A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant V11

Simple Network Management Protocol - OpenScape SNMP

Simple Network Management Protocol -
OpenScape SNMP

Hilfe

02/2024

A31003-H34B0-M122-01-00A9

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.

Inhalt

1 Übersicht

Dieses Übersichtskapitel enthält die folgenden Abschnitte:

1.1 Einführung in SNMP

SNMP gehört zu den von der Internet Engineering Task Force (IETF) definierten Internetprotokollen. Die Abkürzung steht für “Simple Network Management Protocol”. Es wird für die Bereitstellung einer Standardoberfläche zum Überwachen und Konfigurieren von Netzwerkressourcen verwendet.

SNMP basiert auf dem Manager/Agent-Modell. Agents führen Management Information-Datenbanken, die von Managern gelesen und gegebenenfalls geschrieben werden können. Diese Art von Kommunikation wird immer von den Managern initiiert. Agents können auch asynchron Benachrichtigungsereignisse, so genannte “Traps”, an die Manager senden. Neben diesen Vorgängen umfasst die Definition des SNMP-Protokolls auch das Datenmodell und das Netzwerkprotokoll.

Der SNMP-Agent für OpenScape 4000 Assistant unterstützt das Simple Network Management Protocol Version 1 (SNMPv1) und Version 3 (SNMPv3). OpenScape 4000-Hostsysteme unterstützen nur SNMPv3.

Hintergrundinformationen zu SNMPv3

SNMPv3 ist ein auf Interoperabilitäts-Standards basierendes Netzwerkverwaltungsprotokoll. SNMPv3 ermöglicht durch eine Kombination von Authentifizierung und Verschlüsselung von Paketen einen sicheren Zugriff auf Geräte über das Netzwerk. SNMPv3 bietet folgende Sicherheitsfunktionen:

- Integrität von Nachrichten — stellt sicher, dass ein Paket bei der Übertragung nicht manipuliert wird.
- Authentifizierung — ermittellt, ob es sich bei der Nachrichtenquelle um einen gültigen Absender handelt.
- Verschlüsselung — Scrambling von Paketinhalten, um ein Lesen durch unbefugte Dritte zu verhindern.

SNMPv3 verfügt über Sicherheitsmodelle und Sicherheitsstufen. Ein Sicherheitsmodell ist eine Authentifizierungsstrategie, die speziell für einen Benutzer und die Gruppe, der er angehört, eingerichtet wurde.

Eine Sicherheitsstufe ist die zulässige Sicherheitstufe innerhalb eines Sicherheitsmodells.

Eine Kombination aus Sicherheitsmodell und Sicherheitsstufe bestimmt letztendlich, welcher Sicherheitsmechanismus bei der Bearbeitung eines SNMP-Pakets herangezogen wird.

SNMPv3-Objekte besitzen folgende charakteristische Eigenschaften:

- Jeder Benutzer gehört zu einer Gruppe.
- Eine Gruppe definiert die Zugriffsrichtlinie für eine Gruppe von Benutzern.
- Eine Zugriffsrichtlinie bestimmt, welche SNMP-Objekte gelesen, geschrieben und erstellt werden können.
- Über eine Gruppe wird die Liste der Benachrichtigungen definiert, die ihre Benutzer erhalten können.
- Über eine Gruppe wird auch das Sicherheitsmodell und die Sicherheitsstufe ihrer Benutzer festgelegt.

Verwandte Themen

Management Information Base (MIB)

Datentypen

Vorgänge

Traps

Communities

1.2 Management Information Base (MIB)

In der MIB werden die Verwaltungsdaten eines Geräts (oder eines Subsystems des Geräts) angegeben. In der MIB wird ein hierarchischer Namespace definiert, der Objekt-IDs (OIDs) enthält. Diese Hierarchie beginnt bei einem standardmäßigen “iso”-Stamm, und die höheren Stufen entsprechen Organisationen, während die niedrigeren Stufen den Daten auf dem Subsystem entsprechen. Alle Knoten können durch einen eindeutigen Namen oder Pfad identifiziert werden, der die genaue Position in der Hierarchie beschreibt. Der Pfad wird aus den IDs der Knoten auf den verschiedenen Stufen, jeweils durch Punkte getrennt (“.”) aufgebaut. Die MIB-Datenbank enthält zwei Knotentypen:

- innere Knoten, die nur die Struktur definieren und auf die nicht direkt über die Manager zugegriffen werden kann
- Blatt[1]-Knoten, die die Agent-Daten enthalten und von Managern gelesen und gegebenenfalls geschrieben werden können.

Einige Beispiele für OIDs

Pfad	Eindeutiger 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 werden in Beschreibungsdateien angegeben, die in ASN.1 geschrieben sind. Sie werden von den Managern zum ordnungsgemäßen Anzeigen der Agent-Daten benötigt.

Verwandte Themen

Einführung in SNMP

Datentypen

Vorgänge

Traps

Communities

1. Eine MIB kann als Baumgrafik dargestellt werden, in der nur die Blätter Daten enthalten.

1.3 Datentypen

SNMP definiert Datentypen für verwaltete Objekte. Diese werden auch in den MIB-Beschreibungsdateien definiert (siehe oben). Neben einfachen Datentypen wie z. B. *Integer32*, *Counter32* und *OCTET STRING* gibt es für die meisten Konzepte im Zusammenhang mit Netzwerken, z. B. die MAC-Adresse und die IP-Adresse, außerdem vordefinierte Typen (*MacAddress* bzw. *IpAddress*). Der MIB-Designer kann auch neue Typen auf der Grundlage vordefinierter Typen definieren.

Zwei spezielle Datentypen bedürfen einer weiteren Erklärung:

1. INTEGER-Aufzählungen werden verwendet, wenn eine OID nur eine begrenzte Anzahl von Werten haben kann. In diesem Fall können Namen für die numerischen Werte definiert werden, um die Lesbarkeit zu verbessern. Wenn die MIB-Beschreibungsdatei nicht in den Manager importiert wurde, kann der Wert nur als Zahl angezeigt werden.
2. SEQUENCEs sind das SNMP-Gegenstück von Datenbanktabellen. Ein SEQUENCE-Knoten (normalerweise mit dem Namen “xxxTable”) hat ein einziges untergeordnetes Element (“xxxEntry”), dessen untergeordnete Elemente den Feldern (Spalten) in der Tabelle entsprechen. Jede Tabelle enthält Indexfelder, deren Werte mit den OIDs der Felder verkettet werden. So unterscheidet SNMP die Zeilen.

Beispieltabellen

Wenn die OIDs wie unten gezeigt lauten:

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

und die Tabelle zwei Zeilen enthält:

exampleIndexNumber	exampleDataValue
1	10
5	20

dann lauten die OIDs und Werte der Felder in den beiden Zeilen wie folgt:

Erste Zeile	1.3.6.1.4.9999.3.1.1.1	1
	1.3.6.1.4.9999.3.1.2.1	10
Zweite Zeile	1.3.6.1.4.9999.3.1.1.5	5
	1.3.6.1.4.9999.3.1.2.5	20

Beachten Sie, dass es sich bei Verwendung der automatischen Discovery nicht um die Reihenfolge handelt, in der die Daten vom Agent zurückgegeben werden. Da die OIDs der Zellen in der ersten Spalte kleiner sind als die in der zweiten Spalte (die Zeilen-ID befindet sich am Ende der OID, hinter der Spaltennummer), wird die Spalte nicht wie erwartet zeilenweise, sondern spaltenweise zurückgegeben.

Weitere Informationen zu Tabellen und anderen Datentypen finden Sie in einer ausführlicheren Einführung in SNMP. Wikipedia.org ist ein guter Ausgangspunkt.

Verwandte Themen

Einführung in SNMP

Management Information Base (MIB)

Vorgänge

Traps

Communities

1.4 Vorgänge

Ein Manager kann drei Vorgänge an den Agent ausgeben:

1. **GET**: Fragt den Wert des verwalteten Objekts für eine bestimmte OID ab.
2. **GET-NEXT**: Gibt den Wert des ersten verwalteten Objekts zurück, dessen OID größer ist als die angegebene OID. OIDs werden durch Vergleichen der Zahlen der einzelnen Stufen angeordnet. Dieser Vorgang kann für die Discovery einer unbekannten MIB verwendet werden: GET-NEXT wird aufgerufen, bis keine Objekte mehr übrig sind.
3. **SET**: Der Manager kann den Wert des Objekts mit der angegebenen OID überschreiben. Auch wenn alle Objekte in einer MIB gelesen werden können, können normalerweise nur einige geändert werden.

