A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant V11

Simple Network Management Protocol

Simple Network Management Protocol - OpenScape SNMP

Help

11/2023

A31003-H34B0-M122-01-76A9

Mitel

Notices

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

Trademarks

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

Contents

1 Overview

This overview chapter contains the following sections:

1.1 Introduction to SNMP

SNMP is part of the internet protocol suite, as defined by the Internet Engineering Task Force (IETF). It stands for “Simple Network Management Protocol”. It is used to provide a standard interface for monitoring and configuring network resources.

SNMP is based on the manager / agent model. Agents maintain management information databases, which can be read and possibly written by managers. This kind of communication is always initiated by the managers. Agents are also capable of sending notification events, so-called “traps”, to the managers asynchronously. Apart from these operations, the SNMP protocol definition also includes the data model and the network protocol.

OpenScape 4000 Assistant SNMP agent supports Simple Network Management Protocol Version 1 (SNMPv1) and Version 3 (SNMPv3). OpenScape 4000 host systems support SNMPv3 only.

About SNMPv3

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides security models and security levels. A security model is an authentication strategy which is set up for a user and the group in which the user resides.

A security level is the permitted level of security within a security model.

A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

SNMPv3 objects are distinguished by the following properties:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy is what SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users

Related Topics

Management Information Base (MIB)

Data types

Operations

Traps

Communities

1.2 Management Information Base (MIB)

The MIB specifies the management data of a device (or a subsystem thereof). The MIB defines a hierarchical namespace containing object identifiers (OIDs). This hierarchy starts from a standard “iso” root, and the higher levels correspond to organizations, while the lower levels mirror the data on the subsystem. All nodes can be identified by a unique name, or a path, which describes its exact place in the hierarchy. The path is built up from the IDs of the nodes on the different levels, separated by dots (“.”). The MIB database contains two types of nodes:

- inner nodes, which only define the structure and are not accessible to the managers directly
- leaf[1] nodes, which hold the agent data and can be read and possibly written by the managers.

Some examples for OIDs

Path	Unique name
1	iso
1.3	org
1.3.6	dod
1.3.6.1	internet
1.3.6.1.2	mgmt
1.3.6.1.2.1	MIB-2
1.3.6.1.2.1.1	system
1.3.6.1.2.1.1.5	sysName

MIBs are specified in descriptor files, written in ASN.1. These are required by the managers to properly display the agent data.

Related Topics

Introduction to SNMP

Data types

Operations

Traps

Communities

1. A MIB can be depicted as a tree graph, with only the leaves containing data.

1.3 Data types

SNMP defines data types for managed objects. These are also defined in the MIB descriptor files (see above). Apart from simple data types, such as *Integer32*, *Counter32*, and *OCTET STRING*, most network-related concepts such as the MAC address and IP address also have predefined types (*MacAddress* and *IpAddress*, respectively). The MIB designer can also define new types based on the predefined ones.

There are two special data types that need further explanation:

1. INTEGER enumerations are used if an OID can only have a limited number of values. In this case, it is not uncommon to define names for the otherwise numerical values, for better readability. If the MIB descriptor file has not been imported to the manager, the value can only be displayed as a number.
2. SEQUENCEs are the SNMP equivalents of database tables. A SEQUENCE node (usually called xxxTable) has a single child (xxxEntry), whose children are the fields (columns) in the table. Each table has index fields, whose values are concatenated to the OIDs of the fields: this is how SNMP differentiates rows.

An example of tables

If the OIDs are as shown below:

exampleTable	1.3.6.1.4.9999.3
exampleEntry	1.3.6.1.4.9999.3.1
exampleIndexNumber	1.3.6.1.4.9999.3.1.1
exampleDataValue	1.3.6.1.4.9999.3.1.2

Table 1

and there are two lines in the table:

exampleIndexNumber	exampleDataValue
1	10
5	20

Table 2

then the OIDS and values of the fields in the two rows will be as follows:

First row	1.3.6.1.4.9999.3.1.1.1	1
	1.3.6.1.4.9999.3.1.2.1	10
Second row	1.3.6.1.4.9999.3.1.1.5	5
	1.3.6.1.4.9999.3.1.2.5	20

Table 3

Please note that this is not the order the data will be returned from the agent when automatic discovery is used. Since the OIDs of the cells in column one are smaller than those in column two (the row identifier is placed at the end of the OID, after the column number), the table will be returned column-by-column, not row-by-row, as it would be expected.

For further information on tables and other data types, please refer to a more detailed introduction to SNMP. Wikipedia.org is a good starting point.

Related Topics

Introduction to SNMP

Management Information Base (MIB)

Operations

Traps

Communities

1.4 Operations

A manager can issue three operations to the agent:

1. **GET**: queries the value of the managed object for a given OID.
2. **GET-NEXT**: returns the value of the first managed object whose OID is greater than the OID provided. OIDs are ordered by comparing the numbers on each level. This operation can be used for discovering an unknown MIB: GET-NEXT is called until there are no objects left.
3. **SET**: the manager can overwrite the value of the object with the given OID. However, while all objects are readable in a MIB, usually only a few of them are changeable.

Related Topics

Introduction to SNMP

Management Information Base (MIB)

Data types

Traps

Communities

1.5 Traps

Traps are thrown by the agent on a predefined condition. If a manager receives a trap, it can decide to issue GET requests for the agent to determine what has happened. Typical uses of traps include error-reporting and registering a device for the network.

Related Topics

Introduction to SNMP

Management Information Base (MIB)

Data types

Operations

Communities

1.6 Communities

Communities serve as a form of authentication in SNMPv1 and SNMPv2c. They bear a slight resemblance to passwords and must be provided with each request. However, SNMPv1 and SNMPv2c do not support encryption. Furthermore, communities are usually well-known and are often used to specify which part of the MIB the manager wants to access, since it is possible to specify different community names for different parts of the MIB.

SNMPv1 and SNMPv2c are not secure protocols. SNMPv3 is a secure protocol, and it is supported by the Assistant SNMP feature.

Related Topics

Introduction to SNMP

Management Information Base (MIB)

Data types

Operations

Traps

2 Feature Description

The Assistant SNMP feature adds SNMP manageability to the OpenScape 4000 Assistant and all connected host systems like SoftGate, STMIX and OS Enterprise Gateway. It provides the following functions:

- The MIB that is available on the OpenScape 4000 Manager is now available on the Assistant as well.
- An Assistant-specific MIB provides access to
  - data in the OpenScape/HiPath Inventory Management
  - LAN card and Host data from System Management (SysM)
  - data of WAML connections use of LEGK
  - supplementary information about boards and IPDA connections
  - In addition, a trap is thrown whenever a fault or an alarm is reported by the switch

---

NOTE: As of OpenScape 4000 V7 R2, there are 2 new supported MIBs: app4K.mib and MIB2.

In this chapter, you find the following sections:

2.1 Installation and Control

Once enabled, the AFR 3 device is used for the configuration of Automatic Fault Reporting of RMX (Fxxxx and alarm messages).

NOTE: If AFR 3 is already in use by another application, SNMP will overwrite the previous settings.

By default, no trap destinations or community strings are defined.

The SNMP feature can be controlled with the following applications:

- SNMP can be enabled or disabled in the **Application Control** application.
- The **SNMP Configurator** can be used:
  - for the configuration of SNMP on all connected hosts on the Assistant and
  - to specify the trap endpoints,
  - to download the MIB definition files (see SNMP Control: Configure Deletion of Error Messages and Fault Messages on page 39),
  - to enable and disable the sending of traps for particular fault message numbers (see Trap Filter: Enable and Disable Trap Filter on page 42),
  - to configure the MIB2 parameters and filters on all connected hosts,
  - to reset the RMX/Assistant alarms.
- The “**Alarm Configurator**” can be used to specify which alarms should be assigned to specific trunks, and their precise activation conditions. These settings also affect the SNMP trap generation, since they are created from the activated alarms.

Related Topics

Activation

Usage

In the background …

SNMP Discovery

Requirements

2.2 Activation

The SNMP feature is disabled by default. Before it can be used, it must be activated in the Application Control.

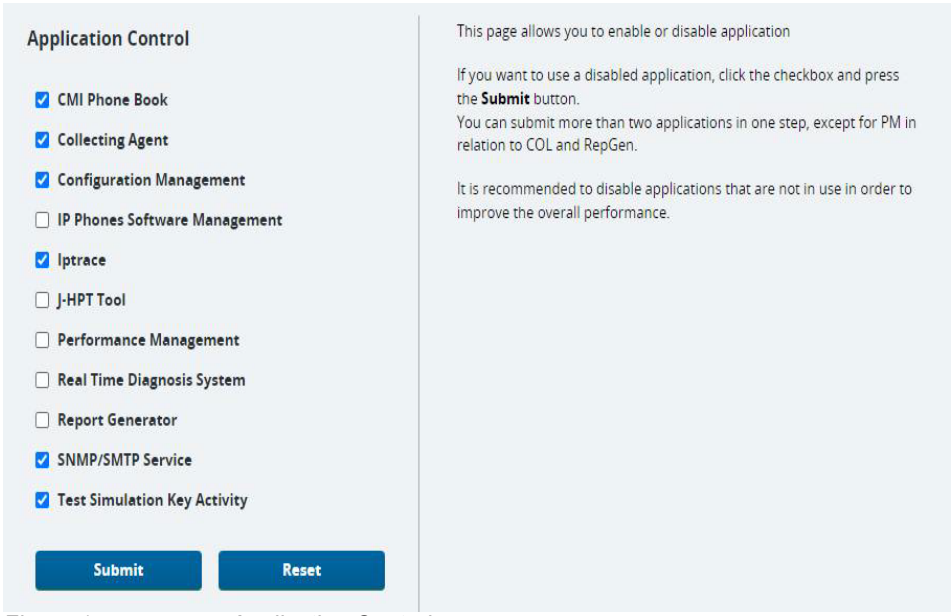

Figure 1 Application Control

Related Topics

Installation and Control

Usage

In the background …

SNMP Discovery

Requirements

2.3 Usage

The usage and the available information depends on the MIB used.

- “Hicom MIB” – the MIB that was ported from the “Manager”:

  This MIB contains information about the switch. The following information can be obtained:

  – board data

  – trunking

  – RMX software version and patches

  – the current and foreign systems

  – alarm configurations

  – list of alarms and errors

  As of V7R2, the hicomMIB is extended by two tables which are filled during the system discovery.

  – hostBaseSystems – table with IP addresses of the 4K host systems (nodeA, nodeB, quorum nodes) that belong to the particular Assistant.

  – hostAPsystems – table with IP addresses and LTUs of Softgate/ SurvivableSoftgate/AP-E host systems that belong to the particular Assistant

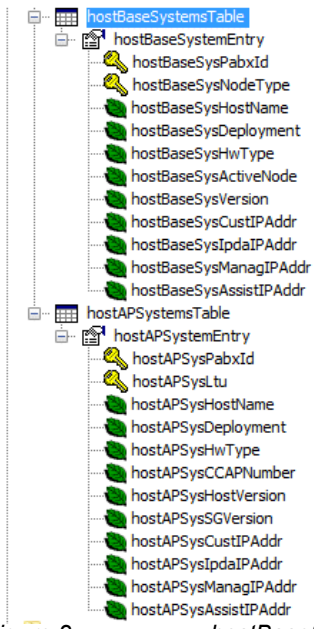

Figure 2 hostBaseSystemsTable / hostAPSystemsTable

The table of host systems (hostBaseSystems) includes the following fields:

- hostBaseSysPabxId - Unique identifier of the 4K system usable on the 4K Manager. On the Assistant this is always 1
- hostBaseSysNodeType - Type of the 4K host node. For simplex only nodeA is used. In case of duplex on the host, the node can be nodeA, nodeB or quorum node (nodeQ)
- hostBaseSysHostName - HostName of the node
- hostBaseSysDeployment - Identification of the deployment type as text, e.g. DuplexNode, SimplexNode ...
- hostBaseSysHWType - Identification of the hardware type, e.g. VM, DSCXLv2, OSA500i, ...
- hostBaseSysActiveNode - Usable in duplex mode for the identification of the activeNode and standby nodes in time.
- hostBaseSysVersion - Version of the 4K host system.
- hostBaseSysCustIPAddr - Customer Lan IP address of the appliance.
- hostBaseSysIpdaIPAddr - IPDA LAN IP address of the appliance.
- hostBaseSysManagIPAddr - Management Lan IP address of the appliance.
- hostBaseSysAssistIPAddr - The appliances associated with the assistant IP address.

The table of sofware based APs (hostAPsystems) includes the following fields:

- hostAPSysPabxId - Unique identifier of the 4K system usable on the 4K Manager. On the Assistant this is always 1
- hostAPSysLtu - LTU (Line Trunk Unit) number of the access point.
- hostAPSysHostName - HostName of the node.
- hostAPSysDeployment - Identification of the deployment type as text, .e.g StandaloneSG, SurvivableSG, ...
- hostAPSysHwType - Identification of the hardware type as text. e.g. DSCXLv2, OSA500i, VM ...
- hostAPSysCCAPNumber - APE/SurvivableSG access point number.
- hostAPSysHostVersion - Platform release version.
- hostAPSysSGVersion - SoftGate release version.
- hostAPSysCustIPAddr - Customer Lan IP address of the appliance.
- hostAPSysIpdaIPAddr - IPDA LAN IP address of the appliance.

  - hostAPSysManagIPAddr - Management Lan IP address of the appliance.
  - hostAPSysAssistIPAddr - The appliances associated with the assistant IP address.

However, this information is not available immediately. A so-called discovery process has to be started first.

NOTE: The original MIB in the OpenScape 4000 Manager could store the information of several Assistants. To maintain compatibility with the Manager, the MIB has not been modified. This means that most data will be available in tables, even tough some of the tables will have only one row – the data of the Assistant. Consequently, all SNMP Get and Set requests have to be indexed with the PabxId field in the tables. On the Assistant, the PabxId is always 1 (one).

- "HIM MIB" – the Assistant specific MIB:

  This MIB contains OpenScape 4000 Assistant-specific information. It includes

  - all data in the OpenScape/HiPath Inventory Management
  - network interfaces:
    - LAN cards
    - hosts
    - WAML connections
- auxiliary information for data in the Hicom MIB: boards and IPDA connections.
- The new app4K MIB is integrated in the OpenScape Fault Management so that the alarms are displayed accordingly. Host-related alarms are mapped to the corresponding IP nodes in the OpenScape Fault Management.

Related Topics

Installation and Control

In the background …

Activation

SNMP Discovery

Requirements

2.4 In the background …

The SNMP service on the Assistant consists of several “agents” that provide information to the user. There are two types of agents: the master agent and subagents. The master agent accepts queries and forwards them to the appropriate subagents, returns the answers from the subagents, and sends traps.

The subagents provide the system data. They are as follows:

Agent	Description	Implemented MIB branch
MIB-2	implements the standard MIB-2, as in RFC 1213	MIB-2
System	provides basic data about the system	hicomSystem
Alarm	responsible for alarm handling; throws traps if the status of an alarm changes	hicomAlarms, hicomAlConf
Error	handles system errors; throws traps if an error occurs	hicomErrors
Topology	contains data on trunking	hicomTopo
Hardware	contains hardware data	hicomHard
Software	data on APS version and RMX patches	hicomSoft
Discovery	manages discovery for the software, hardware, topology and alarm agents; see below	hicomDiscov
HIM	implements the whole HIM MIB	himRegMIB

Related Topics

Installation and Control

Activation

Usage

SNMP Discovery

Requirements

2.5 SNMP Discovery

Discovery is the process that loads the switch data from the RMX database to the OpenScape 4000 Assistant's database so that the user receives the most current data via SNMP queries.

The discovery process can be started for the whole OpenScape 4000 Assistant's MIB, in which case it is called a Master discovery, or only for specific data in the MIB.

Discovery for specific data can be:

- **HicomAlConf discovery**: loads information about the errors and alarms on the Hicom to the OpenScape 4000 Assistant's database
- **hicomSoft discovery**: loads information about the software configuration of the Hicom to the OpenScape 4000 Assistant's database
- **hicomHard discovery**: loads information about hardware of the Hicom to the OpenScape 4000 Assistant's database
- **hicomTopo discovery**: loads information about the topology of the Hicom to the OpenScape 4000 Assistant's database
- **HIM discovery**: loads the most current information for the HIM MIB to the OpenScape 4000 Assistant's database.

NOTE: During the HIM discovery, not all HIM MIB information may be updated. To obtain the most current data in the HIM MIB, you have to start an upload in the CM first and then the HIM discovery process.
During the Master discovery, the HIM MIB-specific data is not updated.

The status of the discoveries is handled by the following MIB node names:

- **hicomAlConfDiscovStatus**: status of the HicomAlConf discovery
- **hicomSoftDiscovStatus**: status of the HicomSoft discovery
- **hicomHWDiscovStatus**: status of the HicomHard discovery
- **hicomTopoDiscovStatus**: status of the hicomTopo discovery
- **himDiscovStatus**: status of the HIM discovery
- **hicomDiscovStatus**: status of the Master discovery

A specific discovery process can by started by setting the appropriate status to a value of 3 (busy).

For example, if the user wants to obtain the most current data on the Hicom's hardware in the MIB, he or she has to start the hicomHard discovery by sending the SNMP Set request to the hicomHWDiscovStatus OID with value 3 (busy).

When the discovery status is finished, the status value is 1 (done). This means that the discovery is not running. If the value of the status is 2 (error), it means something went wrong during the discovery, and so the most current data was not uploaded to the Assistant's database.

The specific discovery process can be stopped by setting the status value to 6 (kill). In this case, no current data is loaded to the Assistant's database, and the status of the specific discovery is set to 2 (error).

If the user wants to start the Master discovery process, he or she has to set the **hicomDiscovStatus** to a value of 13 (masterBusy) by an SNMP Set request. If the Master Discovery is finished successfully, the status is set to 11 (MasterDone). If an error occurs during the Master Discovery process, the status is set to 12 (MasterError).

NOTE: When setting the discovery values, a ".1" has to be appended to the end of the OID.
So if the hicomHWDiscovStatus, OID 1.3.6.1.4.1.231.7.2.1.6.5.2.1.3 is set, the ID that should be used is 1.3.6.1.4.1.231.7.2.1.6.5.2.1.3.1. This is because the discovery tables are also indexed with the PabxId field (see "Usage", page 2-16).

Related Topics

Installation and Control

Activation

Usage

In the background …

Requirements

2.6 Requirements

A network management system or an SNMP client that is capable of receiving traps is required to take advantage of the error and alarm reporting.

A client PC with a MIB browser is required to query data from the Assistant SNMP or to start discoveries.

Related Topics

Installation and Control

Activation

Usage

In the background …

SNMP Discovery

3 SNMP Configurator

SNMP Configurator allows you to configure SNMPv1 and SNMPv3 on OpenScape 4000 Assistant and SNMPv3 on all connected hosts like SoftGate, STMIX and OS Enterprise Gateway.

Accessing the SNMP Configurator Page

On the OpenScape 4000 Assistant start page:

- Select **Diagnostics -> Fault Management**, and click **SNMP Configurator**.

  The SNMP Configurator page is displayed.

