLS Endpoints

If a connection to an OpenScape DLS is established, the page **DLS Endpoints** within the main page **PM=>Endpoints** displays the list of Endpoints that are known by the selected **DLS Server**.

This page can be used to see the Endpoints and to reconfigure them within the OpenScape DLS. All actions performed on this page are directly performed within the OpenScape DLS itself.

Searching DLS Endpoints:

Within the upper part of the page, the **Search Area** can be used to restrict the displayed Endpoints to only those that contain the search string (case insensitive) within the selected column. Pressing **Show All** disables a search filter.

Endpoints are selected by checking the respective list entry on the left hand side of the row.

DLS Endpoints Details:

Clicking an Endpoint within the Endpoint list opens an information window for the Endpoint.

DLS Endpoints Configuration:

The button **Data Collection** can be used to change the configuration of the selected Endpoints within the OpenScape DLS.

When the button is pressed, a window opens in which various configuration parameters can be entered and saved to the DLS.

From here the current configuration can also be stored as a template.

The selection menu **Template Name** can be used to configure the parameters to a predefined set of values (see *Section 9.2.4*). This will copy the values from the template to the current window. If the template is changed at a later time, this change will not automatically apply for the current configuration.

9.2.4 DLS QoS Templates

To simplify the assignment of configuration values to DLS Endpoints, it is possible to define value templates. Templates contain a full set of defined values which can be assigned to an Endpoint with a single selection (see *Section 9.2.3*). They are stored within the OpenScape FM.

The Templates can be viewed and configured on the page **QoS Templates** within the main page **PM=>Endpoints**.

The page displays a list of all QoS Templates.

Searching QoS Templates:

Within the upper part of the page, the **Search Area** can be used to restrict the displayed QoS Templates to only those that contain the search string (case insensitive) within the selected column. Pressing **Show All** disables a search filter.

QoS Templates are selected by checking the respective list entry on the left hand side of the row.

Adding QoS Templates:

The button **Add** opens a window in which the parameters for an additional Template can be entered. The Template is created when the button **Ok** is pressed.

The parameter **Template Name** defines the label that is used to identify the Template within selection menus.

Configuring QoS Templates:

The button **Modify** opens a window to display and modify the parameters of the selected Templates.

If a Template is clicked within the list, the configuration window will be opened for the respective Template.

Deleting QoS Templates:

The button **Delete** removes the selected Templates from the OpenScape FM database.

9.3 CSV Export

To transfer the collected data to e.g. a spreadsheet or database, the Performance Management provides a mechanism to export the data as CSV files. These contain a list of comma-separated values that can be easily imported.

Exporting CSV Data

A CSV file can be created by pressing the button **CSV** after a search has been performed.

All datasets that match the search criteria will be exported into the CSV file. This is independent of the selections made within the displayed results, and all data for the respective datasets will be exported. Each dataset within the created file is represented within a separate line.

Important Note:
The CSV export is not provided for all result lists.
Examples for searches that support the CSV export are the search for Endpoints (see *Section 5.4*) or the listing of Calls (see *Section 6.4.2*).

Viewing CSV Data

Generally CSV data can be seen immediately after the creation on the system on which the local Performance Management client is running. After the collection of the data, a window will be displayed. From this window it can be selected whether the data should be displayed by a chosen program or stored on the local system.

If the number of datasets that has been found by a search exceeds a predefined value (see below: *CSV Configuration*), the file will not be send to the Performance Management client immediately, but it will be created and stored on the server. The access to the stored file can be handled with the same methods that are used for files that are created by scheduled reports (see *Section 6.5.3*)

CSV Configuration

Within the configuration for CSV data export, a limit for the number of datasets that are directly transferred to the client can be defined. If this number is exceeded by a search, the data will be stored on the PM server instead. This makes it possible to save large quantities of data without stressing the client or without preventing the access to the client for long time.

The configuration can be made on the page **Preferences** within the main page **Configuration=>Global** (field: **Limit rows in CSV files**).