Verwandte Themen

Einführung in SNMP

Management Information Base (MIB)

Datentypen

Traps

Communities

1.5 Traps

Traps werden vom Agent bei Eintreffen einer vordefinierten Bedingung ausgelöst. Wenn ein Manager einen Trap erhält, kann er GET-Anforderungen für den Agent ausgeben, um zu ermitteln, was geschehen ist. Zu den typischen Verwendungszwecken für Traps gehören Fehlerberichte und die Registrierung eines Geräts für das Netzwerk.

Verwandte Themen

Einführung in SNMP

Management Information Base (MIB)

Datentypen

Vorgänge

Communities

1.6 Communities

Communities dienen als Form der Authentifizierung in SNMPv1 und SNMPv2c. Sie sind in etwa mit Passwörtern zu vergleichen und müssen bei jeder Anforderung angegeben werden. SNMPv1 und SNMPv2c unterstützen jedoch keine Verschlüsselung. Außerdem sind Communities normalerweise allgemein bekannt und werden häufig zum Angeben des Teils der MIB, auf den der Manager zuzugreifen versucht, verwendet, da für verschiedene Teile der MIB unterschiedliche Community-Namen angegeben werden können.

SNMPv1 und SNMPv2c sind keine sicheren Protokolle. SNMPv3 ist ein sicheres Protokoll; es wird vom SNMP-Leistungsmerkmal des Assistant unterstützt.

Verwandte Themen

Einführung in SNMP

Management Information Base (MIB)

Datentypen

Vorgänge

Traps

2 Leistungsmerkmalbeschreibung

Fügt dem OpenScape 4000 Assistant und allen verbundenen Hostsystemen wie SoftGate, STMIX und OS Enterprise Gateway die SNMP-Verwaltbarkeit hinzu. Die folgenden Funktionen werden bereitgestellt:

- Die im OpenScape 4000 Manager verfügbare MIB steht jetzt auch im Assistant zur Verfügung.
- Eine Assistant-spezifische MIB ermöglicht den Zugriff auf
  - Daten im OpenScape/HiPath Inventory Management
  - LAN-Karte und Hostdaten aus System Management (SysM)
  - Daten zur Verwendung von WAML-Verbindungen durch LEGK
  - Ergänzende Informationen zu Baugruppen und IPDA-Verbindungen
  - Außerdem wird ein Trap ausgelöst, wenn von der Anlage ein Fehler oder Alarm gemeldet wird.

HINWEIS: Ab OpenScape 4000 V7 R2 werden zwei neue MIBs unterstützt: app4K.mib und MIB2.

In diesem Kapitel finden Sie die folgenden Abschnitte:

2.1 Installation und Steuerung

Nach seiner Aktivierung wird das AFR 3-Gerät für die Konfiguration der Funktion “Automatic Fault Reporting (AFR)” des RMX (Fxxxx und Alarmmeldungen) verwendet.

HINWEIS: Wenn AFR 3 bereits von einer anderen Anwendung verwendet wird, überschreibt SNMP die vorherigen Einstellungen.

Standardmäßig sind keine Trap-Ziele oder Community-Zeichenketten definiert.

Das SNMP-Leistungsmerkmal kann mit den folgenden Anwendungen gesteuert werden:

- SNMP kann in der Anwendung **Application Control** aktiviert bzw. deaktiviert werden.
- Der **SNMP-Konfigurator** kann verwendet werden,
  - SNMP auf allen mit dem Assistant verbundenen Hosts zu konfigurieren und
  - um die Trap-Endpunkte anzugeben,
  - um die MIB-Definitionsdateien herunterzuladen (siehe SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren auf Seite 38),
  - um das Versenden von Traps für bestimmte Fehlernummern zu aktivieren/deaktivieren (siehe Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren auf Seite 41),
  - um die MIB2-Parameter und -Filter auf allen verbundenen Hosts zu konfigurieren,
  - um die RMX/Assistant-Alarme zurückzusetzen.
- Der **Alarmkonfigurator** kann verwendet werden, um anzugeben, welche Alarme bestimmten Leitungsbündeln zugewiesen werden und unter welchen Bedingungen sie aktiviert werden sollen. Diese Einstellungen wirken sich auch auf die Generierung von SNMP-Traps aus, da sie anhand der aktivierten Alarme erstellt werden.

Verwandte Themen

Aktivierung

Verwendung

Im Hintergrund …

SNMP Discovery

Voraussetzungen

2.2 Aktivierung

Das SNMP-Leistungsmerkmal ist standardmäßig deaktiviert. Damit es verwendet werden kann, muss es in Application Control aktiviert werden.

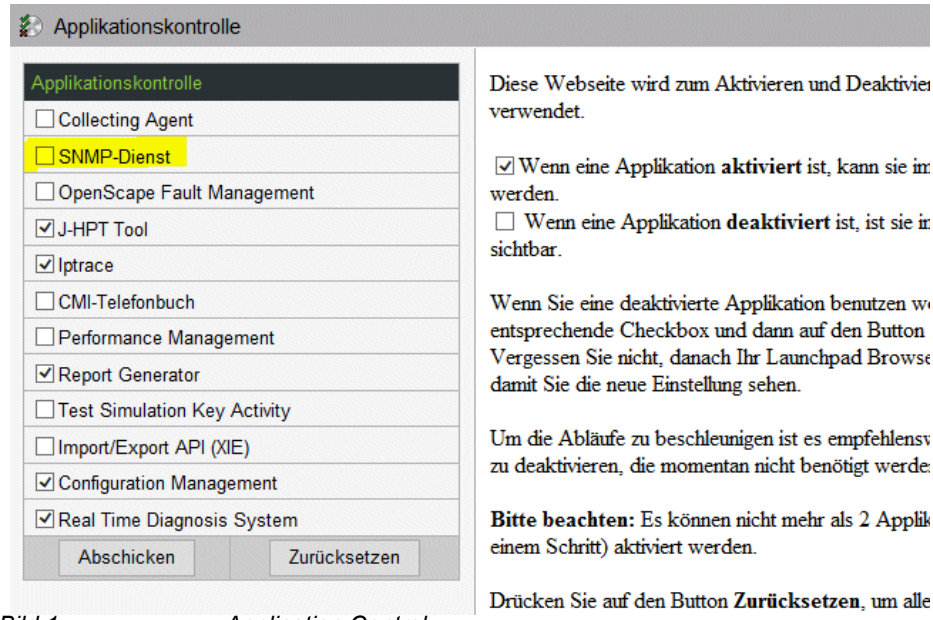


Bild 1 Application Control

Verwandte Themen

Installation und Steuerung

Verwendung

Im Hintergrund …

SNMP Discovery

Voraussetzungen

2.3 Verwendung

Die Verwendung und die verfügbaren Informationen hängen von der verwendeten MIB ab.

- “Hicom MIB” – die vom “Manager” portierte MIB:

  Diese MIB enthält Informationen zur Anlage. Die folgenden Informationen können abgerufen werden:

  – BG-Daten

  – Trunking

  – RMX-Softwareversion und Patches

  – aktuelle und externe Systeme

  – Alarmkonfigurationen

  – Liste der Alarme und Fehler

  Ab V7R2 wird die hicomMIB um zwei Tabellen erweitert, die während der Discovery (Erkennung) des Systems ausgefüllt werden.

  – hostBaseSystems – Tabelle mit den IP-Adressen der zu einem bestimmten Assistant gehörigen 4k-Hostsysteme (Knoten A, Knoten B, Quorum-Knoten).