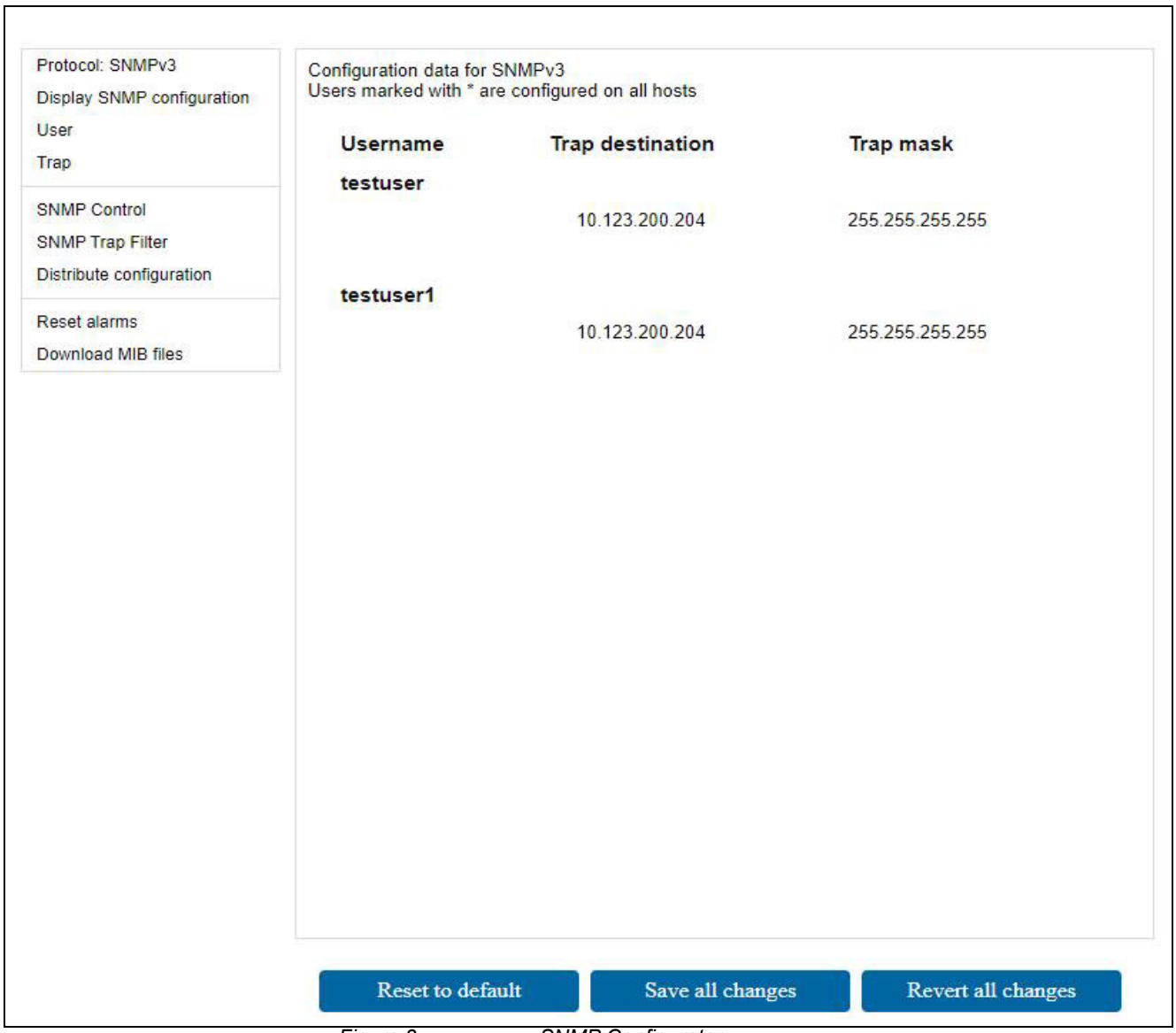

Figure 3 SNMP Configurator

The SNMP Configurator page allows you to

- specify the Network Management Systems (NMS) that are to receive traps sent by the SNMP agents
- add or remove communities (SNMPv1)
- add or remove users and edit passwords (SNMPv3)
- configure deletion intervals of error records and discovery periods for RMX fault messages from the database to free up hard disk space.
- configure a trap filter and distribute it to all hosts
- reset all alarms (set to off status) raised on the RMX or the Assistant
- activate/deactivate host keep-alive traps on all hosts
- setup MIB2 parameters
- download the MIB definition files

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.1 User interface

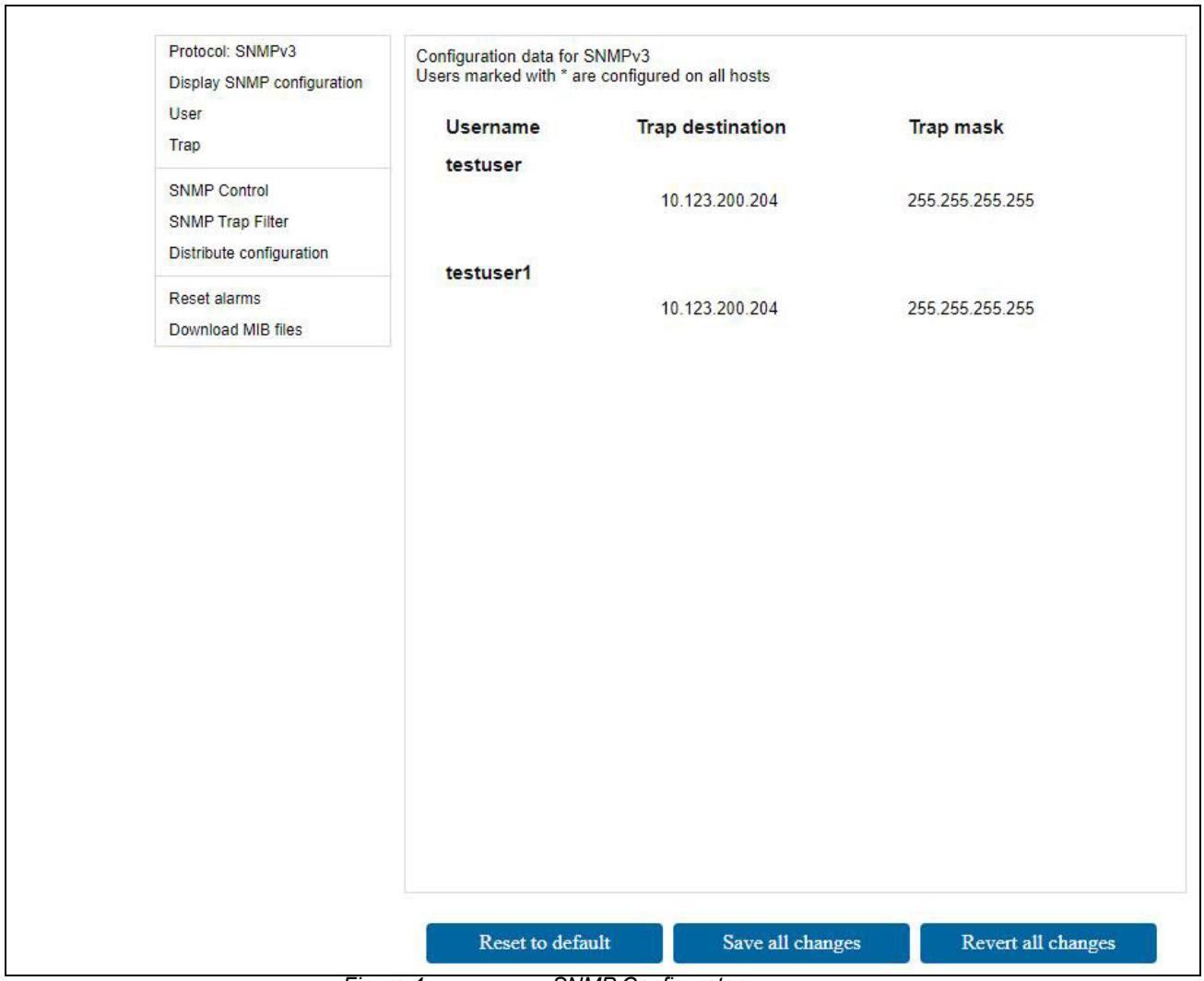

Figure 4 SNMP Configurator

The left hand pane of the page contains the **menu box**, in the right hand pane configuration data are displayed and all configuration actions are done.

Menu Box (left hand pane)

You can choose from different actions in the menu box, which are in summary:

- The upper menu items in the menu box are related to configuring SNMPv1 and SNMPv3 respectively.
  - **Display configuration**
    Configuration data from the currently chosen SNMP version (SNMPv1 or SNMPv3) are displayed.

- **Protocol: SNMPv3** or **Protocol: SNMPv1**
  This is a toggle entry for selecting actions related to SNMPv1 or to SNMPv3 respectively. Which one of both menu entries is available, depends on the currently chosen SNMP version.
- **User** or **Community**
  This is a toggle entry. Which one of both is available depends on the currently chosen SNMP version (**Community** for SNMPv1, **User** for SNMPv3).
- **Trap**
  This includes all actions, which can be configured with SNMP entity traps. There is also the option to remove a trap address from a user/community string.

- The menu items in the lower part of the menu box are common for both SNMP versions.
  - **SNMP Control**
    Using the SNMP Control functions, you can activate the sending of keep-alive traps from all hosts, activate/deactivate the sending of error traps from the entire 4K area, and setup the location and contact person for hosts of the active/standby/quorum nodes. The contact and location will be used for the MIB2 sysLocation and sysContact settings..
  - **Trap Filter**
    You can use the SNMP Configurator -> Trap Filter -> Host System Events feature for the definition of the trap filter for host systems.
  - **Distribute Configuration**
    You can use the SNMP Configurator -> Distribute Configuration feature for saving configuration changes to the host system platform and all connected appliances like SoftGate, STMIX and OS Enterprise Gateway.

    NOTE: HG3500 and HG3575 can not participate by this Distribution.

    The following configuration changes can be saved to connected hosts:
    - SNMPv3 setting
    - Host filter setting
    - SNMP control settings
  - **Reset Alarms**
    Using the SNMP Configurator -> Reset Alarms function you can reset all alarms (set to off status) raised on the RMX or the Assistant.
  - **Download MIB files**
    This allows to download MIB definition files.

Buttons (right hand pane)

The configuration settings done with the SNMP Configurator can be modified with the buttons in the right hand pane:

- **Reset to default**:
  This resets configuration of SNMPv1 and SNMPv3 and sets up default, clear configuration with no users or community strings.
- **Save all changes**:
  This saves all changes made to configuration of SNMPv1 and SNMPv3.
- **Revert changes**:
  This reverts all changes made to configuration to the state of the last save or reset.

As long as there are unsaved changes in the right hand configuration pane, a message is displayed over these buttons, informing that the changes should be saved or reverted.

Related Topics

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.2 Display SNMPv1/SNMPv3 Configuration

To display data of the current SNMPv1 or SNMPv3 configuration:

- Choose the desired SNMP version **Protocol: SNMPv1** or **Protocol: SNMPv3** in the menu box.
- Click **Display Configuration**.

  Depending on the selection of SNMPv1 or SNMPv3, the configuration of the corresponding SNMP protocol is displayed.

Related Topics

User interface

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.2.1 Add/Remove a Community in SNMPv1 Configuration

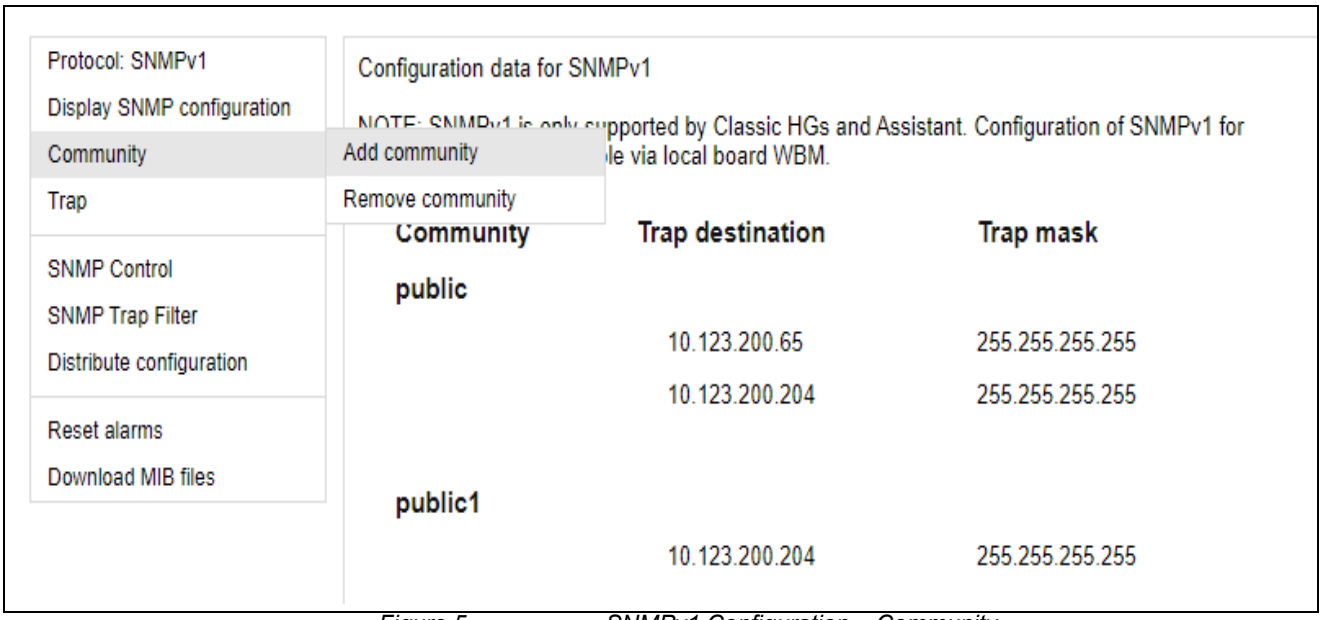

Figure 5 SNMPv1 Configuration – Community

Menu Box

The menu box for SNMPv1 configuration contains the following entries:

- **Community**
  This menu option includes all actions, which can be done with SNMPv1 entity community string. It allows to Add a Community String or to Remove a Community string.

  and

- **Trap**
  See "Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration" on page 36.

Add a Community String

- Choose **Protocol: SNMPv1**.
- Click on **Community** and select **Add community** in menu box.
- Enter the community string.
- Click **Add**.

- Click **Save all changes**.

NOTE: The value of the community string can not be null, the string must not be empty. You also cannot enter a string, which already exists in the configuration both for SNMPv1 and SNMPv3.

After successful addition, you are redirected to default screen, which shows data.

Remove a Community string

Removing community string means that also all trap destination addresses connected to this entity will be removed.

- Choose **Protocol: SNMPv1**.
- Click on **Remove community** in menu box in **Community section**.

  All community strings present in configuration are displayed.
- Delete the chosen community string by clicking red **X** button close to it.
- Click **Save all changes**.

Related Topic

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

3.2.2 Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

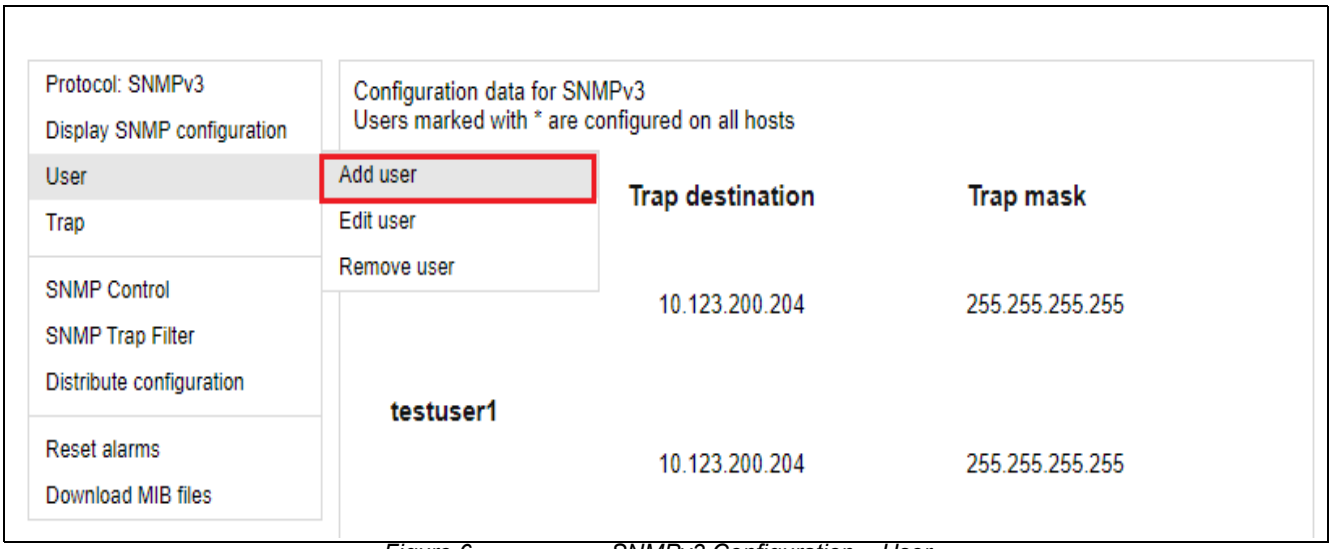

Figure 6 SNMPv3 Configuration – User

Menu Box

The menu box for specific SNMPv3 configurations contains the following entries:

- **User**
  This menu option includes all operations, which user can do with SNMPv3 entity user.
  It allows them to **Add** a new user entry, **Edit** passwords or **Remove** user entries.

  and

- **Trap:**
  See "Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration" on page 36.

Add a new User Entry

- Choose **Protocol: SNMPv3**.
- Click on **Add user** in menu box in **User** section.
- Enter in the new **username**, **authentication password** and **privacy password**.

NOTE: These are mandatory fields and must not be empty.

Password must be at least 8 characters.

- If you select the **Read only user** checkbox, the user will only have read-only access to the MIBs.
- If you select the **Configure on all hosts** checkbox, the user will configured with the same settings on all connected hosts during the distribution of the configuration.
- Click **Add**.

After successful adding, you are redirected to the default screen, which shows the new data.

Change Passwords

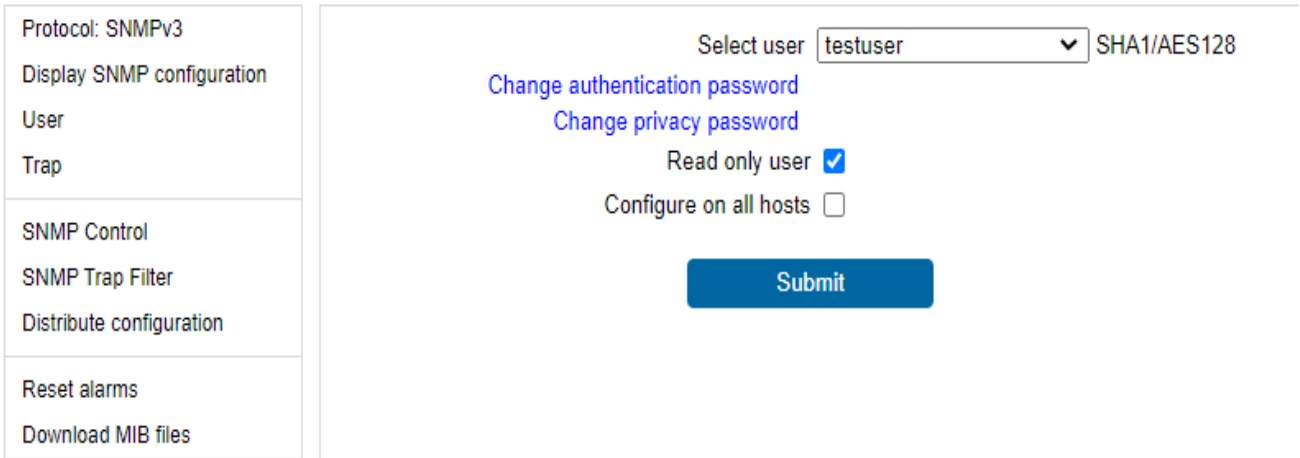

Figure 7 SNMPv3 Configuration - Change Password

- Choose **Protocol: SNMPv3**.
- Click **Edit user** in menu box in **User** section.