Index

A

Acknowledge
- Events 44
- IP Nodes 42
- Networks 40

Add
- IP Nodes 41
- Networks 40
- QoS Templates 50
- Sub Components 41
- Switches/Routers 32

Agent 11
- Configuration 11
- Discovery 11
- Distributed 11
- Installation 11
- List 21

Annotate
- Events 44

Architecture 8
Average Round Trip Delay 13

C

Call Monitor 14
Call Monitor Report 35
Call Report 33
Calls
- Dashboard 30
- Details 30
- Layer-2-Path 31
- List 30
- Performance Graph 31
- Ping 30

Call Search 34
Configuration
- Agent 11
- DLS 48
- DLS Endpoints 49
- Monitor 23
- Trace Manager 45
- Web Client 19, 27

Configure
- IP Nodes 42
- Networks 40
- QoS Templates 50
- Switches/Routers 32

Consecutive Packet Loss 13
Consecutive Packets Over Time Report 35
CSV 50
Cumulative Call Report 34
Cumulative Consecutive Packets Report 35

D

Dashboard
- Calls 30
- Events 43
- IP Manager 39
- Switch/Router 31

Database 9
Data Collection 9
Delete
- Events 44
- IP Nodes 42
- Networks 40
- QoS Templates 50

Details
- Calls 30
- DLS Endpoints 49
- Events 44
- IP Nodes 41
- Networks 40
- Switches/Routers 32

Discovery
- Agent 11

Distributed Agent 11
DLS 47
- Configuration 48
- Endpoints 49
- Preparation 48
- QoS Templates 50

DLS Endpoints
- Configuration 49
- Details 49
- Searching 49

Domains 21

E

Endpoints 22
- DLS 49

Events 43
- Acknowledge 44
- Annotate 44
- Dashboard 43
- Deleting 44

Details 44
List 43
Searching 44
Execution Plans 37

G

Groups 22

I

Installation
Agent 11
Web Client 19
Interfaces 31
IP Manager
Dashboard 39
IP Nodes 41
Acknowledge 42
Adding 41
Configuration 42
Deleting 42
Details 41
Ping 42
Searching 41
Sub Components 41
IP Protocols 11

J

Jitter 13

L

Layer-2-Path
Calls 31
Licensing 20
List
Calls 30
Events 43
Lost Packets Percent 13

M

Maximum Inter Arrival Jitter 13
Monitor 13
Call 14
Configuration 23
QDC 13
QDC Export 14
SLA Call 15
Topology-based Call 16
Trap 14
MOS 12

N

Networks 39
Acknowledge 40
Adding 40
Configuration 40
Deleting 40
Details 40
Searching 40
Show Nodes 41
Nodes
Show Network Nodes 41

O

OpenScape DLS 47
OpenScape FM
IP Manager,IP Manager
OpenScape FM 39
Overviews 29

P

Packet Loss 13
Performance Graph
Calls 31
Ping
Calls 30
IP Nodes 42
Switches/Routers 32
Plugin 7
Licensing 20

Q

QDC Export Monitor 14
QDC Monitor 13
QoS Templates
Adding 50
Configuration 50
Deleting 50
DLS 50
Searching 50

R

Remove
Switches/Routers 32
Report 33
Call 33
Call Monitor 35
Call Search 34
Consecutive Packets Over Time 35
Cumulative Call 34
Cumulative Consecutive Packets 35
Execution Plans 37
Results 38
Scheduling 36
SLA Monitor 36
Templates 37
Topology Monitor 36

Results 29
Overviews 29
Reports 33
Switches/Routers 31
R-Value 12

S

Scheduling 36
Execution Plans 37
Results 38
Templates 37
Search
DLS Endpoints 49
Events 44
IP Nodes 41
Networks 40
QoS Templates 50
Switches/Routers 32
Server 5
SLA Call Monitor 15
SLA Monitor Report 36
SLAs 26
Software Integration 45
Switch/Router
Dashboard 31
Switches/Routers
Adding 32
Configuration 32
Details 32
Ping 32
Removing 32
Results 31
Searching 32

T

Templates 37
Terminology 5
Thresholds 25
Topology-based Call Monitor 16
Topology Monitor Report 36
Trace Manager 45
Configuration 45
Integration 17
Preparation 45
Trouble Shooting 47
Trap Monitor 14
Trouble Shooting
Trace Manager 47

V

Value
Average Round Trip Delay 13
Consecutive Packet Loss 13
Jitter 13
Lost Packets Percent 13
Maximum Inter Arrival Jitter 13
MOS 12
Packet Loss 13
R-Value 12

W

Web Client 19
Configuration 19, 27
Installation 19
Start 19