  – hostAPsystems – Tabelle mit IP-Adressen und LTUs von zu einem bestimmten Assistant gehörigen SoftGate/Survivable SoftGate/AP-E-Hostsystemen

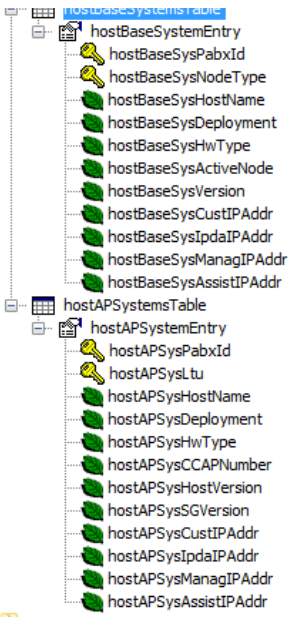


Bild 2 hostBaseSystemsTable/hostAPSystemsTable

Die Tabelle mit den Hostsystemen (hostBaseSystems) enthält die folgenden Felder:

- hostBaseSysPabxId – Eindeutige Kennung des 4k-Systems auf dem 4k-Manager. Im Assistant ist dieser Wert immer 1.
- hostBaseSysNodeType – Typ des 4k-Hostknotens. Bei einem Simplex-Knoten wird nur Knoten A (nodeA) verwendet. Bei einem Duplex-Knoten auf dem Host kann der Knoten vom Typ Knoten A (nodeA), Knoten B (nodeB) oder Quorum-Knoten (nodeQ) sein.
- hostBaseSysHostName – Hostname des Knotens
- hostBaseSysDeployment – ID des Bereitstellungstyps in Textform, z. B. DuplexNode, SimplexNode ...
- hostBaseSysHWType – ID des Hardwaretyps, z. B. VM, DSCXLv2, OSA500i, ...
- hostBaseSysActiveNode – Wird im Duplex-Modus zur Identifizierung des aktiven Knotens und der Standby-Knoten verwendet.
- hostBaseSysVersion – Version des 4k-Hostsystems.
- hostBaseSysCustIPAddr – Kunden-LAN-IP-Adresse der Appliance.
- hostBaseSysIpdaIPAddr – IPDA-LAN-IP-Adresse der Appliance.
- hostBaseSysManagIPAddr – Management-LAN-IP-Adresse der Appliance.
- hostBaseSysAssistIPAddr – Die zur Assistant-IP-Adresse gehörigen Appliances.

Die Tabelle mit den Software-basierten APs (hostAPsystems) enthält die folgenden Felder:

- hostAPSysPabxId – Eindeutige Kennung des 4k-Systems auf dem 4k-Manager. Im Assistant ist dieser Wert immer 1.
- hostAPSysLtu – LTU-Nummer des Access Points.
- hostAPSysHostName – Hostname des Knotens.
- hostAPSysDeployment – ID des Bereitstellungstyps in Textform, z. B. StandaloneSG, SurvivableSG, ...
- hostAPSysHwType – ID des Hardwaretyps in Textform, z. B. DSCXLv2, OSA500i, VM ...
- hostAPSysCCAPNumber – Nummer des APE/SurvivableSG Access Points.
- hostAPSysHostVersion – Release-Version für die Plattform.
- hostAPSysSGVersion – Release-Version des SoftGates.

- hostAPSysCustIPAddr – Kunden-LAN-IP-Adresse der Appliance.
- hostAPSysCustIPAddr – IPDA-LAN-IP-Adresse der Appliance.
- hostAPSysManagIPAddr – Management-LAN-IP-Adresse der Appliance.
- hostAPSysAssistIPAddr – Die zur Assistant-IP-Adresse gehörigen Appliances.

Diese Informationen stehen jedoch nicht sofort zur Verfügung. Zuerst muss ein so genannter Discovery-Prozess gestartet werden.

HINWEIS: In der Original-MIB im OpenScape 4000 Manager konnten die Informationen verschiedener Assistants gespeichert werden. Um die Kompatibilität mit dem Manager aufrechtzuerhalten, wurde die MIB nicht geändert. Das bedeutet, dass sich die meisten Daten in Tabellen befinden, obwohl einige der Tabellen nur eine Zeile enthalten – die Daten des Assistants. Daher müssen alle SNMP Get- und Set-Anforderungen mit dem Feld “PabxId” in den Tabellen indiziert werden. Im Assistant entspricht die PabxId immer 1 (eins).

- “HIM MIB” – die Assistant-spezifische MIB:

  Diese MIB enthält OpenScape 4000 Assistant-spezifische Informationen. Umfasst Folgendes:

  - Alle Daten im OpenScape/HiPath Inventory Management
  - Netzwerkschnittstellen:
    - LAN-Karten
    - Hosts
    - WAML-Verbindungen
- Zusätzliche Informationen für Daten in der Hicom MIB: Baugruppen und IPDA-Verbindungen.
- Die neue app4K-MIB ist in das OpenScape Fault Management integriert, so dass die Alarme entsprechend angezeigt werden. In OpenScape Fault Management werden die Host-Alarme den entsprechenden IP-Knoten zugeordnet.

Verwandte Themen

Installation und Steuerung

Im Hintergrund …

Aktivierung

SNMP Discovery

Voraussetzungen

2.4 Im Hintergrund …

Der SNMP-Service des Assistants besteht aus verschiedenen “Agents”, die dem Benutzer Informationen bereitstellen. Es gibt zwei Agent-Typen: den Master-Agent und die Unteragents. Der Master-Agent akzeptiert Abfragen, die er an die entsprechenden Unteragents weiterleitet, gibt die Antworten der Unteragents zurück und sendet Traps.

Die Unteragents stellen die Systemdaten bereit. Es handelt sich dabei um folgende Daten:

Agent	Beschreibung	Implementierter MIB-Zweig
MIB-2	Implementiert die Standard-MIB-2 gemäß RFC 1213.	MIB-2
System	Enthält Basisdaten zum System.	hicomSystem
Alarm	Zuständig für die Alarmbehandlung; löst Traps aus, wenn sich der Status eines Alarms ändert.	hicomAlarms, hicomAlConf
Fehler	Behandelt Systemfehler; löst beim Auftreten eines Fehlers Traps aus.	hicomErrors
Topologie	Enthält Trunking-Daten	hicomTopo
Hardware	Enthält Hardwaredaten	hicomHard
Software	Daten zur APS-Version und zu RMX-Patches	hicomSoft
Discovery	Verwaltet die Discovery für Software, Hardware, Topologie und Alarm-Agents; siehe unten.	hicomDiscov
HIM	Implementiert die gesamte HIM MIB.	himRegMIB

Verwandte Themen

Installation und Steuerung

Aktivierung

Verwendung

SNMP Discovery

Voraussetzungen

2.5 SNMP Discovery

Eine Discovery ist der Prozess, bei dem die Anlagendaten aus der RMX-Datenbank in die Datenbank des OpenScape 4000 Assistants geladen werden, so dass der Benutzer bei SNMP-Abfragen die aktuellen Daten erhält.

Der Discovery-Prozess kann für die gesamte MIB des OpenScape 4000 Assistants gestartet werden (dann wird er als Master-Discovery bezeichnet) oder nur für bestimmte Daten in der MIB.

Folgende Discoverys sind für bestimmte Daten möglich:

- **HicomAlConf discovery**: Lädt Informationen zu den Fehlern und Alarmen der Hicom in die Datenbank des OpenScape 4000 Assistants.
- **hicomSoft discovery**: Lädt Informationen zur Softwarekonfiguration der Hicom in die Datenbank des OpenScape 4000 Assistants.
- **hicomHard discovery**: Lädt Informationen zur Hicom-Hardware in die Datenbank des OpenScape 4000 Assistants.
- **hicomTopo discovery**: Lädt Informationen zur Topologie der Hicom in die Datenbank des OpenScape 4000 Assistants.
- **HIM discovery**: Lädt die aktuellen Informationen für die HIM MIB in die Datenbank des OpenScape 4000 Assistants.

HINWEIS: Während der HIM-Discovery werden möglicherweise nicht alle HIM MIB-Informationen aktualisiert. Um die neuesten Daten in der HIM MIB abzurufen, müssen Sie zuerst einen Upload im CM starten und dann den HIM-Discovery-Prozess starten.
Während der Master-Discovery werden die HIM MIB-spezifischen Daten nicht aktualisiert.

Der Status der Discoverys wird von den folgenden MIB-Knotennamen verarbeitet:

- **hicomAlConfDiscovStatus**: Status der HicomAlConf-Discovery
- **hicomSoftDiscovStatus**: Status der HicomSoft-Discovery
- **hicomHWDiscovStatus**: Status der HicomHard-Discovery
- **hicomTopoDiscovStatus**: Status der hicomTopo-Discovery
- **himDiscovStatus**: Status der HIM-Discovery
- **hicomDiscovStatus**: Status der Master-Discovery

Ein bestimmter Discovery-Prozess kann gestartet werden, indem der entsprechende Status eines Wertes auf 3 (busy) festgelegt wird.