- Choose a user from the **Select user** dropdown list.
- Now you can choose to change the following passwords:
  - authentication password
  - privacy password
- Enter the currently valid password and repeat the new one.
- Click **Submit**.

Remove a User Entry

- Choose **Protocol: SNMPv3**.
- Click **Remove user** in menu box in **User** section.

  All user entries are displayed which are existing in the configuration.
- Delete the chosen user entry by clicking red **X** button close to it.
- Click **Save all changes**.

Related Topic

Add/Remove a Community in SNMPv1 Configuration

3.3 Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

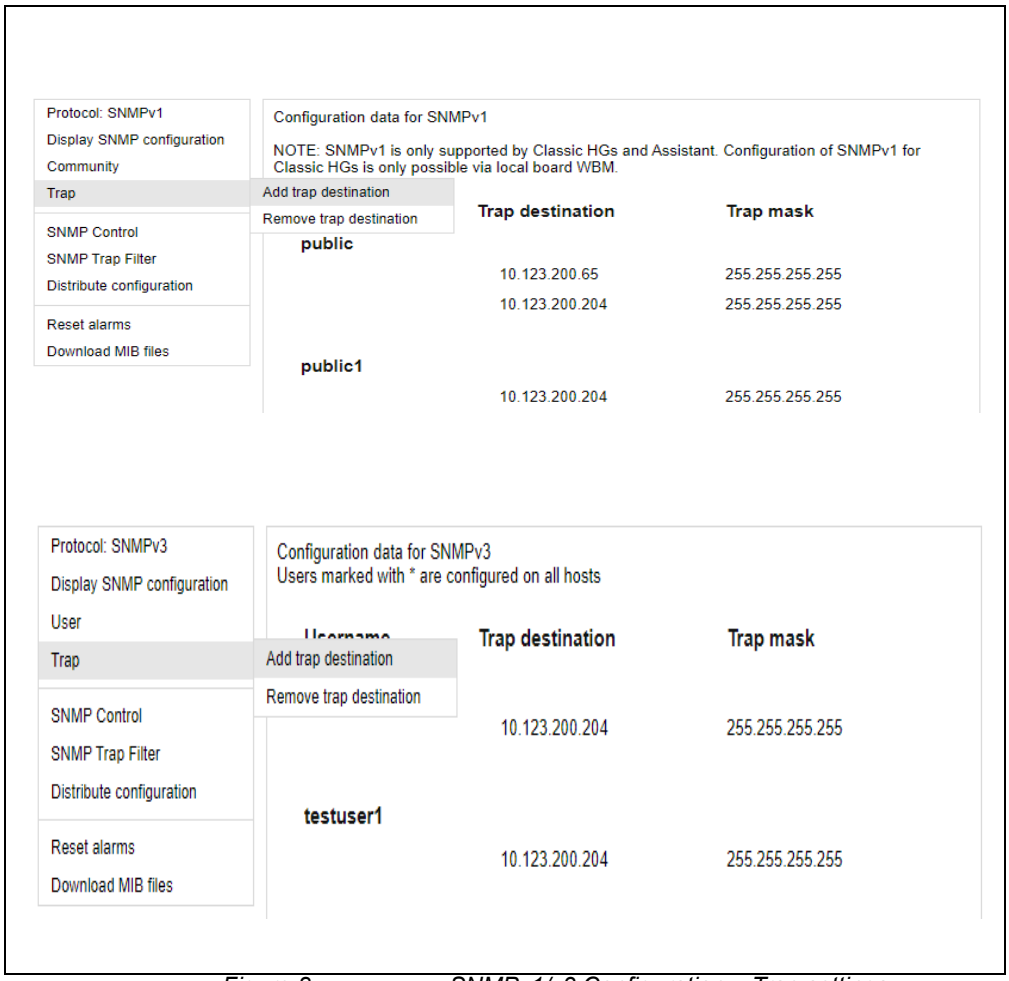

Figure 8 SNMPv1/v3 Configuration – Trap settings

With the configuration of trap destinations you set the IP address of machine, to which the traps from SNMP agents will be sent and connect it to the user/ community string.

Menu Box

The common menu box both for SNMPv1 and SNMPv3 configurations contains the following entries:

- **Add trap destination**:
  Set the IP address of the machine of the management system to which the traps from SNMP agents will be sent and connect it to the user/community string.
- **Remove trap**:
  Removes a trap address from user/community string.

Add a New Trap Destination

- Choose the desired SNMP version **Protocol: SNMPv1** or **Protocol: SNMPv3** in the menu box
- Click **Add trap destination** in the sub menu.

  You can choose a community (for SNMPv1) or a user (for SNMPv3), which you would like to add a trap destination address to.

  Name: A name can be added to each entry. This name is not used anywhere in the system; it is only included as a memory aid.

  SNMP Version: the version of the SNMP protocol used for the traps.
- Enter a trap destination IP address and a trap mask for that IP. Default trap mask is set to 255.255.255.255, which describes exactly 1 machine.

NOTE: If an IP address or a trap mask is not valid, you cannot submit any further data.

- Click **Save all changes**.

NOTE: You cannot add a new trap destination if no community strings (SNMPv1) or users (SNMPv3) exist. An error message will be displayed and you will be redirected to the page where you can add a new entry.

Remove a Trap destination

- Choose the desired SNMP version **Protocol: SNMPv1** or **Protocol: SNMPv3** in the menu box
- Click **Remove trap destination** in the sub menu.

  Communities (SNMPv1) or users (SNMPv3) with their trap destination addresses will be displayed.
- Delete the chosen trap destination by clicking on red **X** button close to it.
- Click **Save all changes**.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.4 SNMP Control: Configure Deletion of Error Messages and Fault Messages

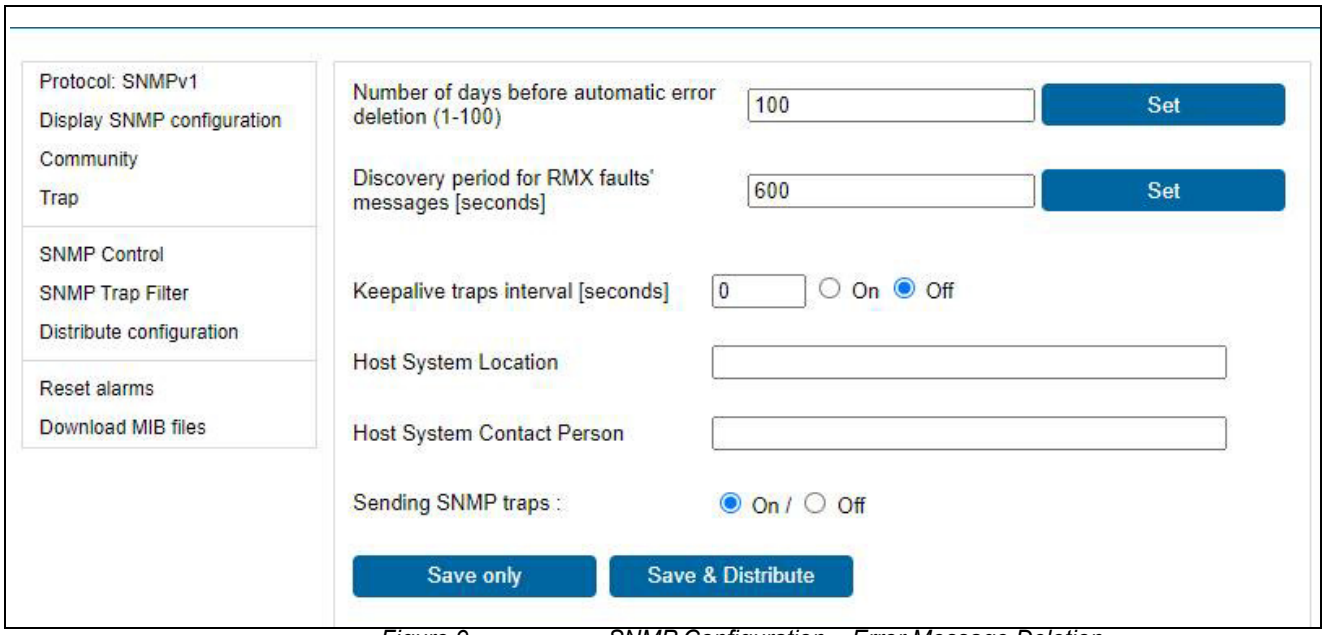

Figure 9 SNMP Configuration – Error Message Deletion

With the **SNMP Control** both for SNMPv1 and SNMPv3 you can

- set the error deletion interval within an interval from 1 to 100 days
- set the discovery period for RMX faults' messages
- set the keepalive traps interval
- identify the host system location
- identify the host system contact person
- set whether or not SNMP traps will be sent

Set the error deletion interval

- In the input field **Number of days before automatic error deletion (1-100)** enter the desired number of days before the errors should be deleted.
- Click **Set**.
- Click **Save only or Save & Distribute**.

Set the discovery period for RMX faults' messages

RMX error faults are polled by default every 10 minutes and error traps are generated if new faults are discovered. You can change this value in case that the delay of received traps on your NMS or on your trap receiver is too long for your needs. Minimum poll value is 30 minutes.

Changing this value will restart erroragt, which causes sending the last 100 fault traps on RMX in hista file.

- In the input field **Discovery period for RMX faults' messages (seconds)** enter the desired discovery period; default is 10 minutes, minimum value is 30 seconds.
- Click **Set**.
- Click **Save only or Save & Distribute**.

Set the keepalive traps interval

Some of the NMS are using so called keepalive traps to monitor whether the system is up and running. A keepalive trap is only an information message; if it is not received by the NMS in the specified time interval, the NMS reports a critical error on the monitored node.

By default the keepalive traps are deactivated (**Off**). The time intervals for sending keep-alive traps can be configured centrally here.

- In the input field **Keepalive traps interval (seconds)** enter the desired number of seconds defining the interval between the sending of keepalive traps.
- Select **On**.
- Click **Save only or Save & Distribute**.

Specify the host system location

Enter the physical location of this node (e.g. *Hessen, Frankfurt am Main, L12/ Nord*).

This location information will be used for all traps sent from Assistant, Platform, CSTA, and integrated SoftGates on central host deployments. On Standalone or Survivable SoftGates, Enterprise Gateways or STMIX boards the location information from AMO UCSU will be used instead.

Specify the host system contact person

Enter a textual identification of the contact person for this managed node, together with information on how to contact this person (e.g. *Doe, John, +1 202 xxxxxxx*).

Switching the sending of SNMP traps On/Off

Here you can activate (On) or deactivate (Off) switch the sending of SNMP traps.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.5 Trap Filter: Enable and Disable Trap Filter

3.5.1 Trap Filter: RMX Fault Messages

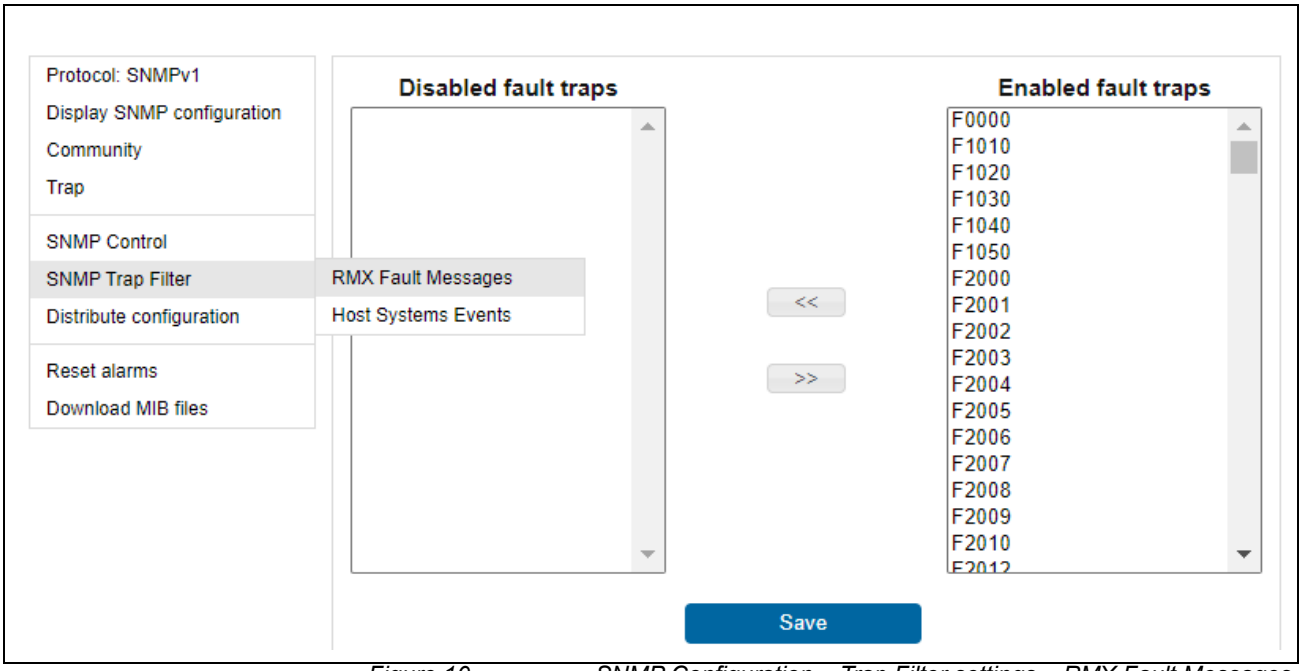

Figure 10 SNMP Configuration – Trap Filter settings – RMX Fault Messages

In the **Trap Filter** – **RMX Fault Messages** section you can enable or disable fault traps from RMX both for SNMPv1 and SNMPv3.

Two columns with fault traps are displayed:

- **Disabled fault traps** (column on the left hand side):
  Displays a list of all fault numbers for which trap sending is disabled.
- **Enabled fault traps** (column on the right hand side):
  Displays a list of all fault numbers for which trap sending is enabled.

Enable Fault Traps

- Select one or multiple traps from the **Disabled fault traps** column.
- Click the **<<** button between the columns.
- The selected traps are moved to the **Enabled fault traps** column.
- Click **Save**.
- Click **Save all changes**.

Disable Fault Traps

- Select one or multiple traps from the **Enabled fault traps** column.
- Click the **>>** button between the columns.
- The selected traps are moved to the **Disabled fault traps** column.
- Click **Save**.
- Click **Save all changes**.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.5.2 Trap Filter: Host System Events

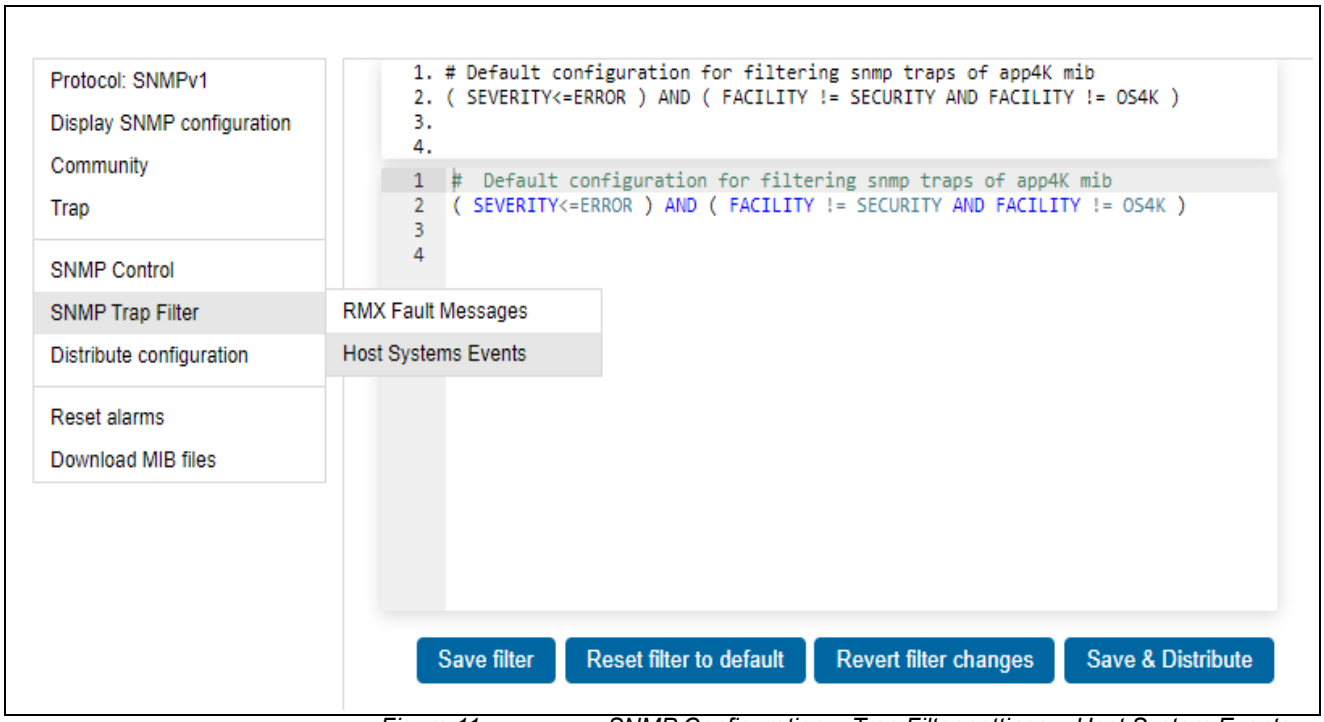

Figure 11 SNMP Configuration – Trap Filter settings – Host System Events

In the **Trap Filter – Host System Events** section you can set the trap filters for all connected hosts.

You can define rules for filtering traps on the host systems. The definition is written in a multiline text area using expressions that must have the correct syntax. The syntax is verified so you cannot save a filter with syntax errors.

This configuration can contain:

- Comments – all texts from character # to the end of line. A comment can start at the beginning of a line or in the middle.
- Conditions on separate lines

Using these conditions you can specify what has to be filtered out (which traps should not be sent by the host systems). So each trap meeting the condition set from this file is filtered out.

Conditions can contain:

- keywords: SEVERITY, FACILITY, OID, MSG, TRAP_ID
- operators {=, !=, <, >, <=, >=} for SEVERITY
- operators {=, !=} for FACILITY, OID, TRAP_ID
- operators {MATCH, NOT MATCH} for MSG

- logical operators AND, OR
- brackets, can be nested ((... OR ...) AND ...)