Wenn der Benutzer z. B. die neuesten Daten zur Hicom-Hardware in der MIB abrufen möchte, muss er die hicomHard-Discovery starten, indem er die Anforderung “SNMP Set” mit dem Wert 3 (busy) an die hicomHWDiscovStatus-OID sendet.

Wenn der Discovery-Status beendet ist, lautet der Statuswert 1 (done). Das bedeutet, dass die Discovery nicht ausgeführt wird. Wenn der Wert des Status 2 (error) entspricht, ist während der Discovery ein Fehler aufgetreten. Daher wurden die neuesten Daten nicht in die Datenbank des Assistants hochgeladen.

Der jeweilige Discovery-Prozess kann durch Festlegen des Statuswertes auf 6 (kill) abgebrochen werden. In diesem Fall werden keine aktuellen Daten in die Datenbank des Assistants geladen, und der Status der jeweiligen Discovery wird auf 2 (error) festgelegt.

Wenn der Benutzer den Master-Discovery-Prozess starten möchte, muss er den **hicomDiscovStatus** durch eine SNMP Set-Anforderung auf den Wert 13 (masterBusy) festlegen. Wenn die Master-Discovery erfolgreich abgeschlossen wurde, wird der Status auf 11 (MasterDone) festgelegt. Wenn während des Master-Discovery-Prozesses ein Fehler auftritt, wird der Status auf 12 (MasterError) festgelegt.

HINWEIS: Beim Festlegen der Discovery-Werte muss am Ende der OID eine “.1” angefügt werden. Wenn für den hicomHWDiscovStatus die OID 1.3.6.1.4.1.231.7.2.1.6.5.2.1.3 festgelegt ist, sollte die ID 1.3.6.1.4.1.231.7.2.1.6.5.2.1.3.1 verwendet werden. Der Grund hierfür liegt darin, dass auch die Discovery-Tabellen mit dem Feld “PabxId” indiziert werden (siehe “Verwendung”, Seite 16)

Verwandte Themen

Installation und Steuerung

Aktivierung

Verwendung

Im Hintergrund …

Voraussetzungen

2.6 Voraussetzungen

Zum Nutzen von Fehler- und Alarmreporten wird ein Netzwerkverwaltungssystem oder ein SNMP-Client, der Traps empfangen kann, benötigt.

Zum Abfragen von Daten aus dem Assistant SNMP oder zum Starten von Discoverys wird ein Client-PC mit einem MIB-Browser benötigt.

Verwandte Themen

Installation und Steuerung

Aktivierung

Verwendung

Im Hintergrund …

SNMP Discovery

3 SNMP-Konfigurator

Mit dem SNMP-Konfigurator können Sie SNMPv1 und SNMPv3 auf dem OpenScape 4000 Assistant sowie SNMPv3 auf allen verbundenen Hosts konfigurieren.

Zugriff auf die Seite “SNMP-Konfigurator”

Führen Sie auf der OpenScape 4000 Assistant-Startseite folgende Schritte durch:

- Wählen Sie **Diagnose -> Fault Management** und klicken Sie auf **SNMP-Konfigurator**.

  Die Seite “SNMP-Konfigurator” wird angezeigt

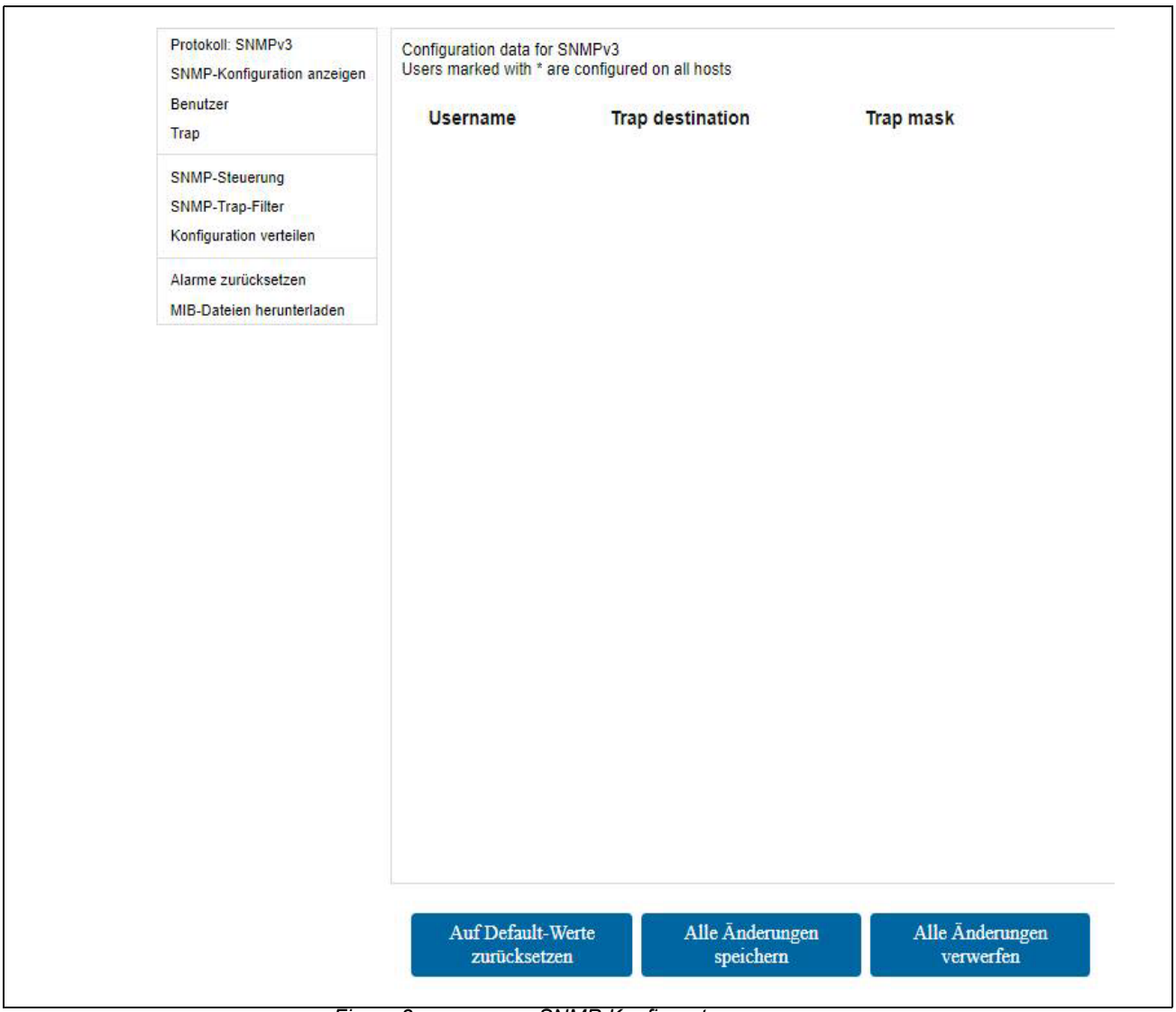


Figure 3 SNMP-Konfigurator

Auf der Seite “SNMP-Konfigurator” haben Sie folgende Möglichkeiten:

- Angeben der Netzwerkverwaltungssysteme (Network Management Systems, NMS), die zum Empfangen der von den SNMP-Agents gesendeten Traps verwendet werden
- Hinzufügen oder Entfernen von Communities (SNMPv1)
- Hinzufügen oder Entfernen von Benutzern und Bearbeiten von Kennwörtern (SNMPv3)
- Konfigurieren von Löschungsintervallen für fehlerhafte Datensätze und der Erkennungszeitdauer für RMX-Fehlermeldungen, um durch Löschen dieser Datenbankeinträge Festplattenspeicher freizugeben.
- Konfigurieren eines Trap-Filters einschließlich Verteilung an alle Hosts
- Rücksetzen aller auf dem RMX oder Assistant ausgelösten Alarme (Setzen auf Status “Aus”)
- Aktivieren/Deaktivieren von Host-Keep-Alive-Traps auf allen Hosts
- Einrichten von MIB2-Parametern
- Herunterladen der MIB-Definitionsdateien