Keyword options:

- valid SEVERITY values are: {emergency, alert, critical, error, warning, notice, info, debug}
- valid FACILITY values are: {os4k, kernel, user, mail, daemon, security, syslog}, where os4k are traps generated by os4k processes.
- valid OID values are strings inside the "" which can contain a * character at the end. This character stands for an arbitrary count of any characters.
- valid MSG values are strings inside the "" which can contain special characters for regular expressions. Here the regex syntax is supported.
- valid TRAP_ID values are strings inside the "" marks. Special characters (wildcards) are not supported. The TRAP_ID value is compared with predefined values and must match one of them. If it does not match any, a predefined TRAP ID error is logged in the parsing file.

NOTE: The difference between the wildcards in OID and MSG is that in an OID string you use the character *; for the same meaning in an MSG string you must use .* because . stands for an arbitrary character and * for its repetition.

Other rules:

- All keywords, logical operators and facility and severity values are case insensitive.
- Strings in quotation marks are case sensitive.
- Priority of AND, OR is the same, so use brackets if you need to determine priority.
- Brackets can be nested several times, e.g. ((...)...(...)...(...(...)...)).
- Logical operation between lines is OR.

Correct examples of configuration file:

```
(SEVERITY < Error) AND (FACILITY = OS4K)
SEVERITY < INFO
FACILITY = MAIL OR FACILITY = SYSLOG
OID = "154.121.45.74.1.1.2.3.*"
MSG MATCH "Message 123.*"
MSG NOT MATCH ".*temperature.*"
TRAP_ID = "tooHighTemperatureOfBoard"   # trap with given ID
must exist of course
```

Incorrect usage (each line contains some error):

undefined operation <> and undefined binary minus

```
(SEVERITY <> ERROR OR FACILITY - USER)
```

for FACILITY only operators = and != are allowed

```
(FACILITY > USER)
```

compare operator cannot be used twice for one severity / facility

```
(ALERT > SEVERITY > NOTICE)
```

wrong order, first the keyword SEVERITY must be used and it is compared to its value,

correct is (SEVERITY > NOTICE)

```
(NOTICE < SEVERITY)
```

unsupported operation for OID

```
OID > "127.5.5.4.1"
```

character * cannot be inside of string. Must be at the end.

```
OID = "154.2.1.54.7.8.4.*.1.2.1"
```

missing quotation marks.

```
MSG MATCH 1234:
```

character * cannot be interpreted as wild card.

You cannot expect wildcard behaviour for TRAP_ID.

```
TRAP_ID = "highTemperature*"
```

When the GUI of the Trap Filter is opened, the last saved filter is displayed on top.

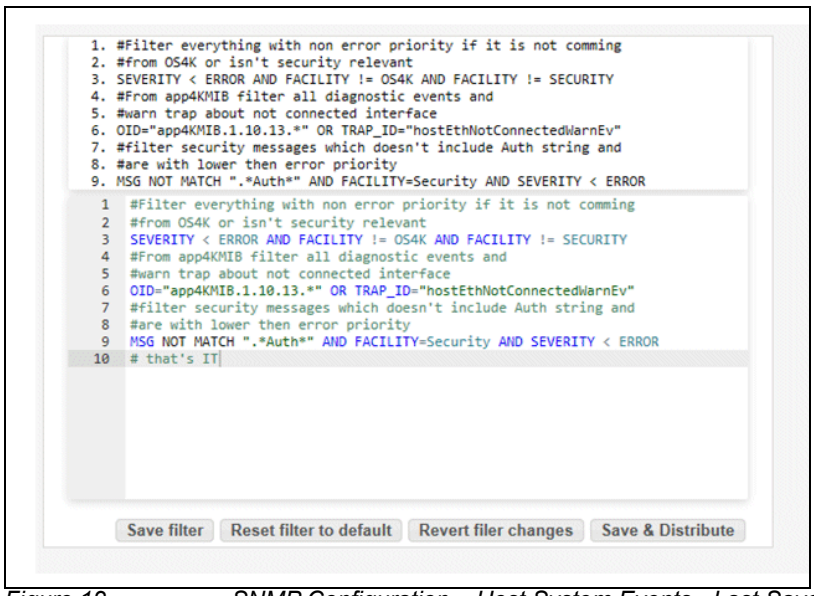

Figure 12 SNMP Configuration – Host System Events - Last Saved Filter Example

Action buttons description:

- **Save filter** – The filter is stored and text from the editable area is copied to the top.
- **Reset filter to default** – You can reset the filter to the default configuration predefined during the OS4k installation.
- **Revert file changes** – The last saved configuration is restored.
- **Save & Distribute** - The filter is stored and you are redirected to the Distribute Configuration page where you can distribute it into all hosts in the 4K area.

Before the distribution starts, you can specify which data should be distributed (**Distribution to hosts**).

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.6 Configuration of SNMPv3 on all connected hosts

Using the Assistant SNMP Configurator, you can select whether the particular SNMPv3 user definition with the related trap destination should be configured on all connected appliances like SoftGate, STMIX and OS Enterprise Gateway.

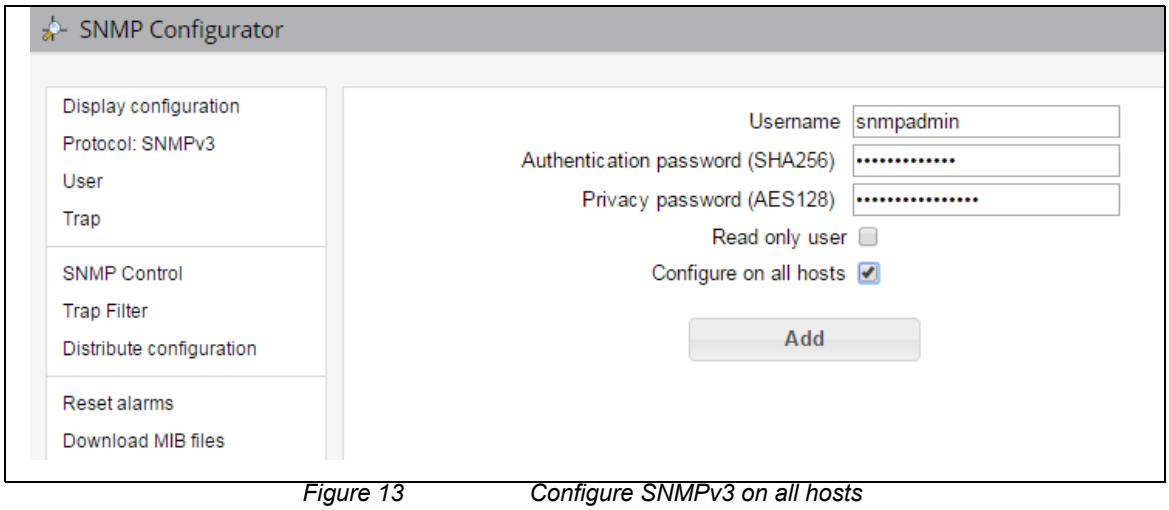

Figure 13 Configure SNMPv3 on all hosts

NOTE: Username is an alphanumeric entry without spaces or special characters.
Authentication password uses SHA256 digest algorithm. Privacy password uses AES128 cipher.

During the distribution of the configuration, this user (including the trap destinations assigned to this user) will be configured as a read-only user on all host systems.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.7 Distribution to hosts

Using the Assistant SNMP Configurator, you can select whether configuration changes shall be saved on all connected hosts like SoftGate, STMIX and OS Enterprise Gateway.

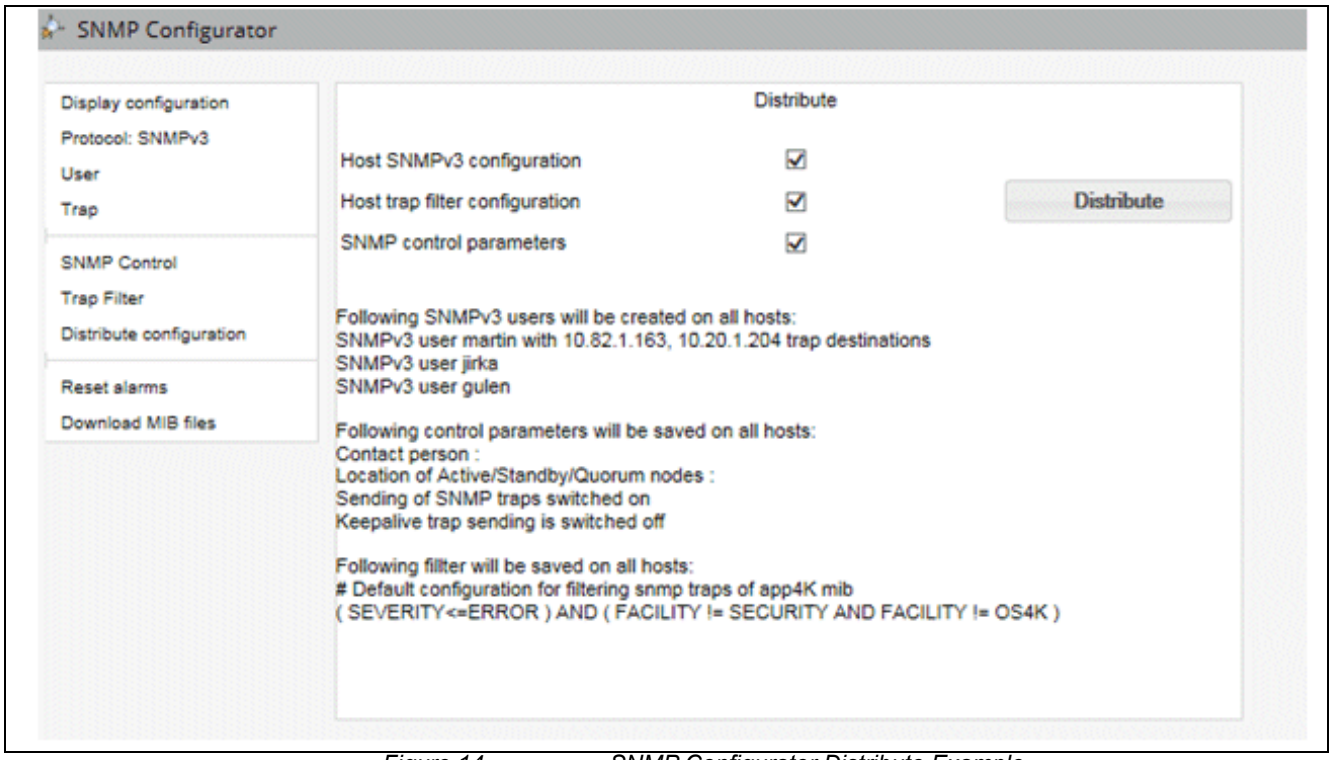

Figure 14 SNMP Configurator Distribute Example

The following configuration changes can be saved to connected hosts:

- SNMPv3 setting
- Host filter setting
- SNMP control settings

Before the distribution starts, you can also select which configuration should be distributed to the connected hosts.

Clicking on the Distribute button will start the distribution process; this may take several seconds. During the distribution, all data selected are configured and saved on all nodes in the 4K area (except on IPDA-based APE systems).

NOTE: It is mandatory to have the NGS IP address setup on for the distribution to AP, APEs and STMIX boards.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Reset all alarms on RMX or Assistant

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.8 Reset all alarms on RMX or Assistant

Using the Assistant SNMP Configurator, you can reset all alarms (set to off status) raised on the RMX or the Assistant.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

View and Download MIB files

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.9 View and Download MIB files

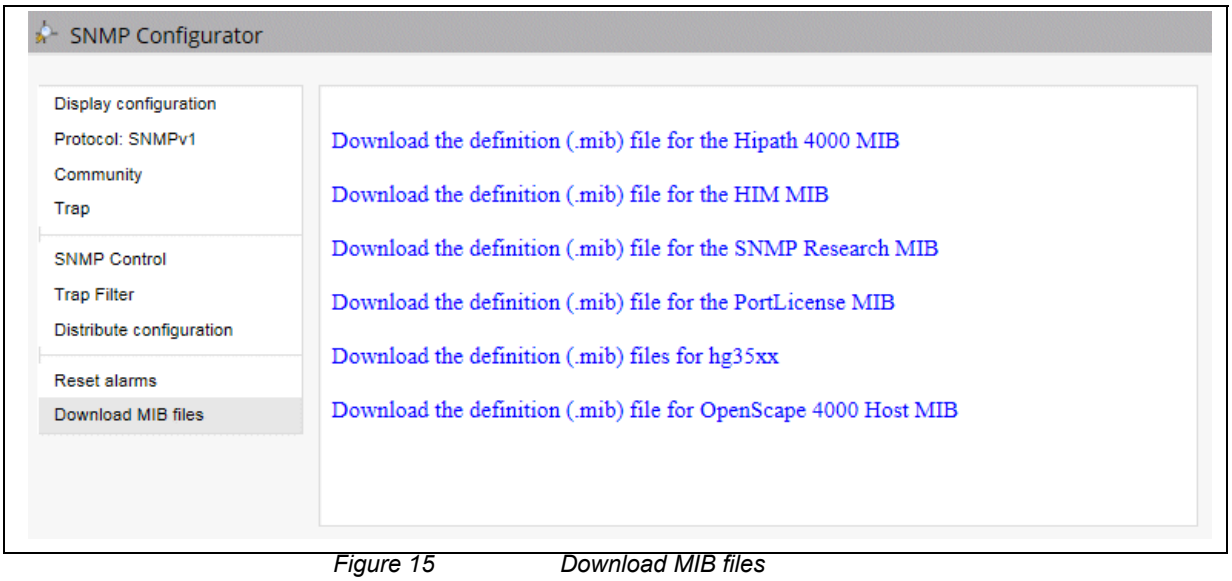

Figure 15 Download MIB files

To view and download MIB files (.mib) that describe MIB structures:

- Click **Download MIB files** in the menu box.

  Next you can select to view the definition files for:

  – OpenScape 4000 MIB,

  – OpenScape/HiPath Inventory Management MIB or

  – SNMP Research MIB

  – Host 4000 MIB.

  A new window containing the MIB description appears.

The MIB files can then be saved to the hard disk and later imported into a network management system.

NOTE: It is possible that Internet Explorer may save the files in html format, i.e., with html formatting. This makes the file unintelligible for MIB Browsers. To avoid this, use either Mozilla Firefox or save the file as text and rename it to “*.mib” if necessary.

Related Topics

User interface

Display SNMPv1/SNMPv3 Configuration

Add/Remove a Community in SNMPv1 Configuration

Add and Remove User with Trap Destination in SNMPv3 Configuration, Edit Passwords

Trap: Add and Remove Trap Destinations in SNMPv1/SNMPv3 Configuration

SNMP Control: Configure Deletion of Error Messages and Fault Messages

Trap Filter: Enable and Disable Trap Filter

Configuration of SNMPv3 on all connected hosts

Distribution to hosts

Reset all alarms on RMX or Assistant

Management of OpenScape 4000 Systems via app4K.mib

Monitoring via SNMP get

3.10 Management of OpenScape 4000 Systems via app4K.mib

The Host 4000 MIB (ASN-1 syntax notation) is structured as follows:

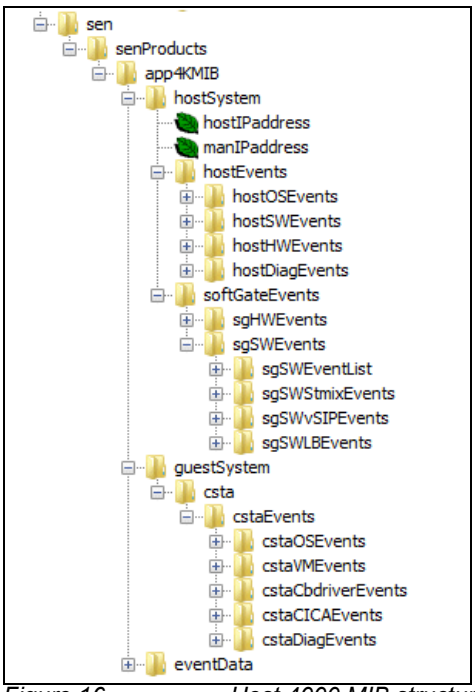

Figure 16 Host 4000 MIB structure

- hostSystem - Host system of OpenScape 4000 appliance
  - hostEvents - Group of events produced by applications and monitoring processes running on appliance of OpenScape 4000 host system
    - hostOSEvents - Events which can be produced by Operating System of OpenScape 4000 host system
    - hostSWEvents - Events from host software applications and deamons
    - hostHWEvents - Hardware events reported by the host system
    - hostDiagEvents - Events used for diagnostic purposes
  - softGateEvents - Group of events produced by SoftGate and Enterprise Gateway system and relevant hardware
    - sgHWEvents - Hardware events produced by Softgate or Enterprise Gateway system running on host.
    - sgSWEvents - Software events produced by SoftGate or Enterprise Gateway running on host.
  - stmixEvents - Group of events produced by STMIX boards
    - stmixHWEvents - Hardware events produced by STMIX boards

    - stmixSWEvents - Software events produced by STMIX boards*
- guestSystem - Operating system or application hosted on OpenScape 4000 host appliance
    - csta - CSTA guest system running on OpenScape4000 appliance
        - cstaEvents - Events produced by CSTA
        - cstaOSEvents - Events from Operating System of CSTA
        - cstaVMEvents - Events related to VM of CSTA
        - cstaCbdriverEvents - Events related to CSTA cbdriver software
        - cstaCICAEvents - CICA related events
        - cstaDiagEvents - CSTA diagnostic events

Additionally each event/trap will include following data as variable bindings:

- evSeverity - severity (priority) level
- sysDescr – system description from host’s MIB2
- sysName – system name from host’s MIB2
- sysLocation – system location from host’s MIB2
- hostIPaddress – IP address of the host which is generating the trap
- manIPaddress – clan IP address of OpenScape 4000 Assistant which is used for administration/management of SNMP setting
- eventDateTime – date and time when the event occurred
- evDescr - detailed text of the event message

3.10.1 Severity Level (evSeverity)

The host 4000 MIB uses the severity levels from syslog-ng (RFC 5424):

Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	Alert	alert	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	Critical	crit	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	Error	err (error)	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	Warning	warning (warn)	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	Notice	notice	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	Informational	info	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	Debug	debug	Debug-level messages.	Info useful to developers for debugging the application, not useful during operations.