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.1 Benutzeroberfläche

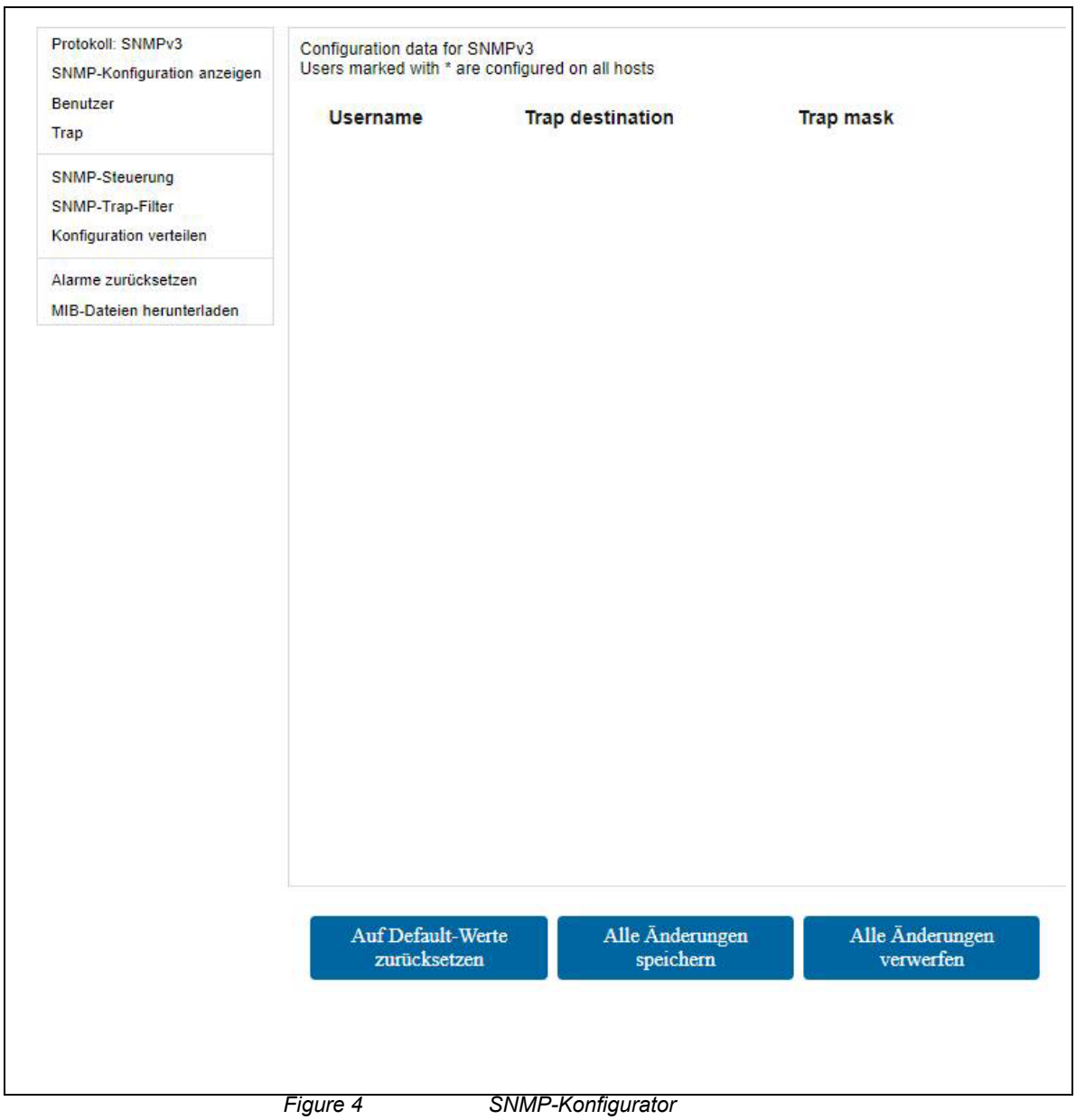


Figure 4 SNMP-Konfigurator

Der linke Bereich der Seite enthält das **Menüfeld**. Im rechten Bereich werden die Konfigurationsdaten angezeigt; dort können auch alle zur Konfiguration notwendigen Aktionen ausgeführt werden.

Menüfeld (linker Bereich)

Im Menüfeld können Sie verschiedene Aktionen auswählen, die nachfolgend aufgelistet und kurz erklärt werden:

- Die oberen Menüpunkte im Menüfeld beziehen sich auf die Konfiguration von SNMPv1 und SNMPv3.
  - **Konfiguration anzeigen**
    Mithilfe dieses Menüpunktes können Sie Konfigurationsdaten zur derzeit ausgewählten SNMP-Version (SNMPv1 oder SNMPv3) anzeigen.
  - **Protokoll: SNMPv3** oder **Protokoll: SNMPv1,**
    Mit dieser Umschaltfläche können Sie zwischen SNMPv1- bzw. SNMPv3-bezogenen Aktionen hin- und herwechseln. Welcher der beiden Menüeinträge jeweils verfügbar ist, hängt von der aktuell ausgewählten SNMP-Version ab.
  - **Benutzer** oder **Community**
    Auch bei diesem Menüpunkt handelt es sich um eine Umschaltfläche. Welcher der beiden Menüeinträge jeweils verfügbar ist, hängt von der aktuell ausgewählten SNMP-Version ab (**Community** für SNMPv1, **Benutzer** für SNMPv3).
  - **Trap**
    Dieser Menüpunkt umfasst alle mithilfe von SNMP-Entität-Traps konfigurierbaren Aktionen. So besteht zum Beispiel die Möglichkeit, eine Trap-Adresse aus einer Benutzer-/Community-Zeichenfolge zu entfernen.
- Die Menüelemente im unteren Teil des Menüfeldes gelten für beide SNMP-Versionen.
  - **SNMP-Steuerung**
    Über die Funktionen der SNMP-Steuerung können Sie das Senden von Keep-Alive-Traps von allen Hosts aus aktivieren, das Senden von Fehlertraps aus dem gesamten 4K-Bereich aktivieren bzw. deaktivieren sowie Standort und Kontaktperson für Hosts von aktiven Knoten, Standby-Knoten oder Quorum-Knoten einrichten. Kontakt und Standort werden für die Einstellungen MIB2 sysLocation und sysContact verwendet.
  - **Trap-Filter**
    Mit dem Leistungsmerkmal SNMP-Konfigurator -> Trap-Filter -> Hostsystemereignisse können Sie den Trap-Filter für Hostsysteme definieren.
  - **Konfiguration verteilen**
    Mit dem Leistungsmerkmal SNMP-Konfigurator -> Konfiguration verteilen können Sie Änderungen an der Konfiguration der Hostsysteme speichern. Folgende Konfigurationsänderungen können auf verbundenen Hosts gespeichert werden:
    - SNMPv3-Einstellung
    - Host-Filter-Einstellung

  - SNMP-Steuerungsparameter

– **Alarme zurücksetzen**
Mit dem Leistungsmerkmal SNMP-Konfigurator-> Alarme zurücksetzen können Sie alle auf dem RMX oder dem Assistant ausgelösten Alarme zurücksetzen (auf den Status “Aus” setzen).

– **MIB-Dateien herunterladen**
dient zum Herunterladen von MIB-Definitionsdateien.

Schaltflächen (rechter Fensterbereich)

Mit den Schaltflächen im rechten Fensterbereich können die über den SNMP-Konfigurator vorgenommenen Konfigurationseinstellungen geändert werden:

- **Auf Default-Werte zurücksetzen**:
Mit diesem Menüpunkt setzen Sie die Konfiguration von SNMPv1 und SNMPv3 auf die Default-Werte zurück und löschen Konfigurationen ohne Benutzer bzw. Community-Zeichenfolgen.
- **Alle Änderungen speichern**:
Hiermit speichern Sie alle Änderungen an der Konfiguration von SNMPv1 und SNMPv3.
- **Alle Änderungen verwerfen**:
Mit diesem Menüpunkt machen Sie alle Konfigurationsänderungen rückgängig und kehren zu dem Konfigurationstand zurück, der nach dem letzten Speichern oder Neustart gültig war.

Solange es ungespeicherte Änderungen im rechten Konfigurationfenster gibt, werden Sie durch eine Meldung über diesen Schaltflächen daran erinnert, dass Änderungen an der Konfiguration vorgenommen wurden, die entweder gespeichert oder verworfen werden sollten.

Verwandte Themen

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.2 SNMPv1/SNMPv3-Konfiguration anzeigen

So können Sie sich die Daten der aktuellen SNMPv1- bzw. SNMPv3-Konfiguration anzeigen lassen:

- Wählen Sie die gewünschte SNMP-Version **Protokoll: SNMPv1** oder **Protokoll: SNMPv3** im Menüfeld.
- Klicken Sie auf **Konfiguration anzeigen**.