Figure 17 Host 4000 MIB severity levels

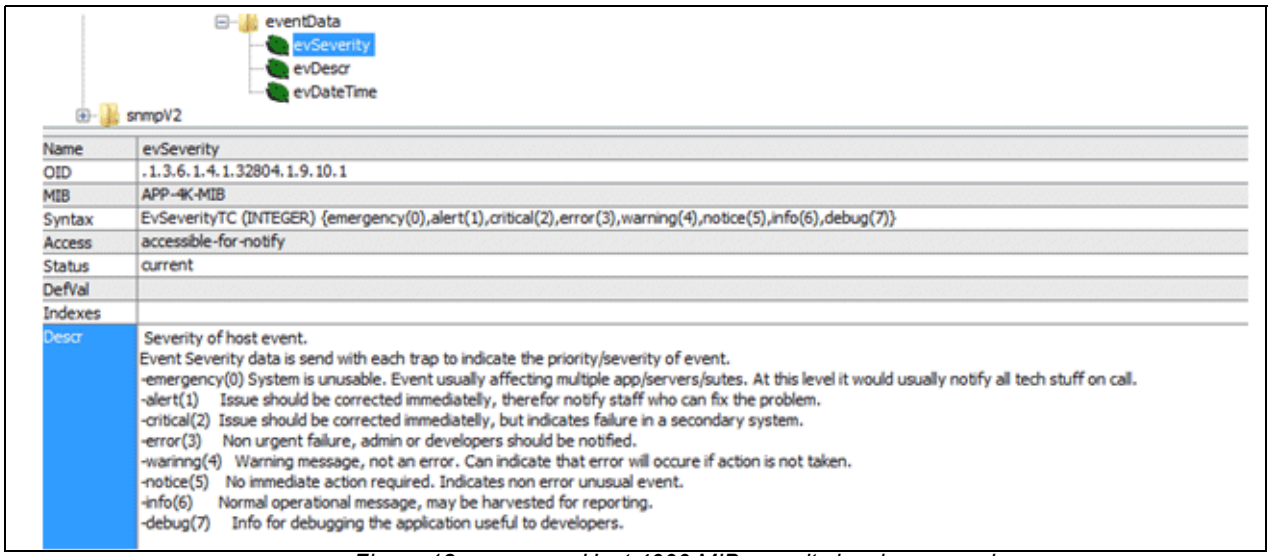

Figure 18 Host 4000 MIB severity levels - example

3.10.2 hostOSEvents

The hostOSEvents trap uses a generic trap model, i.e. it is unclear from the trap name what type of error occurred. Each trap includes an evDescr as trap variable binding; this is used to find the reason for the error. Based on the trap name, you can only detect the trap severity (priority) and facility (which OS subsystem produced the trap).

Example: This is a log from a trap receiver which caught a hostOSSecurityErrEv trap - it is clear this error was produced by the security subSystem of the operating system; however, to find out exact reason you have to check the evDecr variable binding:

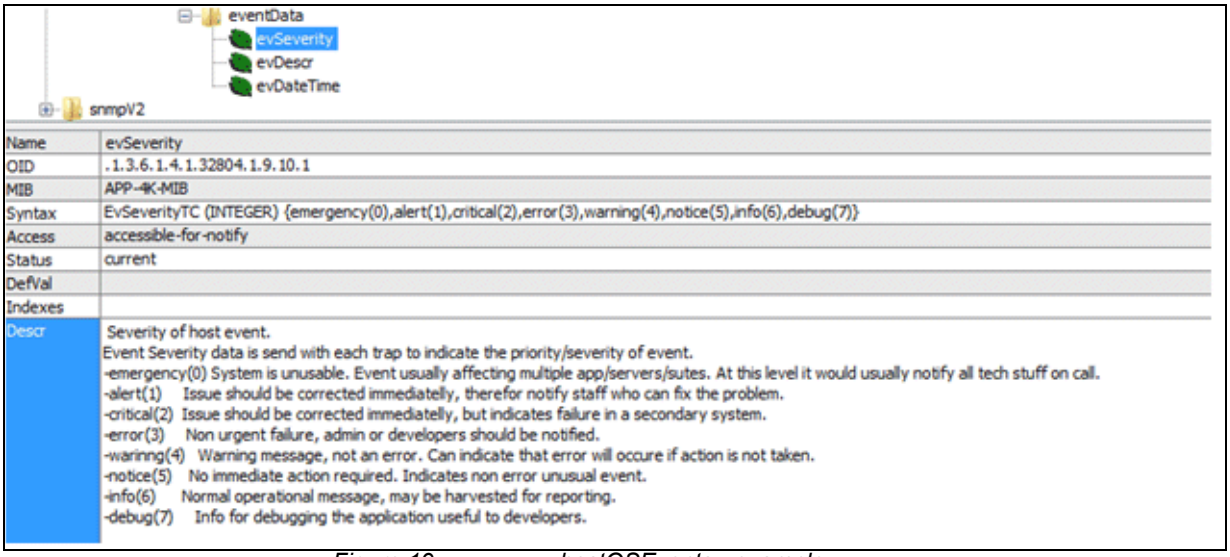

Figure 19 hostOSEvents - example

The SNMP engine is preset to send trap messages from the operating system with severity levels up to "emerg" only. Messages with lower priorities are not send as snmp traps.

The hostOSEvents includes the following trap categories:

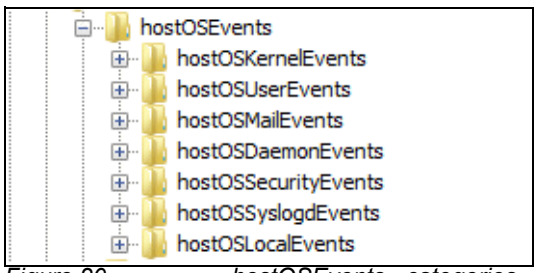

Figure 20 hostOSEvents - categories

- hostOSKernelEvents - Host operating systemkernel messages
- hostOSUserEvents - Host operating systemapplication/service messages
- hostOSMailEvents - Host operating systemmail system messages

- hostOSDaemonEvents - Messages from system daemons host operating system
- hostOSSecurityEvents - Host operating system security/authorization messages
- hostOSSyslogdEvents - Messages generated internally by syslogd of the host Operating system
- hostOSLocalEvents - Messages generated by the administrator or applications from the host operating system

3.10.3 hostSWEvents

Software-based events that may be produced by OpenScape 4000 processes/ monitoring applications running on the host include:

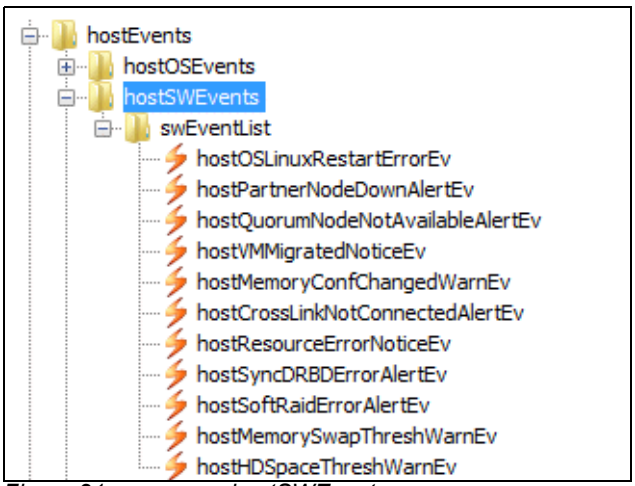

Figure 21 hostSWEvents

- hostOSLinuxRestrtErrorEv - Host operating system restart.
- hostPartnerNodeDownAlertEv - Duplex System:one node is out of service
- hostQuorumNodeNotAvailableAlertEv - Separate Duplex System:Quorum node is not available
- hostVMMigratedNoticeEv - VM was migrated via vMotion to an other physical Server
- hostMemoryConfChangedWarnEv - Memory configuration of VM was changed
- hostCrossLinkNotConnectedAlertEv - Cross-Link not connected. Check connector and duplex systems.
- hostResourceErrorNoticeEv - Error of system application, info only - check functionality of the resource

- hostSyncDRBDErrorAlertEv - DRBD Error, check duplex functionality
- hostSoftRaidErrorAlertEv - SoftRaid Error, check recovery HD generation
- hostMemorySwapThreshWarnEv - System is swapping - check RAM usage
- hostHDSpaceThreshWarnEv - Hard Drive Space - value is over threshold

3.10.4 hostHWEvents

Hardware-based events that may be produced by OpenScape 4000 processes/ monitoring applications running on the host include:

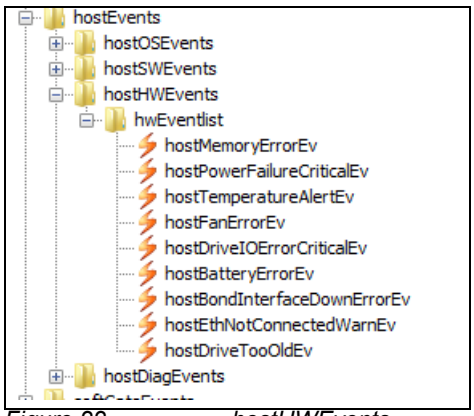

Figure 22 hostHWEvents

- hostMemoryErrorEv - Memory error, replacement of memory needed
- hostPowerFailureCriticalEv - Power failure AC/DC, replacement of PSU is needed
- hostTemperatureAlertEv - CPU temperature is over threshold
- hostFanErrorEv - FAN error - FAN needs to be replaced
- hostDriveIOErrorCriticalEv - Drive I/O Error - check HD/SSD
- hostBateryErrorEv - Replacement of BIOS battery is needed
- hostBondInterfaceDownErrorEv - Bond Interfaces:redundant interface down, check connectivity
- hostEthNotConnectedWarnEv - Ethernet Interface configured but not connected
- hostDriveTooOld - The harddisk Power-on Hours overreached standard threshold. Replace harddisk or switch to newer hardware

3.10.5 hostDiagEvents

The SNMP traps can be used as diagnostic traps. This only includes 2 traps:

Figure 23 hostDiagEvents

- hostKeepAliveInfoEv– the periodically generated trap based on keepalive interval setup. If received by NMS, this means the system is up and running.
- hostTestDebugEv– trap generated when the user clicks on the Test button in the SNMP configuration of the portal. It is only used to test whether the SNMP engine works, and it sends traps to predefined trap destinations.

3.10.6 sgHWEvents

The hardware-based events produced by the Softgate system running on the host operating system include:

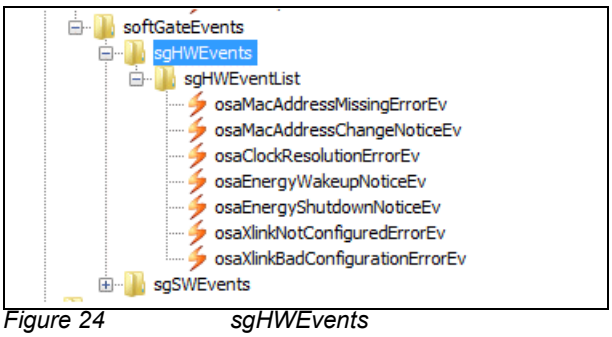

Figure 24 sgHWEvents

- osaMacAddressMissingErrorEv - Configuration Problem OSA module - MAC address missing
- osaMacAddressChangeNoticeEv - Configuration Problem OSA module - MAC address change
- osaClockResolutionErrorEv - Clock resolution too bad for OSA usage
- osaEnergyWakeupNoticeEv - Energy saving is active:start-up after wakeup
- osaEnergyShutdownNoticeEv - Energy saving is active:shutdown started
- osaXlinkNotConfiguredErrorEv - Xlink Lan-Interface is not configured
- osaXlinkBadConfigurationErrorEv - Xlink Interface is the same as the IPDA Interface e.g. xlink Lan-Interface is not configured or bad IP address

3.10.7 sgSWEvents

Software-based events produced by the SoftGate system running on the host; these are split into 4 categories:

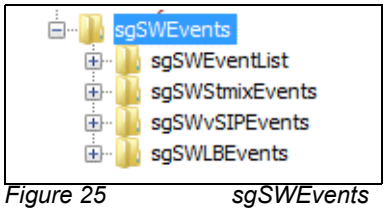

Figure 25 sgSWEvents

- sgSWLBEvents - OpenSIPS Load Balancer events
- sgSWvSIPEvents - vHG3500 (SIP) events
- sgSWStmixEvents - STMIX events
- sgSWEventList - the rest of software events produced by Softgate system

3.10.7.1 sgSWLBEvents

OpenSIPS Load Balancer events include:

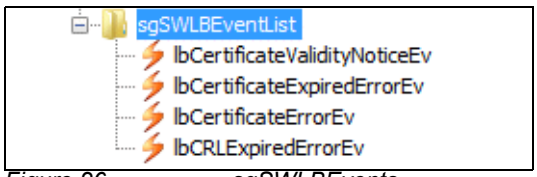

Figure 26 sgSWLBEvents

- lbCertificateValidityNoticeEv - OpenSIPS Load Balancer security active and SPE Certificate ends
- lbCertificateExpiredErrorEv - OpenSIPS Load Balancer security active and SPE Certificate expired
- lbCertificateErrorEv - OpenSIPS Load Balancer security active and there are problems with SPE certificate
- lbCRLExpiredErrorEv - OpenSIPS Load Balancer security active and CRL (certificate revocation list) expired

3.10.7.2 sgSWvSIPEvents

vHG3500 (SIP) events include:

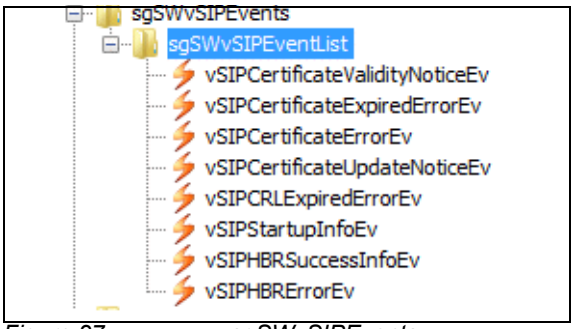

Figure 27 sgSWvSIPEvents

- vSIPCertificateValidityNoticeEv - SPE active and SPE Certificate ends
- vSIPCertificateExpiredErrorEv - SPE active and SPE Certificate expired
- vSIPCertificateErrorEv - SPE active and there are problems with SPE Certificate
- vSIPCertificateUpdateNoticeEv - SPE active and SPE Certificate has been updated
- vSIPCRLExpiredErrorEv - SPE active and CRL (certificate revocation list) expired
- vSIPStartupInfoEv - vHG3500 startup event
- vSIPHBRSuccessInfoEv - HBR ip address configured in AMO. Automatic configuration restore has finished successfully
- vSIPHBRErrorEv - HBR ip address configured in AMO, but bad credentials or bad address. Automatic configuration restore has failed

3.10.7.3 sgSWStmixEvents

STMIX events include:

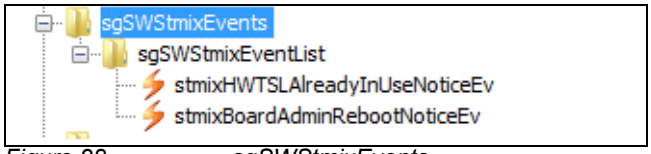

Figure 28 sgSWStmixEvents

- stmixHWTSLAlreadyInUseNoticeEv - Timeslot already in use, will be automatically cleared in SG or STMIX by RTO
- stmixBoardAdminRebootNoticeEv - Board is intentionally rebooted

3.10.7.4 sgSWEventList

The remaining software events produced by the Softgate system which are not specific for the given board types:

Figure 29 sgSWEventList

- sgNotRunningOnApplianceInfoEv - SoftGate is not running on a appliance

- sgStartupInfoEv - Info about platform, displayed during start-up. SG on VM,UNKNOWNVM,HPA500A,HPA500I,DSCXL2,COTS or unknown.
- sgKernelTooOldWarnEv - Kernel is too old for SG usage
- sgMemoryTuningInfoEv - On SoftGate HW with 4 GB memory webservice will be automatically disabled after 7 days to reduce memory consumption.
- sgLicenseValidInfoEv - Softgate License is valid info.
- sgLicenseInFailoverPeriodErrorEv - Probably licensing server CLA not reachable.
- sgLicenseLeavingFailoverPeriodNoticeEv - Licensing server CLA reachable again.
- sgLicenseInGracePeriodNoticeEv - SoftGate is in Grace Period regarding the license.
- sgLicenseInfoEv - Message from CsCM.
- sgLicenseUnavailableWarnEv - SoftGate license not available
- sgLicenseValidityNoticeEv - Period of validity of SoftGate license.
- sgCertificateValidityNoticeEv - SPE active and SPE Certificate ends.
- sgCertificateExpiredErrorEv - SPE active and SPE Certificate expired
- sgCertificateErrorEv - SPE active and there are problems with SPE Certificate
- sgCRLExpiredErrorEv - SPE active and CRL (certificate revocation list) expired
- sgLawChangeNoticeEv - Law configuration changed for Slot.
- sgNPCIreusedWarnEv - IPDA Port reuse.
- sgMOHConfigurationErrorEv - Music on hold configuration problem.
- sgShelfChangeNoticeEv - SoftGate shelf type or shelf config has changed, SoftGate will reboot automatically.
- sgTSAErrorEv - TSA Error
- sgLSDCLTimeoutCriticalEv - Restart of SoftGate due to timeout of native lsdcl.
- sgUnsupportedBoardErrorEv - Board type is not supported in SoftGate (even you can configure it in AMO).
- sgBoardAdminRebootNoticeEv - Board is intentionally rebooted
- osaIllegalVirtualizationErrorEv - Illegal virtualization for board or module.

- ngsDataNotConsistentErrorEv - NGS address is configured and NCUI payload ip from RMX boarddata differ from NGS database.

3.10.8 cstaEvents

The CSTA running inside of the active node of the OpenScape4000 also sends SNMPv3 traps from its operating system and CSTA processes.

3.10.8.1 cstaOSEvents

The cstaOSEvents trap uses a generic trap model, i.e. it is unclear from the trap name what type of error occurred. Each trap includes an evDescr as trap variable binding; this is used to find the reason for the error. Based on the trap name, you can only detect the trap severity (priority) and facility (which OS subsystem produced the trap).

The SNMP engine is preset to send traps messages from the operating system with severity levels up to "emerg" only. Messages with lower priorities are not send as snmp traps.