  Je nachdem, ob Sie SNMPv1 oder SNMPv3 ausgewählt haben, wird die Konfiguration des dazugehörigen SNMP-Protokolls angezeigt.

Verwandte Themen

Benutzeroberfläche

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.2.1 Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Menüfeld

Das Menüfeld für die SNMPv1-Konfiguration enthält die folgenden Einträge:

- **Community**
  Diese Menüoption umfasst alle mithilfe der SNMPv1-Entität-Community-Zeichenfolge möglichen Aktionen. Sie bietet folgende Möglichkeiten: Community-Zeichenfolge hinzufügen oder Eine Community-Zeichenfolge löschen.

  und

- **Trap**
  See "Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen" on page 34.

Community-Zeichenfolge hinzufügen

- Wählen Sie **Protokoll: SNMPv1**.
- Klicken Sie auf **Community** und wählen Sie **Community hinzufügen** im Menüfeld.
- Geben Sie die Community-Zeichenfolge ein.
- Klicken Sie auf **Hinzufügen**.
- Klicken Sie auf **Alle Änderungen speichern**.

NOTE: Der Wert der Community-Zeichenfolge darf nicht Null sein; dies bedeutet, dass die Zeichenfolge nicht leer sein darf. Außerdem dürfen Sie keine Zeichenfolge eingeben, die bereits in der Konfiguration für SNMPv1 und SNMPv3 existiert.

Nach erfolgreichem Hinzufügen der Zeichenfolge wird wieder der Standard-Bildschirm mit den entsprechenden Daten angezeigt.

Eine Community-Zeichenfolge löschen

Beim Löschen einer Community-Zeichenfolge werden auch alle mit dieser Entität verbundenen Trap-Ziel-Adressen entfernt.

- Wählen Sie **Protokoll: SNMPv1**.
- Klicken Sie im Menüfeld unter **Community** auf **Community löschen**.

  Alle in der Konfiguration vorhandenen Community-Zeichenfolgen werden angezeigt.

- Löschen Sie die ausgewählte Community-Zeichenfolge, indem Sie auf die daneben liegende rote Schaltfläche **X** klicken.
- Klicken Sie auf **Alle Änderungen speichern**.

Verwandte Themen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

3.2.2 Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

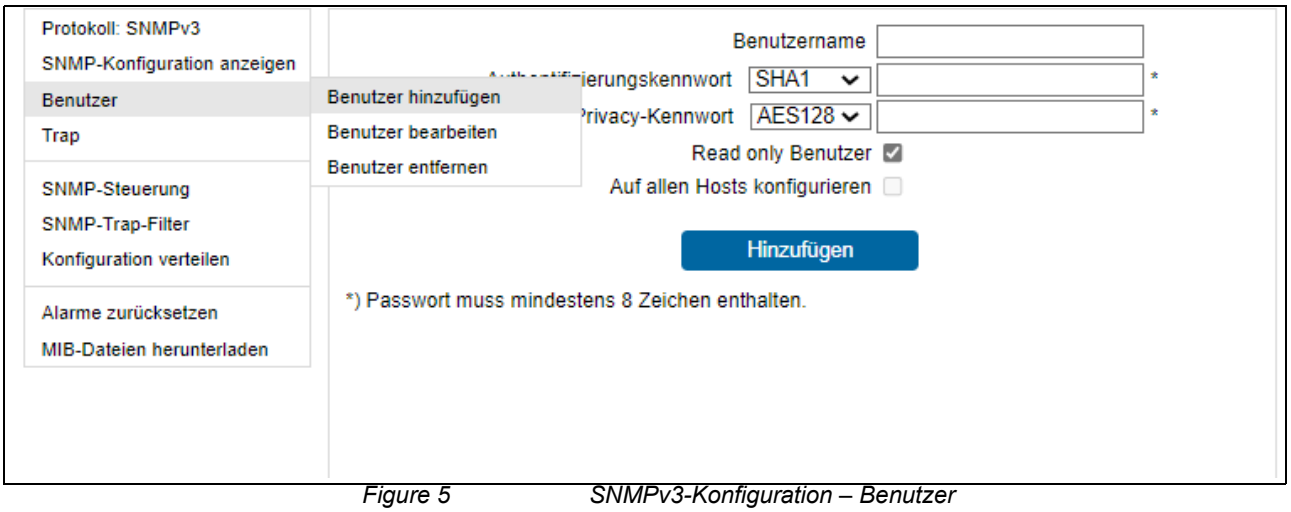


Figure 5 SNMPv3-Konfiguration – Benutzer

Menüfeld

Das Menüfeld für bestimmte SNMPv3-Konfigurationen enthält die folgenden Einträge:

- **Benutzer**
  Diese Menüoption enthält alle Aktionen, die der Benutzer mit der SNMPv3-Entität durchführen kann.
  Er kann Benutzer hinzufügen, Kennwörter bearbeiten oder Benutzer entfernen.

  und

- **Trap:**
  See "Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen" on page 34.

Einen neuen Benutzereintrag hinzufügen

- Wählen Sie **Protokoll: SNMPv3**.
- Klicken Sie im Menüfeld unter **Benutzer** auf **Benutzer hinzufügen**.
- Geben Sie den neuen **Benutzernamen**, das **Authentifizierungskennwort** und das **Privacy-Kennwort** ein.

NOTE: Diese Felder sind Pflichtfelder, dürfen also nicht leer gelassen werden.

- Wenn Sie das Kontrollkästchen **Read only-Benutzer** aktivieren, hat der Benutzer nur Lesezugriff auf die MIBs.
- Wenn Sie das Kontrollkästchen **Auf allen Hosts konfigurieren** aktivieren, wird der Benutzer bei der Verteilung der Konfiguration auf allen verbundenen Hosts mit den gleichen Einstellungen konfiguriert.
- Klicken Sie auf **Hinzufügen**.

Nach erfolgreichem Hinzufügen der Zeichenfolge wird wieder der Standard-Bildschirm mit den neuen Daten angezeigt.

Kennwörter ändern

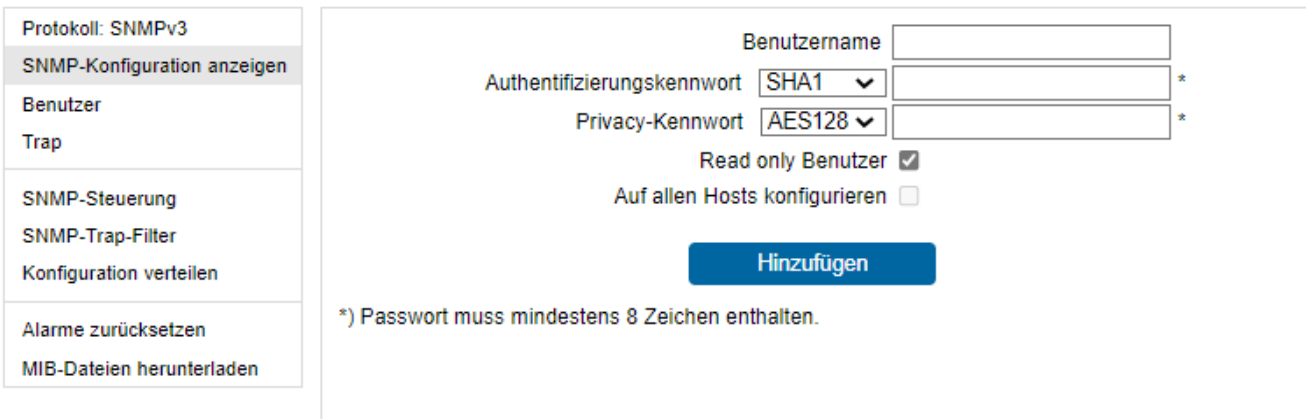


Figure 6 SNMPv3-Konfiguration - Kennwort ändern

- Wählen Sie **Protokoll: SNMPv3**.
- Klicken Sie im Menüfeld unter **Benutzer** auf **Benutzer bearbeiten**.
- Wählen Sie in der Dropdown-Liste **Benutzer auswählen** einen Benutzer aus.
- Jetzt können Sie die folgenden Kennwörter ändern:

  - Authentifizierungskennwort
  - Privacy-Kennwort
- Geben Sie das aktuell gültige Kennwort ein und wiederholen Sie es.
- Klicken Sie auf **Abschicken**.