The cstaOSEvents includes following trap categories:

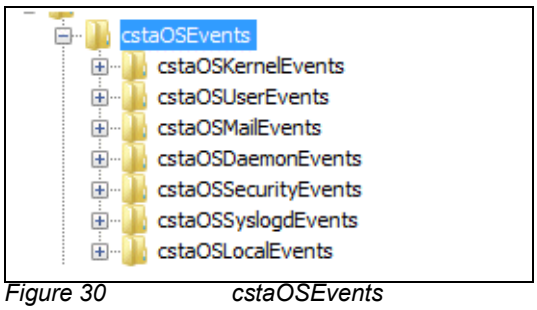

Figure 30 cstaOSEvents

- cstaOSKernelEvents - CSTA Operating system kernel messages
- cstaOSUserEvents - CSTA Operating system application/service messages
- cstaOSMailEvents - CSTA Operating system mail system messages
- cstaOSDaemonEvents - Messages from system daemons CSTA Operating system
- cstaOSSecurityEvents - CSTA Operating system security/authorization messages
- cstaOSSyslogdEvents - Messages generated internally by syslogd of the CSTA Operating system
- cstaOSLocalEvents - Messages generated by administrator or applications from CSTA Operating System

3.10.8.2 cstaVMEvents

Events related to monitoring and processes of the Virtual Machine of CSTA include:

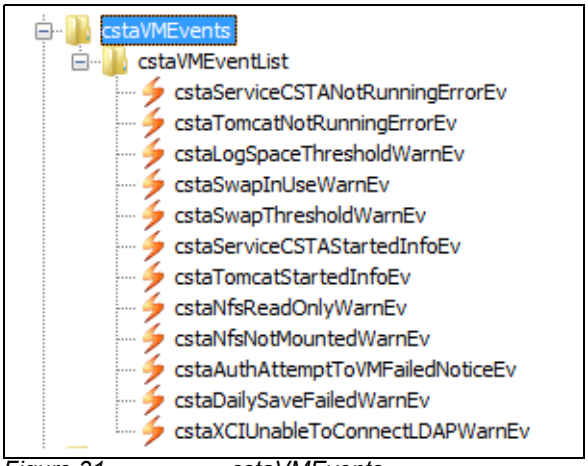

Figure 31 cstaVMEvents

- cstaServiceCSTANotRunningErrorEv - CSTA service not running
- cstaTomcatNotRunningErrorEv - Tomcat service not running
- cstaLogSpaceThresholdWarnEv - Log partition full over threshold
- cstaSwapInUseWarnEv - System is swaping
- cstaSwapThresholdWarnEv - Swap is full over threshold
- cstaServiceCSTAStartedInfoEv - CSTA service started
- cstaTomcatStartedInfoEv - Tomcat server started.
- cstaNfsReadOnlyWarnEv - NFS mounted read-only
- cstaNfsNotMountedWarnEv - NFS not mounted
- cstaAuthAttemptToVMFailedNoticeEv - Failed authentication attempt on VM
- cstaDailySaveFailedWarnEv - Daily automatic backup for reinstall failed
- cstaXCIUnableToConnectLDAPWarnEv - XCI unable to connect LDAP

3.10.8.3 cstaCdbDriverEvents

Events related to the CSTA cbdriver software include:

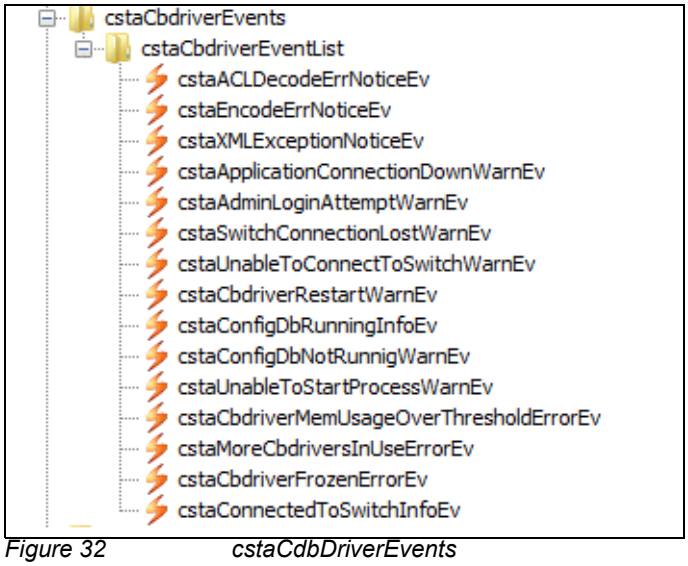

Figure 32 cstaCdbDriverEvents

- cstaACLDecodeErrNoticeEv - ACL decode error
- cstaEncodeErrNoticeEv - CSTA encode error
- cstaXMLExceptionNoticeEv - XML exception
- cstaApplicationConnectionDownWarnEv - Application connection down
- cstaAdminLoginAttemptWarnEv - Login attempt with Admin
- cstaSwitchConnectionLostWarnEv - Connection to switch lost
- cstaUnableToConnectToSwitchWarnEv - Unable to connect to switch, check AMO config
- cstaCbdriverRestartWarnEv - Cbdriver stopped with <error> - restarted
- cstaConfigDbRunningInfoEv - Configdb running
- cstaConfigDbNotRunnigWarnEv - Configdb not running
- cstaUnableToStartProcessWarnEv - Unable to start process - see evDescr of trap
- cstaCbdriverMemUsageOverThresholdErrorEv - Cbdriver uses memory over threshold, restart it
- cstaMoreCbdriversInUseErrorEv - More than N cbdrivers are in use
- cstaCbdriverFrozenErrorEv - Cbdriver process stuck in memory, kill it manually
- cstaConnectedToSwitchInfoEv - CSTA connection to switch established

3.10.8.4 cstaCICAEvents

Events related to CICA include:

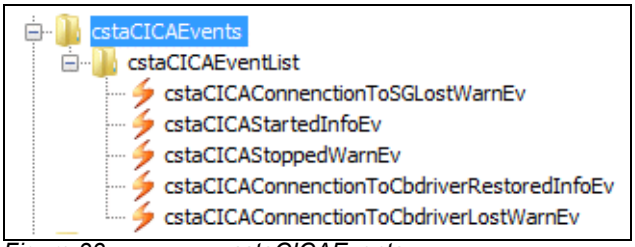

Figure 33 cstaCICAEvents

- cstaCICAConnenctionToSGLostWarnEv - CICA conenction to SG lost
- cstaCICAStartedInfoEv - CICA started
- cstaCICAStoppedWarnEv - CICA stopped
- cstaCICAConnenctionToCbdriverRestoredInfoEv - CICA conenction to cbdriver restored
- cstaCICAConnenctionToCbdriverLostWarnEv - CICA conenction to cbdriver lost

3.10.8.5 cstaDiagEvents

Events used for CSTA diagnostic purposes include:

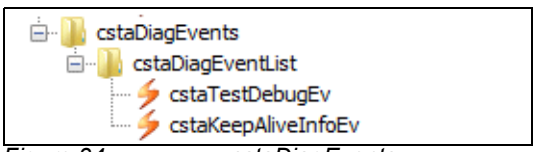

Figure 34 cstaDiagEvents

- cstaTestDebugEv - Event used for testing of SNMP functionality on the CSTA.
- cstaKeepAliveInfoEv - Keep alive event send by CSTA software

3.11 Monitoring via SNMP get

The Net-SNMP Agent active on each host of any 4K system provides a wide variety of performance information over the SNMP protocol.

In addition, the agent can be queried for a listing of the installed RPM packages on the system, a listing of currently running processes on the system, or the network configuration of the system.

This section provides a brief overview of the data available via the SNMP Host Resources MIB, USDAVIS mib (UCD-SNMP-MIB, UCD-DISKIO-MIB) and IF-MIB.

3.11.1 UCD-SNMP-MIB

The majority of the system performance data is available in the UCD SNMP MIB.

3.11.1.1 Monitoring Processors Usage

The systemStats OID provides a number of counters around processor usage:

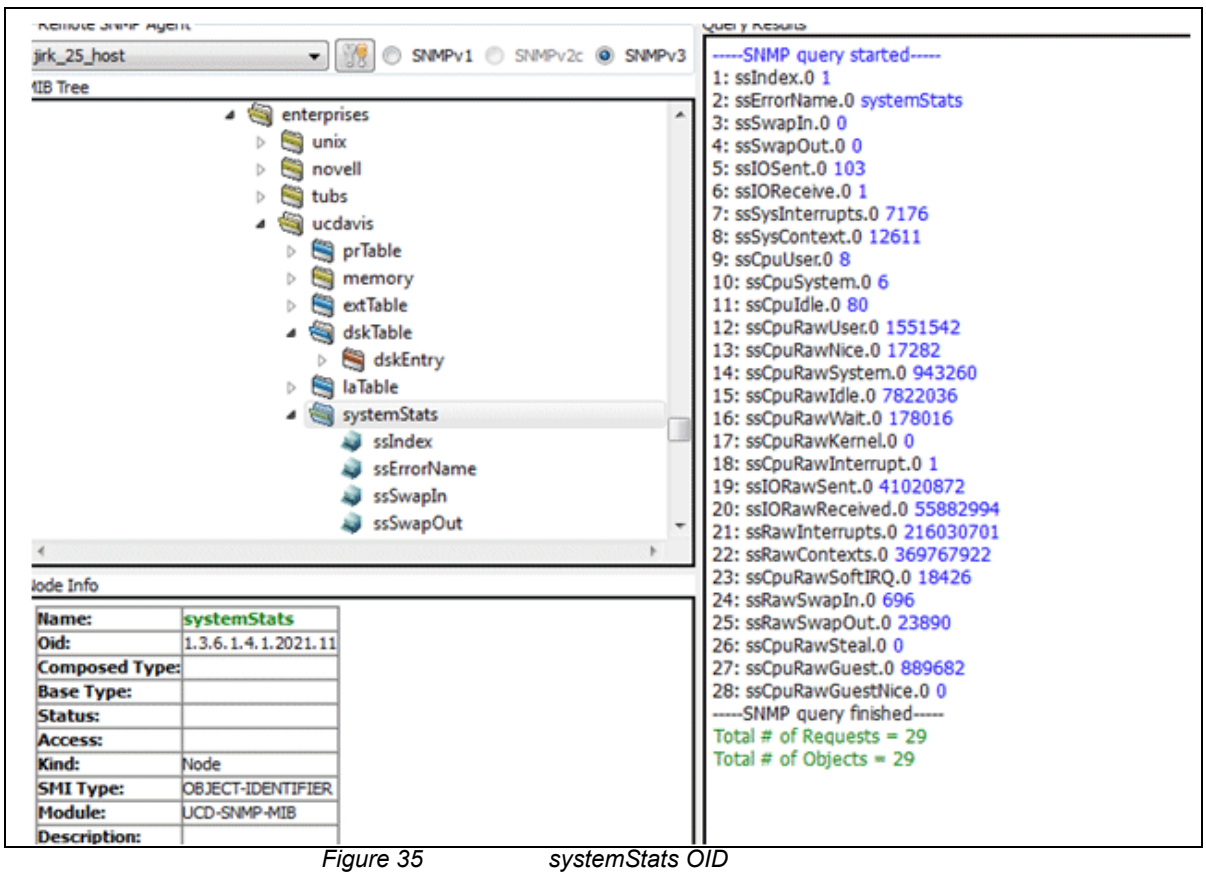

Figure 35 systemStats OID

In particular, the ssCpuRawUser, ssCpuRawSystem, ssCpuRawWait, and ssCpuRawIdle OIDs provide counters which are helpful when determining whether a system is spending most of its processor time in kernel space, user space, or I/O. ssRawSwapIn and ssRawSwapOut can be helpful when determining whether a system is suffering from memory exhaustion.

3.11.1.2 Monitoring Memory Usage

Memory information is available under the UCD-SNMP-MIB::memory OID, which provides similar data to the free command:

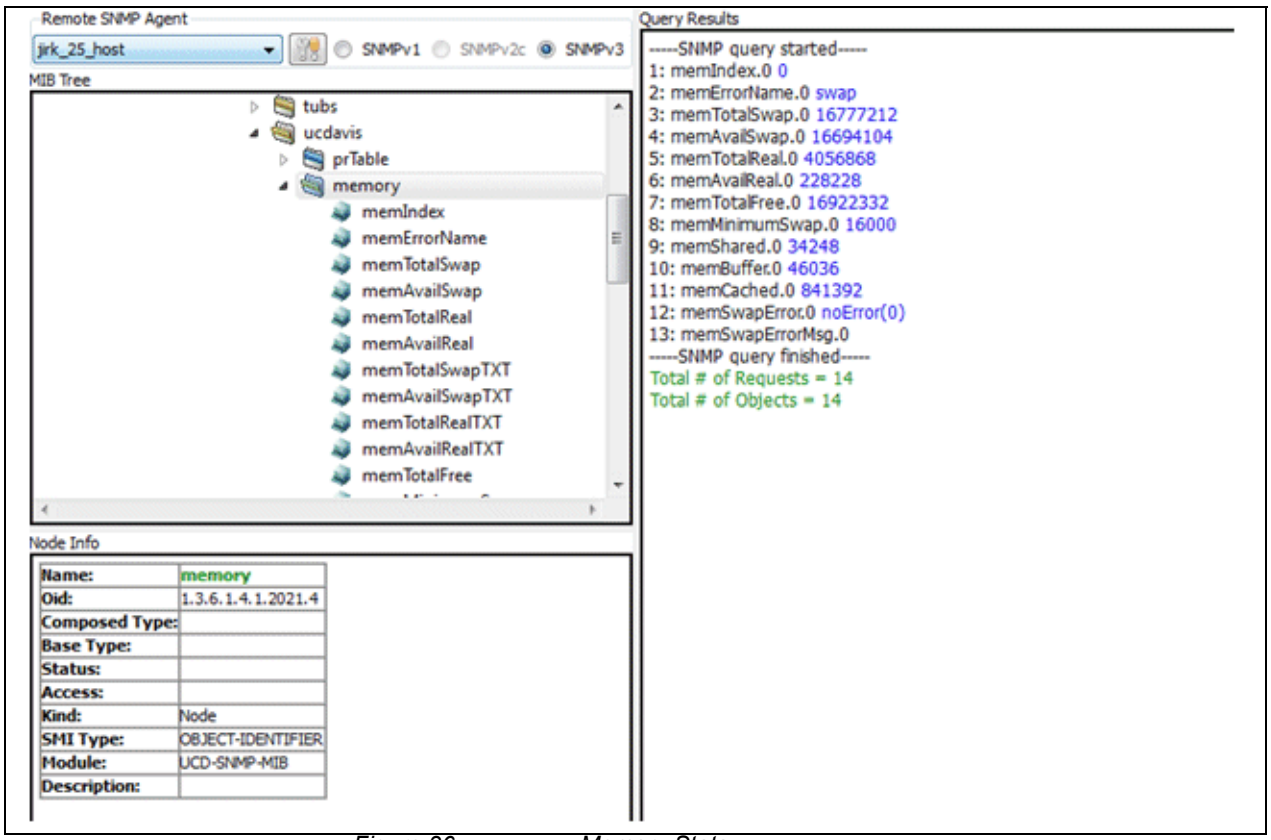

Figure 36 Memory Stats

Load averages are also available in the UCD SNMP MIB. The SNMP table UCD-SNMP-MIB::laTable has a listing of the 1, 5, and 15 minute load averages:

Instance	laIndex	laNames	laLoad	laConfig	laLoadInt	laLoadFloat	laErrorFlag	laErrMessage
1	1	Load-1	0.68	12.00	68	9F 78 04 3F 2E 14 7B .x.?..{	noError(0)	
2	2	Load-5	0.73	12.00	73	9F 78 04 3F 3A E1 48 .x.?:.H	noError(0)	
3	3	Load-15	0.69	12.00	69	9F 78 04 3F 30 A3 D7 .x.?0..	noError(0)	

Figure 37 Load Averages

3.11.2 Host Resources MIB

The Host Resources MIB included with Net-SNMP displays information about the current hardware and software configuration of a host. The following OIDs are available under that MIB:

- HOST-RESOURCES-MIB::hrSystem - contains general system information such as uptime, number of users, and number of running processes
- HOST-RESOURCES-MIB::hrStorage - contains data on memory and file system usage
- HOST-RESOURCES-MIB::hrDevices - contains a listing of all processors, network devices, and file systems
- HOST-RESOURCES-MIB::hrSWRun - contains a listing of all running processes
- HOST-RESOURCES-MIB::hrSWRunPerf - contains memory and CPU statistics on the process table from HOST-RESOURCES-MIB::hrSWRun
- HOST-RESOURCES-MIB::hrSWInstalled - contains a listing of the RPM database

3.11.2.1 General System Information (hrSystem)

The hrSystem OID of HOST-RESOURCES-MIB provides general information about the system:

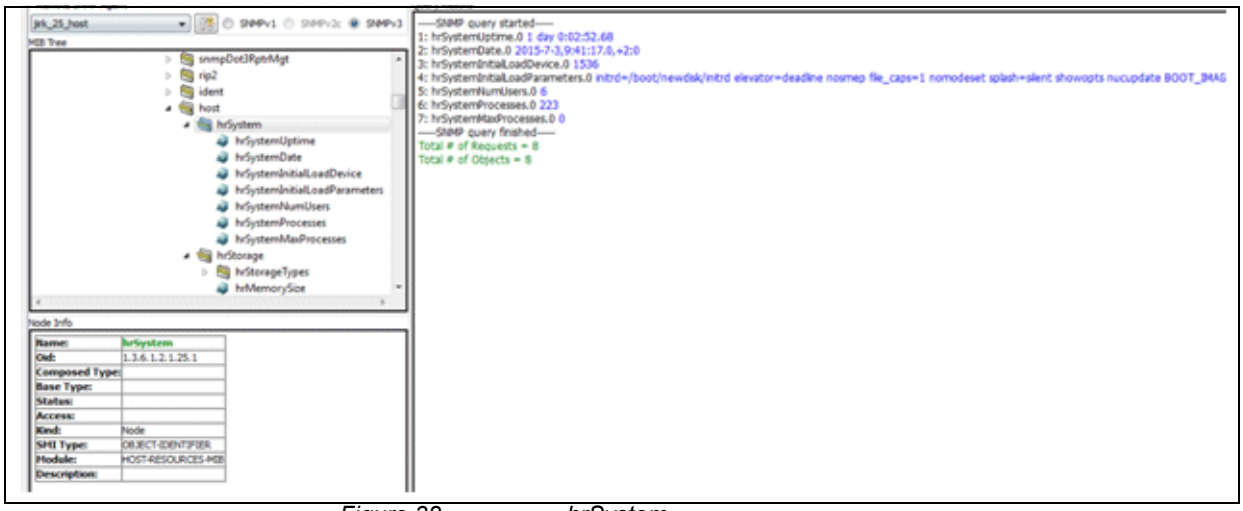

Figure 38 hrSystem

3.11.2.2 File System and Disk Information (hrStorage)

The Host Resources MIB provides information about the size and usage of the file systems. Each file system (and also each memory pool) has an entry in the HOST-RESOURCES-MIB::hrStorageTable table:

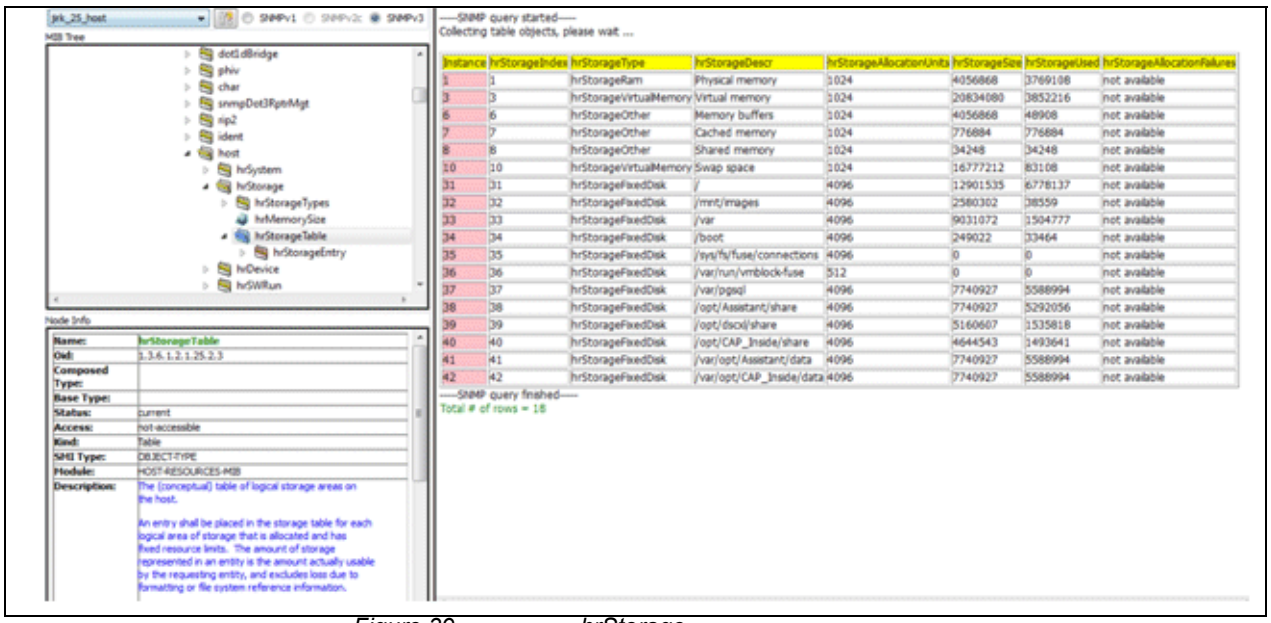

Figure 39 hrStorage

The OIDs under HOST-RESOURCES-MIB::hrStorageSize and HOST-RESOURCES-MIB::hrStorageUsed can be used to calculate the remaining capacity of each mounted file system.