Einen Benutzereintrag entfernen

- Wählen Sie **Protokoll: SNMPv3**.
- Klicken Sie im Menüfeld unter **Benutzer** auf **Benutzer entfernen**.

  Alle in der aktuellen Konfiguration vorhandenen Benutzereinträge werden angezeigt.
- Löschen Sie den ausgewählten Benutzereintrag, indem Sie auf die daneben liegende rote Schaltfläche **X** klicken.
- Klicken Sie auf **Alle Änderungen speichern**.

Verwandte Themen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

3.3 Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

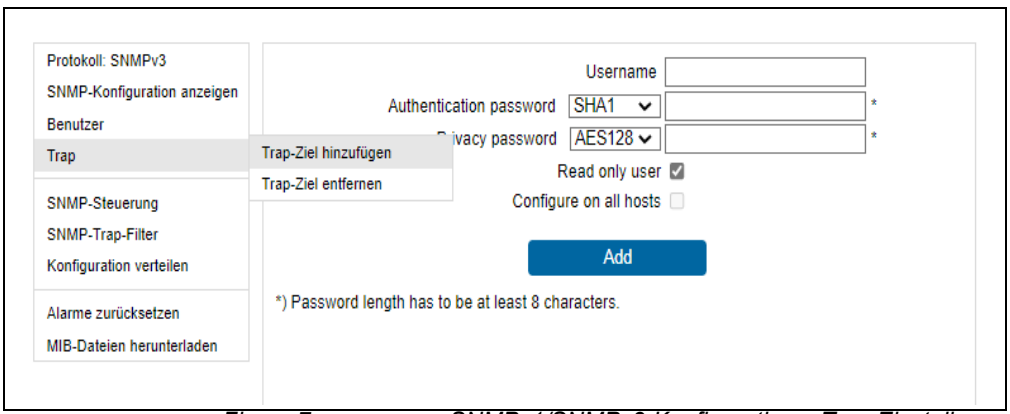


Figure 7 SNMPv1/SNMPv3-Konfiguration – Trap-Einstellungen

Bei der Konfiguration von Trap-Adressen definieren Sie die IP-Adresse des Rechners, an den die Traps von SNMP-Agenten gesendet werden, und verbinden diese Adresse mit der Benutzer/Community-Zeichenfolge.

Menüfeld

Das gemeinsame Menüfeld für SNMPv1 und SNMPv3-Konfigurationen enthält die folgenden Einträge:

- **Trap-Ziel hinzufügen**:
  Definieren Sie die IP-Adresse des Verwaltungssystemrechners, an den die Traps von SNMP-Agenten gesendet werden und verbinden Sie diese Adresse mit der Benutzer/Community-Zeichenfolge.
- **Trap entfernen**:
  Löscht die Verbindung zwischen einer Trap-Adresse und der Benutzer/Community-Zeichenfolge.

Ein neues Trap-Ziel hinzufügen

- Wählen Sie die gewünschte SNMP-Version **Protokoll: SNMPv1** oder **Protokoll: SNMPv3** im Menüfeld.
- Klicken Sie im Untermenü auf **Trap-Ziel hinzufügen**.

  Sie können einen Community- (SNMPv1) oder Benutzereintrag (SNMPv3) auswählen, um diesen durch Hinzufügen mit einer Trap-Ziel-Adresse zu verbinden.

  Name: Für jeden Eintrag kann ein Name hinzugefügt werden. Dieser Name wird nicht im System verwendet; er ist nur als Gedächtnisstütze gedacht.

  SNMP-Version: Die Version des für die Traps verwendeten SNMP-Protokolls.
- Geben Sie für das Trap-Ziel eine IP-Adresse und eine dazu passende Trap-Maske ein. Standardmäßig wird die Trap-Maske auf 255.255.255.255 gesetzt, was genau einem Rechner entspricht.

NOTE: Wenn eine IP-Adresse oder Trap-Maske ungültig ist, können Sie keine weiteren Daten übermitteln.

- Klicken Sie auf **Alle Änderungen speichern**.

NOTE: Sie können keine neue Trap-Adresse hinzufügen, wenn noch keine Community-Zeichenfolgen (SNMPv1) oder Benutzer (SNMPv3) existieren. Eine entsprechende Fehlermeldung wird angezeigt und Sie werden auf eine Seite umgeleitet, auf der Sie einen neuen Eintrag hinzufügen können.

Ein Trap-Ziel entfernen

- Wählen Sie die gewünschte SNMP-Version **Protokoll: SNMPv1** oder **Protokoll: SNMPv3** im Menüfeld.
- Klicken Sie im Untermenü auf **Trap-Ziel entfernen**.

Communities (SNMPv1) oder Benutzer (SNMPv3) mit ihren Trap-Ziel-Adressen werden angezeigt.

- Löschen Sie das ausgewählte Trap-Ziel, indem Sie auf die daneben liegende rote Schaltfläche **X** klicken.
- Klicken Sie auf **Alle Änderungen speichern**.

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.4 SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Über den Menüeintrag **SNMP-Steuerung** können Sie für SNMPv1 und SNMPv3 folgende Aktionen durchführen:

- das Fehlerlöschungsintervall auf einen Wert zwischen 1 und 100 Tage festlegen
- die Erkennungszeitdauer für RMX-Fehlermeldungen festlegen
- das Keep-Alive-Trap-Intervall festlegen
- den Standort des Hostsystems identifizieren
- die Kontaktperson des Hostsystems identifizieren
- festlegen, ob SNMP-Traps gesendet werden oder nicht

Fehlerlöschungsintervall festlegen

- Geben Sie in das Eingabefeld **Anzahl der Tage vor der automatischen Fehlerlöschung (1-100)** die Anzahl der Tage bis zur nächsten Fehlerlöschung ein.
- Klicken Sie auf **Einstellen**.
- Klicken Sie auf **Nur speichern oder Speichern & verteilen**.

Erkennungszeitdauer für RMX-Fehlermeldungen festlegen

RMX-Fehler werden standardmäßig alle 10 Minuten abgefragt und beim Erkennen von neuen Fehlern werden Fehlertraps generiert. Ändern Sie diesen Wert, wenn der Empfang der Traps auf Ihrem NMS oder Ihrem Trap-Receiver zu lange dauert. Der Mindestwert für das Abfrageintervall beträgt 30 Sekunden.

Beim Ändern dieses Wertes wird erroragt neu gestartet; dies wiederum führt dazu, dass die letzten 100 für RMX protokollierten Fehlertraps in die Hista-Datei geschrieben werden.

- Geben Sie in das Eingabefeld **Erkennungszeitdauer für RMX-Fehlermeldungen (Sekunden)** die gewünschte Erkennungszeitdauer ein. Der Standardwert liegt bei 10 Minuten; der Mindestwert beträgt 30 Sekunden.
- Klicken Sie auf **Einstellen**.
- Klicken Sie auf **Nur speichern oder Speichern & verteilen**.

Keep-Alive-Trap-Intervall festlegen

Einige NMS verwenden sog. Keep-Alive-Traps, um zu überwachen, ob das System funktionsbereit ist oder nicht. Wenn diese nicht innerhalb des angegebenen Zeitraums beim NMS eingeht, meldet das NMS einen schwerwiegenden Fehler auf dem überwachten Knoten.

Standardmäßig sind die Keep-Alive-Traps deaktiviert (**Aus**). Die Zeitintervalle für das Senden von Keep-Alive-Traps können hier zentral konfiguriert werden.

- Tragen Sie im Eingabefeld **Keep-Alive-Trap Intervall (Sekunden)** die gewünschte Anzahl von Sekunden ein, um das Keep-Alive-Trap-Sendeintervall festzulegen.
- Aktivieren Sie die Option **Ein**.
- Klicken Sie auf **Nur speichern oder Speichern & verteilen**.

Standort des Hostsystems angeben

Geben Sie den physischen Standort dieses Knotens ein (z. B. *Hessen, Frankfurt am Main, L12/Nord*).

Diese Standortinformationen werden für alle Traps verwendet, die von Assistant, Plattform, CSTA und integrierten SoftGates auf zentralen Host-Bereitstellungen gesendet werden. Auf eigenständigen oder Survivable SoftGates, Enterprise Gateways oder STMIX-Baugruppen werden stattdessen die Standortinformationen von AMO UCSU verwendet.

Kontaktperson für das Hostsystem angeben

Geben Sie für diesen verwalteten Knoten eine Bezeichnung sowie zusätzliche Angaben zur Kontaktperson ein (z .B. *Mustermann, Max, +49 89 xxxxxxx*).