I/O data is available both in UCD-SNMP-MIB::systemStats (ssIORawSent.0 and ssIORawRecieved.0) and in UCD-DISKIO-MIB::diskIOTable. The latter provides much more granular data. Under this table you will find OIDs for diskIONReadX and diskIONWrittenX, providing counters for the number of bytes read from and written to the block device in question since the system boot:

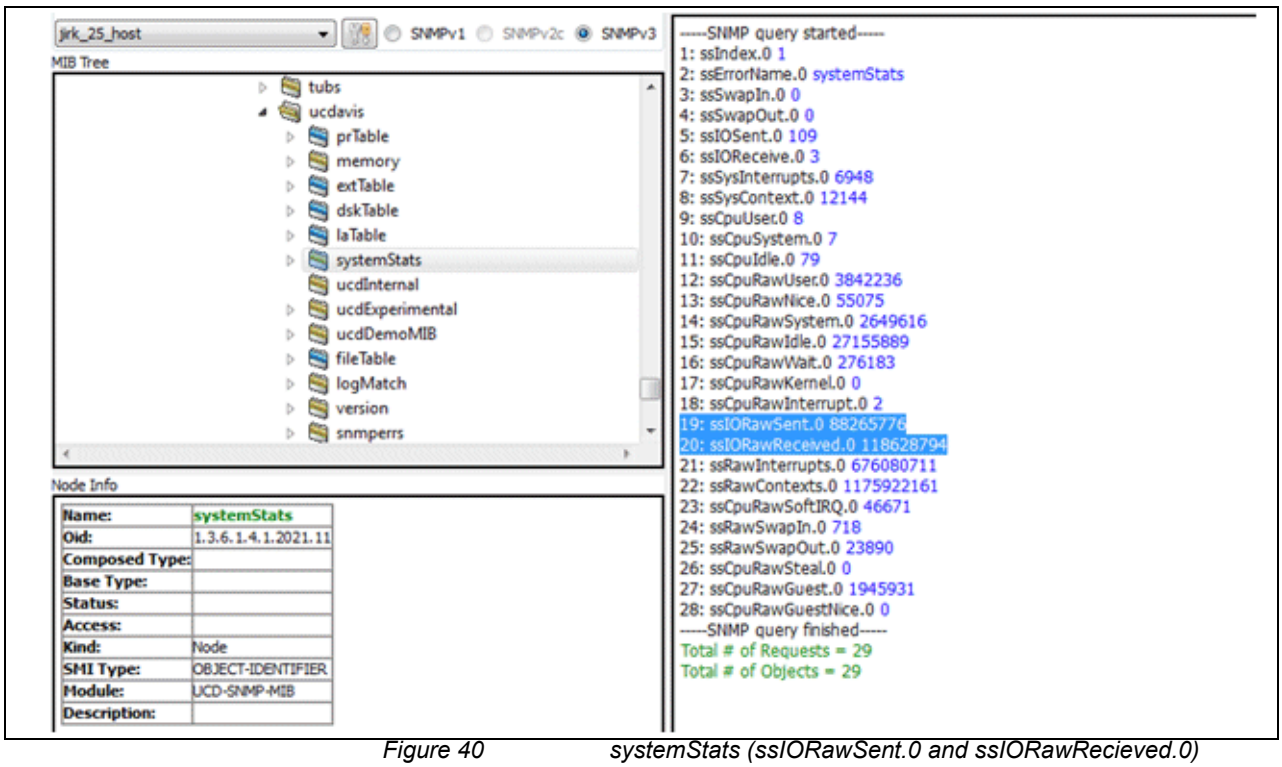

Figure 40 systemStats (sslORawSent.0 and sslORawRecieved.0)

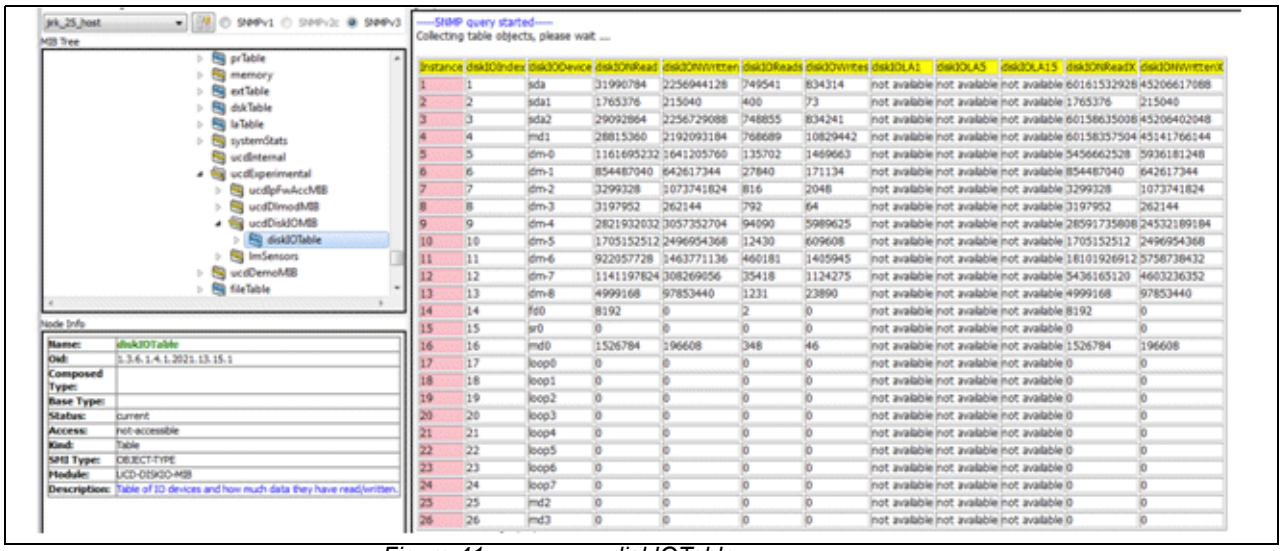

Figure 41 diskIOTable

3.11.2.3 Network Information

The Interfaces MIB provides information on network devices. IF-MIB::ifTable provides an SNMP table with an entry for each interface on the system, the configuration of the interface, and various packet counters for the interface. The following example shows an ifTable on an OpenScape4000 active simplex node system running on VM:

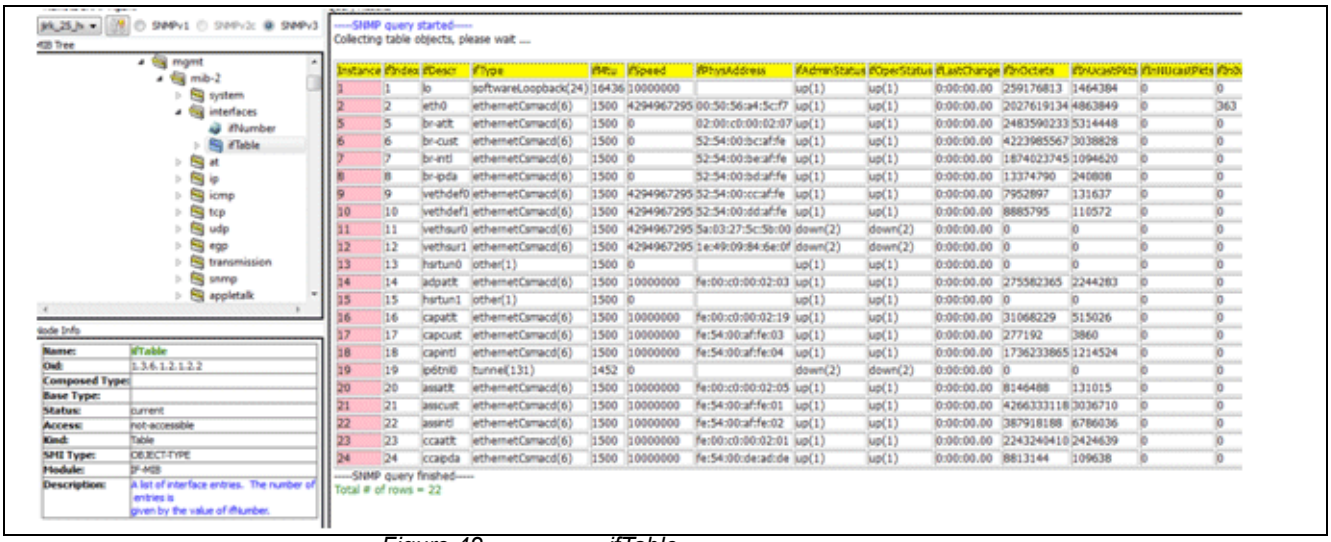

Figure 42 ifTable

However, as you can see the network speed (ifSpeed) is at the maximum value; so this value is not sufficient for network monitoring of OpenScape 4000 interfaces.

You have to use the IF-MIB:ifXTable which is an extension of ifTable.

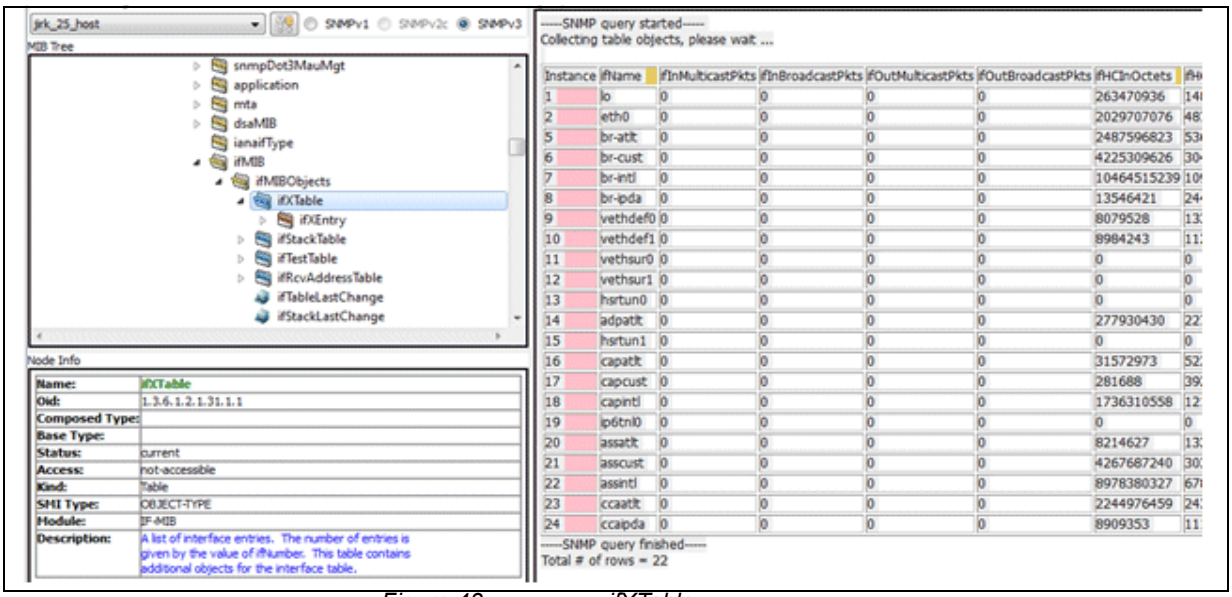

Figure 43 ifXTable

Here the ifHighSpeed value can be used for finding correct interface speed:

Instance	ifName	ifInMulticastPkts	ifInBroadcastPkts	ifOutMulticastPkts	ifOutBroadcastPkts	ifHCInOctets	ifHCInUcastPkts	ifHCInMulticastPkts	ifHCInBroadcastPkts	ifHCOutOctets	ifHCOutUcastPkts	ifHCOutMulticastPkts	ifHCOutBroadcastPkts	ifLinkUpDownTrapEnable	ifHighSpeed	ifPromiscuousMode	ifConnectorPresent	ifAlias	ifCounterDiscontinuityTime
1	lo	0	0	0	0	263470936	1488501	0	0	263470936	1488501	0	0	not availabl	10	false(2)	not availabl		00:00.0
2	eth0	0	0	0	0	2029707076	4878289	0	0	14756027201	8036477	0	0	not availabl	10000	false(2)	true(1)		00:00.0
5	br-ark	0	0	0	0	2487536823	5364119	0	0	1382816	24158	0	0	not availabl	0	true(1)	true(1)		00:00.0
6	br-cust	0	0	0	0	4225309626	3041873	0	0	73723658	595233	0	0	not availabl	0	true(1)	true(1)		00:00.0
7	br-intl	0	0	0	0	10464515233	1038163	0	0	16785410356	1054237	0	0	not availabl	0	true(1)	true(1)		00:00.0
8	br-ipda	0	0	0	0	13546421	244522	0	0	61038	711	0	0	not availabl	0	true(1)	true(1)		00:00.0
9	vethdef0	0	0	0	0	8079528	133738	0	0	8364243	112207	0	0	not availabl	10000	false(2)	true(1)		00:00.0
10	vethdef1	0	0	0	0	8364243	112207	0	0	8079528	133738	0	0	not availabl	10000	false(2)	true(1)		00:00.0
11	vethsur0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	10000	false(2)	true(1)		00:00.0
12	vethsur1	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	10000	false(2)	true(1)		00:00.0
13	hsrun0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00.0
14	adpark	0	0	0	0	277930430	2270531	0	0	2286007836	3116796	0	0	not availabl	10	false(2)	true(1)		00:00.0
15	hsrun1	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00.0
16	capark	0	0	0	0	31572973	523406	0	0	15684267	269805	0	0	not availabl	10	false(2)	true(1)		00:00.0
17	capcust	0	0	0	0	281688	3924	0	0	4267770636	3041044	0	0	not availabl	10	false(2)	true(1)		00:00.0
18	capintl	0	0	0	0	1736310558	1215111	0	0	8397023682	6866207	0	0	not availabl	10	false(2)	true(1)		00:00.0
19	ip6in0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00.0
20	assark	0	0	0	0	8214627	132266	0	0	14225988	139395	0	0	not availabl	10	false(2)	true(1)		00:00.0
21	asscust	0	0	0	0	4267687240	3039693	0	0	73812136	597120	0	0	not availabl	10	false(2)	true(1)		00:00.0
22	assintl	0	0	0	0	8978380327	6788978	0	0	18433400582	2143665	0	0	not availabl	10	false(2)	true(1)		00:00.0
23	ccaark	0	0	0	0	2244976459	2437916	0	0	245225220	1839255	0	0	not availabl	10	false(2)	true(1)		00:00.0
24	ccaipda	0	0	0	0	8909353	111240	0	0	7437320	126824	0	0	not availabl	10	false(2)	true(1)		00:00.0

Figure 44 ifHighSpeed table

The traffic is available under the OIDs IF-MIB::ifHCOutOctets and IF-MIB::ifHCInOctets. Based on these values taken from two subsequent calls you can determine the interface load.

3.11.2.4 Software Information

- Information about installed software rpm packages, running processes and their performance statistics (CPU/MEM usage) can be collected from following three OIDs:
- HOST-RESOURCES-MIB::hrSWRun - contains a listing of all running processes
- HOST-RESOURCES-MIB::hrSWRunPerf - contains memory and CPU statistics on the process table from HOST-RESOURCES-MIB::hrSWRun
- HOST-RESOURCES-MIB::hrSWInstalled - contains a listing of the RPM database

Running software

HOST-RESOURCES-MIB::hrSWRun - contains a listing of all running processes on a OpenScape 4000 host system:

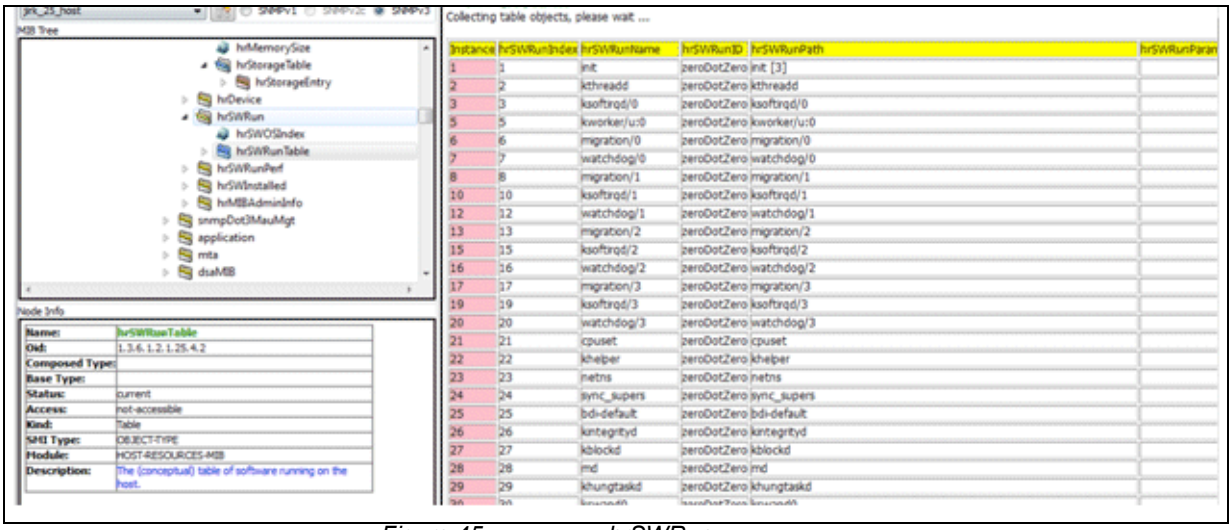

Figure 45 hrSWRun

Installed software performance

HOST-RESOURCES-MIB::hrSWRunPerf - contains memory and CPU statistics on the process table from HOST-RESOURCES-MIB::hrSWRun:

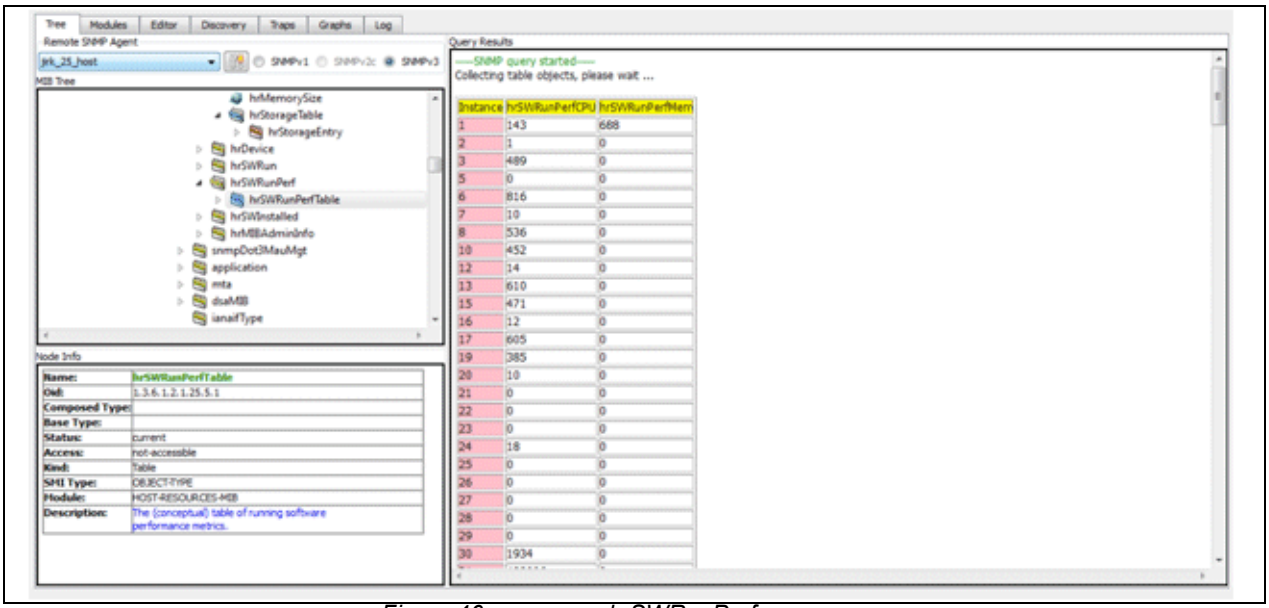

Figure 46 hrSWRunPerf

Installed software packages

The table hrSWInstalledTable from HOST-RESOURCES-MIB::hrSWInstalled part of mib can be used to collect information about the installed rpm packages on the OpenScape4000 host system:

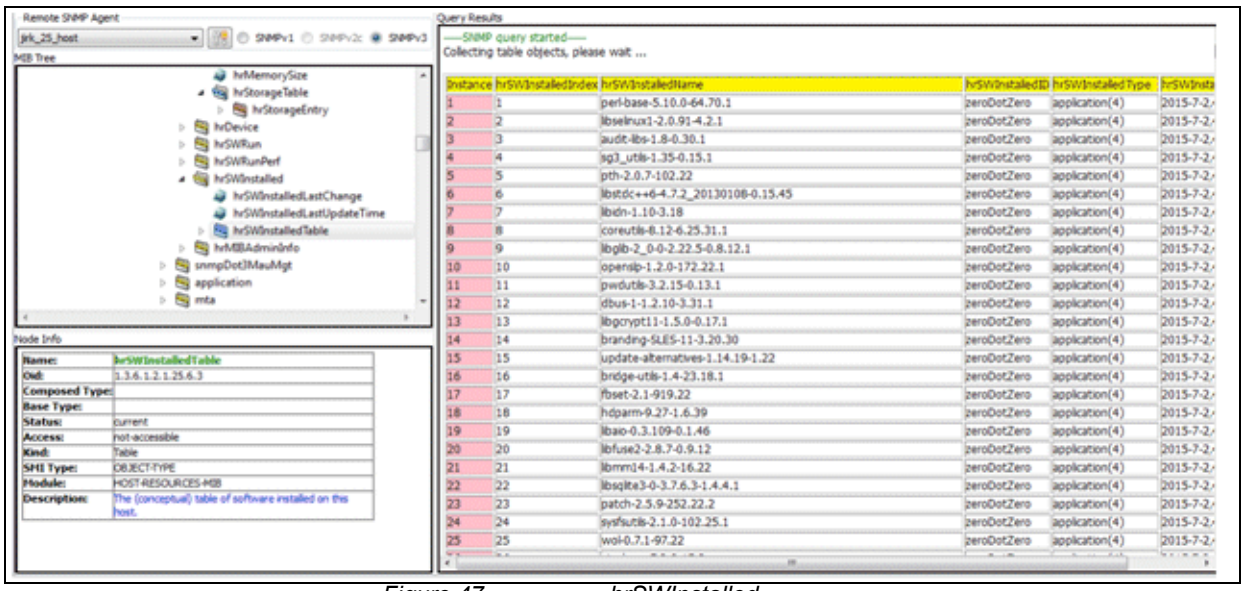

Figure 47 hrSWInstalled

4 Troubleshooting

To resolve some possible errors, refer to:

General Error Messages

This error message is when a server-side script is missing. Contact customer support.

4.1 General Error Messages

There are three types of general error messages:

1. **Error 500 - Internal server error**

   This error message is usually displayed when one or more server-side scripts are not present in system or their access rights are not set properly. It can be also caused by error in server-side scripts. Contact customer support.

2. **Internal server error. Data might be corrupted**

   This error message is displayed when database is in inconsistent state or data entered by user caused database error. Contact customer support.

3. **Content-type=text/plain**

   This error message is when a server-side script is missing. Contact customer support.

5 OpenScape 4000 Alarms

Basically the alarm reporting of OpenScape works like this:

- In case of Network Management (OpenScape Manager is in use), the faults (Fxxxx)/alarms (Axxxx) from OpenScape RMX are sent directly (by AFR2 process on RMX – depending on the CPTP,AFR,SIGNL,… RMX configuration) to the OpenScape Manager SNMP service, where they can be filtered or sent as SNMP hicomAlarm or hicomError trap messages.
- If the OpenScape Manager is not used, the AFR3 process on RMX is configured to send the alarm/error messages to the local OpenScape Assistant where the messages can be filtered or sent as SNMP hicomAlarm/ hicomError trap messages.

Each alarm (hicomAlarmOnMajor, hicomAlarmOnMinor, …) trap message includes the following parameters:

- **hicomSysPabxId**: index of system in chdmain table (basically usable only in case of Network Management); this parameter identifies the node where the alarm occured.
- **hicomSysMnemonic**: mnemonic of the system as it is configured in SysM (text representation of hicomSysPabxId); this parameter identifies the node where the alarm occured.
- **hicomAlGroup**: Group of the Alarm, which can be
  - Central (1),
  - SWU Peripheral (2),
  - SWU Logical (3 and 4),
  - SM Peripheral (5),
  - Manager/Assistant (7)
- **hicomAlSubId**: Alarm Number within the group (see the table below)
- **hicomAlPriority**: priority of the alarm: 0 = minor, 1 = major, 2 = device (always 1 in this trap)
- **hicomAlAbsMod**: module that produced the alarm, e.g. BPA, NM
- **hicomAlStatus**: 0= Alarm Off, 1 = Alarm On
- **hicomAlTimDat**: Date of Alarm occurence in seconds since 01/01/1970
- **hicomAlName**: Alarm Name, e.g. CC RESTARTS; LTU FAILURE; …

For the alarms of groups 1 – 5 see AMOs (VADSU, VADSM). These alarms are produced by RMX and propagated into the SNMP system of the OpenScape Manager or OpenScape Assistant.

Apart from the alarm messages produced by the OpenScape RMX, there can be alarm messages produced by the Manager or the Assistant itself. These alarms have **hicomAlGroup 7 (NM)**.

Here is a list of these predefined alarms from group 7:

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major/ Minor)	Short description
1	RETRY EXCEEDED	major	Col could not fetch CDR file
2	NOT ENOUGH SPACE	major	No Space for Performance Management
3	SWITCH ACCESS FAILING	major	Polling of OpenScape failed (activation project specific)
4	PM-DB FULL	major	Informix DB reached high water
5	INFORMIX	major	General DB problems
6	DISK FULL	major	No Disk space
7	AFR FILE COUNT	major	Number of fault messages coming from RMX too high -> System is overloaded by so many faults
8	AFR DB SPACE	major	Database Threshold reached: Inserting error messages into Database table "lerror" was stopped
9	AFR STOPPED	major	No alarm and error messages will be received because AFR was stopped on RMX side
10	AFR FAULT	major	An error occured during analysis of received AFR message
11	AUTOLCK:	major	User account automatically locked
12	BACKUP FAILED	major	An error occured during RMX data backup
13	RESTORE FAILED	major	An error occured during restore of RMX data
14	DISK FULL	major	Disc space has reached threshold level
15	THRESH. EXCEEDED	major	Database of PM has reached threshold level
16	LMT_CDW_UPDATE	minor	License Management Tool wasn't able update codeword on the switch
17	LMT_LICENSE_REDUCTION	major	Licenses were reduced in the License Management Tool
18	LMT_GLOBAL_ALARM_ THRESHOLD	minor	Threshold alarm is set in one of the Admin Group in License Management Tool
19	LMT_GLOBAL_ALARM	major	Alarm is set in one of the AdminGroups in License Management Tool - codewords for systems in this Admin Group were not updated
20	LMT_GLOBAL_WARNING_ THRESHOLD	minor	Threshold warning is set in one of the Admin Group in License Management Tool
21	LMT_GLOBAL_WARNING	minor	Warning is set in one of the AdminGroups in License Management Tool - codewords for systems in this Admin Group will not be updated
22	PROCM_PM_CONTROL	major	System daemon pm_control from Performace Management terminated unexpectedly

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major/ Minor)	Short description
23	PROCM_PM_COL	major	System daemon pm_col from Performace Management terminated unexpectedly
24	PROCM_PM_SCHED	major	System daemon pm_sched from Performace Management terminated unexpectedly
25	PROCM_COL_SCHEDULE	major	System daemon col_schedule from Collecting Agent terminated unexpectedly
26	PROCM_COL_TRANSFORM	major	System daemon col_transform from Collecting Agent terminated unexpectedly
27	PROCM_COL_CYCLICCHECK	major	System daemon col_cycliccheck from Collecting Agent terminated unexpectedly
28	PROCM_COL_LINE	major	System daemon col_line from Collecting Agent terminated unexpectedly
29	PROCM_COL_DB_PROXY	major	System daemon col_db_proxy from Collecting Agent terminated unexpectedly
30	PROCM_COL_RECEIVE	major	System daemon col_receive from Collecting Agent terminated unexpectedly
31	PROCM_COL_METERING	major	System daemon col_metering from Collecting Agent terminated unexpectedly
32	PROCM_FTW_TRANSFER_ CONTROL	major	System daemon FTW_Transfer_Control from FlagTrace Watchdog terminated unexpectedly
33	PROCM_IDS_ONINIT	major	System database daemon IDS_oninit from Infromix database terminated unexpectedly
34	PROCM_LMT_DAEMON	major	System daemon lmtd from License Management Tool terminated unexpectedly
35	PROCM_SWTD_SERVER	major	System daemon SWTDServer from Software Transfer terminated unexpectedly
36	PROCM_HTTP_USSW	major	Appache server daemon terminated unexpectedly
37	PROCM_HTTP_TOMCAT	major	Tomcat server deamon terminated unexpectedly
38	PROCM_LOGMEVTLOG	major	System daemon LogMEvtLog from Logging Management terminated unexpectedly
39	PROCM_LOGMRECEIVER	major	System daemon LogMReceiver from Logging Management terminated unexpectedly
40	PROCM_LOGMERRH	major	System daemon LogMErrH from Logging Management terminated unexpectedly
41	PROCM_LOGMCONTROL	major	System daemon LogMControl from Logging Management terminated unexpectedly
42	PROCM_LOGMDISPATCH	major	System daemon LogMDispatch from Logging Management terminated unexpectedly
43	PROCM_LOGMSESS CONTROL	major	System daemon LogMSessControl from Logging Management terminated unexpectedly
44	PROCM_SECM_SMW	major	System daemon secm_smw from Security Management terminated unexpectedly

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major/ Minor)	Short description
45	PROCM_SECM_CORE	major	System daemon secm_core from Security Management terminated unexpectedly
46	PROCM_SYMUPLOAD CONTROL	major	System daemon symUploadControl from System Management terminated unexpectedly
47	PROCM_SYMSERVICE	major	System daemon symService from System Management terminated unexpectedly
48	PROCM_CMPROC_DOM_ UXBPROC	major	System daemon cmproc_dom_uxbproc from Configuration Management terminated unexpectedly
49	PROCM_CMPROC_DOM_ UXLMAIN	major	System daemon cmproc_dom_uxlmain from Configuration Management terminated unexpectedly
50	PROCM_CMPROC_CCS	major	System daemon cmproc_ccs from Configuration Management terminated unexpectedly
51	PROCM_CMPROC_SUB_ UXSDBSYN	major	System daemon cmproc_sub_unxsdbsyn from Configuration Management terminated unexpectedly
52	PROCM_CMPROC_DOM_ CSERVER	major	System daemon cmproc_dom_cserver from Configuration Management terminated unexpectedly
53	PROCM_CMPROC_DOM_ CMIPSA	major	System daemon cmproc_dom_cmipsa from Configuration Management terminated unexpectedly
54	PROCM_CMPROC_DOM_ CONVBJOB	major	System daemon cmproc_dom_convbjob from Configuration Management terminated unexpectedly
55	PROCM_CMPROC_DOM_ CDBSERVER	major	System daemon cmproc_dom_cdbserver from Configuration Management terminated unexpectedly
56	PROCM_CMPROC_SUB_ ICPROCESSING	major	System daemon cmproc_sub_icprocessing from Configuration Management terminated unexpectedly
57	PROCM_CMPROC_SUB_ CSERVER	major	System daemon cmproc_sub_cserver from Configuration Management terminated unexpectedly
58	PROCM_CMPROC_DOM_ UMPROC	major	System daemon cmproc_dom_umproc from Configuration Management terminated unexpectedly
59	PROCM_CMPROC_DOM_ UXSDBSYN	major	System daemon cmproc_dom_uxsdbsyn from Configuration Management terminated unexpectedly
60	PROCM_CMPROC_DOM_ UXSFILED	major	System daemon cmproc_dom_uxsfiled from Configuration Management terminated unexpectedly

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major/ Minor)	Short description
61	PROCM_CMPROC_DOM_ DLSPROXY	major	System daemon cmproc_dom_dlsproxy from Configuration Management terminated unexpectedly
62	PROCM_FM_AER_DAEMON	major	System daemon AER_Daemon from Fault Management terminated unexpectedly
63	PROCM_FM_DB_SERVER	major	System daemon FM_DB_Server from Fault Management terminated unexpectedly
64	PROCM_NAMING_SERVICE	major	System daemon NamingService from CORBA communication framework terminated unexpectedly
65	PROCM_FM_FTSERV	major	System daemon ftserv from Batch Generator terminated unexpectedly
66	PROCM_FM_FTSUCC	major	System daemon ftsucc from Batch Generator terminated unexpectedly
67	PROCM_MPCID	major	System daemon mpcid from Multi Purpose Client Interface used for communication with RMX terminated unexpectedly
68	PROCM_MPCIDLOG	major	System daemon mpcidlog from Multi Purpose Client Interface used for communication with RMX terminated unexpectedly
69	PROCM_HISPAD	major	System daemon hispad from HiSPA 4000 terminated unexpectedly
70	PROCM_REPORTGENERATOR	major	System daemon ReportGenerator from Report Generator terminated unexpectedly
71	PROCM_REPGENREADY	major	System daemon RepgenReady from Report Generator terminated unexpectedly
72	PROCM_DMSIED	major	System daemon dmsied from Export Import Interface (XIE) terminated unexpectedly
73	PROCM_XIESERVER	major	System daemon xieserver from Export Import Interface (XIE) terminated unexpectedly
74	PROCM_COMWINACCESS	major	System daemon comwinaccess from Expert Access terminated unexpectedly
75	LOGM_ACTIVITY_TABLE_ THRESHOLD	minor	Activity table from the Logging Management reached its threshold
76	LOGM_ERROR_TABLE_ THRESHOLD	minor	Error table from the Logging Management reached its threshold
77	LICM_LICENSE_EXCEEDED	major	OpenScape 4000 Management License has expired
78	HBR_DATA_BACKUP	major	Data backup failed
79	HBR_LOGICAL_ABD	major	Logical backup of ABD unit failed
80	HBR_LOGICAL_BUM	major	Logical backup of BUM unit failed
81	HBR_LOGICAL_CDB	major	Logical backup of CDB unit failed
82	HBR_LOGICAL_CHD	major	Logical backup of CHD unit failed

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major/ Minor)	Short description
83	HBR_LOGICAL_COMWIN	major	Logical backup of COMWIN unit failed
84	HBR_LOGICAL_HBR	major	Logical backup of HBR unit failed
85	HBR_LOGICAL_HBR_MPCID	major	Logical backup of MPCID unit failed
86	HBR_LOGICAL_HBR_TSYNC	major	Logical backup of TSYNC unit failed
87	HBR_LOGICAL_LAP2	major	Logical backup of LAP2 unit failed
88	HBR_LOGICAL_LOGM	major	Logical backup of LOGM unit failed
89	HBR_LOGICAL_SSO	major	Logical backup of SSO unit failed
90	HBR_LOGICAL_SECM	major	Logical backup of SECM unit failed
91	HBR_LOGICAL_UBA	major	Logical backup of UBA unit failed
92	HBR_LOGICAL_WEBMIN	major	Logical backup of WEBMIN unit failed
93	FM_COMANDFILE_SEND	minor	Batch Generator cannot send amo job to the switch
94	PM_DATABASE_THRESHOLD	minor	Threshold is reached in PM database
95	PM_REPORT	major	Performance management time controlled report was not successful.
96	COL_FETCH	major	Reception (fetch) in Collection Agent from the switch was not successful
97	COL_RECEIVE	major	Conversion (transform) in received file in Collection Agent was not successful
98	COL_OUTPUT_FILE_PROD	minor	Production of the output file in Collection Agent was not successful
99	COL_PARTITION_FILLED	major	Fetching in Collection Agent deactivated because of full COL-Backup directory
100	CM_DB_SYNCH	minor	Database synchronization with the switch was not successful in Configuration Management
101	SWA_ACTIVATION_FAILED	major	Software activation of the Major/Minor/FixRelease or Hotfix failed
102	DISK_SATURATION_ THRESHOLD	minor	Threshold on one of the monitored system partitions is reached
103	SSO_REPLICATION	major	Smart switch over replication was not successful
104	LICM_H300_PORTCOUNT_ WARN_REACHED	minor	Threshold for H300 port counts was reached in License Management.
105	LICM_HP4K_V1_PORTCOUNT_WARN_REACHED	minor	Threshold for OpenScape4000 V1 port counts was reached in License Management.
106	LICM_HP4K_V2_PORTCOUNT_WARN_REACHED	minor	Threshold for OpenScape4000 V2 port counts was reached in License Management.
107	LICM_HP4K_V3_PORTCOUNT_WARN_REACHED	minor	Threshold for OpenScape4000 V3 port counts was reached in License Management.
108	LICM_HP4K_V4_PORTCOUNT_WARN_REACHED	minor	Threshold for OpenScape4000 V4 port counts was reached in License Management.

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major/ Minor)	Short description
109	LICM_HP4K_V5_PORTCOUNT_WARN_REACHED	minor	Threshold for OpenScape4000 V5 port counts was reached in License Management.
110	LICM_PORTCOUNT_ EXCEEDED	major	Portcount for OpenScape4000 licenses were exceeded in License Management.
111	LICM_HP4K_V6_PORTCOUNT_WARN_REACHED	minor	Threshold for OpenScape4000 V6 port counts was reached in License Management.
112	LICM_SLES_UPDATE_ PROTECTION	major	System doesn't have enhough SLES Update protection Licenses. The RLC, minor, major updates might be blocked.

For more information about fault management, alarms and SNMP see Chapter 6, "OpenScape 4000 SNMP Management" in the Installation and Service Manual.

Index

T

U