SNMP-Traps senden ein/aus

Hier können Sie das Senden von SNMP-Traps aktivieren (Ein) oder deaktivieren (Aus).

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Überwachung mittels SNMP-get-Anfragen

3.5 Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

3.5.1 Trap-Filter: RMX-Fehlermeldungen

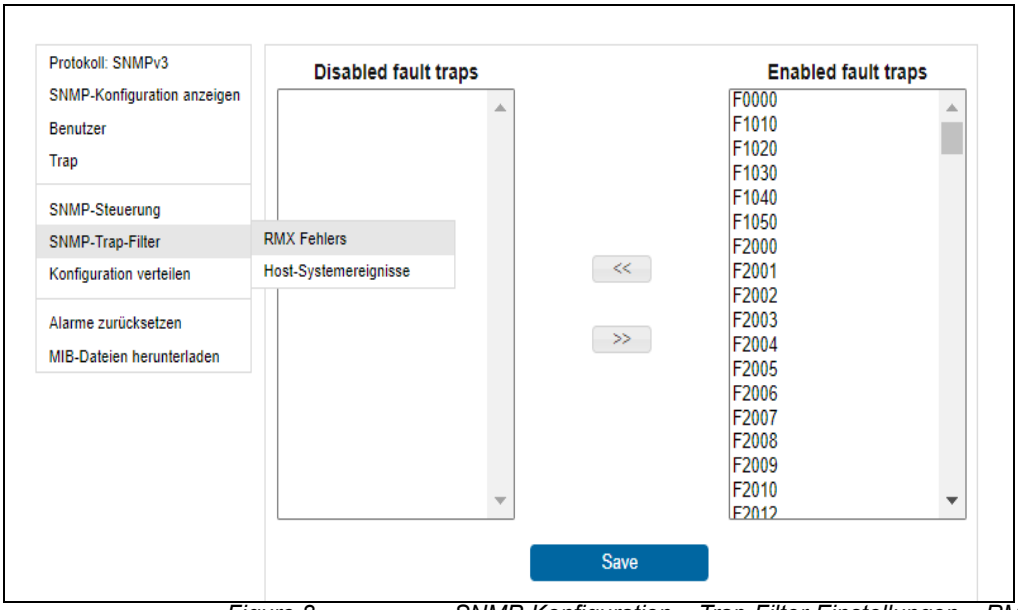


Figure 8 SNMP-Konfiguration – Trap-Filter-Einstellungen – RMX-Fehlermeldungen

Im Bereich **Trap-Filter** – **RMX-Fehlermeldungen** können Sie RMX-Fehlertraps für SNMPv1 und SNMPv3 aktivieren bzw. deaktivieren.

Zwei Spalten mit Fehlertraps werden angezeigt:

- **Deaktivierte Fehlertraps** (Spalte links):
  Listet alle Fehlernummern auf, für die das Versenden von Traps deaktiviert ist.
- **Aktivierte Fehlertraps** (rechte Spalte):
  Listet alle Fehlernummern auf, für die das Versenden von Traps aktiviert ist.

Fehlertraps aktivieren

- Wählen Sie einen oder mehrere Traps in der Spalte **Deaktivierte Fehlertraps** aus.
- Klicken Sie auf die Schaltfläche **<<** zwischen den Spalten.
- Die ausgewählten Traps werden in die Spalte **Aktivierte Fehlertraps** verschoben.
- Klicken Sie auf **Speichern**.
- Klicken Sie auf **Alle Änderungen speichern**.

Fehlertraps deaktivieren

- Wählen Sie einen oder mehrere Traps in der Spalte **Aktivierte Fehlertraps** aus.
- Klicken Sie auf die Schaltfläche **>>** zwischen den Spalten.
- Die ausgewählten Traps werden in die Spalte **Deaktivierte Fehlertraps** verschoben.
- Klicken Sie auf **Speichern**.
- Klicken Sie auf **Alle Änderungen speichern**.

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.5.2 Trap-Filter: Hostsystemereignisse

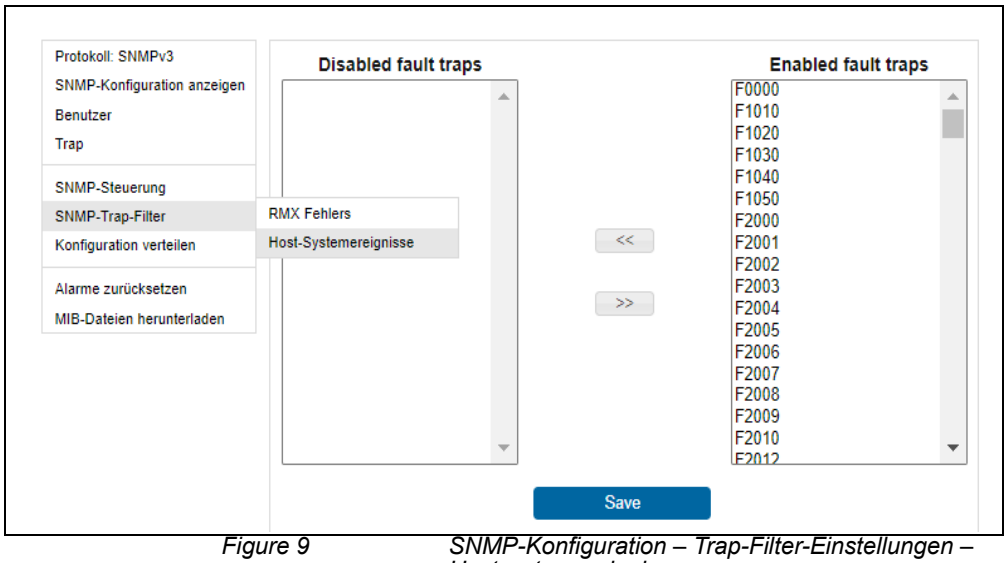


Figure 9 SNMP-Konfiguration – Trap-Filter-Einstellungen – Hostsystemereignisse

Im Bereich **Trap-Filter** – Hostsystemereignisse können Sie die Trap-Filter für alle verbundenen Hosts festlegen.

Sie können Regeln für das Filtern von Traps auf den Hostsystemen definieren. Die Definition wird in einen mehrzeiligen Textfeldbereich eingegeben; dabei ist auf die korrekte Syntax der Ausdrücke zu achten. Die Syntax wird überprüft, so dass ein Filter mit Syntaxfehlern nicht abgespeichert werden kann.

Diese Konfiguration kann Folgendes enthalten:

- Kommentare – alle Texte nach dem Zeichen # bis zum Zeilenende. Ein Kommentar kann am Anfang oder in der Mitte einer Zeile beginnen.
- Bedingungen für separate Zeilen

Anhand dieser Bedingungen können Sie angeben, was herausgefiltert werden soll (d. h. welche Traps nicht durch die Hostsysteme gesendet werden sollten). Jeder Trap, der die in dieser Datei angegebenen Bedingungen erfüllt, wird herausgefiltert.

Bedingungen können Folgendes enthalten:

- Schlüsselwörter: SEVERITY, FACILITY, OID, MSG, TRAP_ID
- Operatoren {=, !=, <, >, <=, >=} für SEVERITY
- Operatoren {=, !=} für FACILITY, OID, TRAP_ID
- Operatoren {MATCH, NOT MATCH} für MSG
- logische Operatoren AND, OR

- Klammern können verschachtelt sein ((... OR ...) AND ...)

Optionen für Schlüsselwörter:

- gültige Werte für SEVERITY: {emergency, alert, critical, error, warning, notice, info, debug}
- gültige Werte für FACILITY: {os4k, kernel, user, mail, daemon, security, syslog}, wobei es sich bei os4k um Traps handelt, die von os4k-Prozessen generiert werden.
- gültige OID-Werte sind in “” gesetzte Zeichenfolgen, die durch ein *-Zeichen abgeschlossen werden können. Der Asterisk steht für eine beliebige Anzahl von Zeichen.
- gültige MSG-Werte sind in “” gesetzte Zeichenfolgen, die Sonderzeichen für reguläre Ausdrücke enthalten können. Hierbei wird die Regex-Syntax unterstützt.
- gültige TRAP_ID-Werte sind in “” gesetzte Zeichenfolgen. Sonderzeichen (Platzhalter) werden nicht unterstützt. Der TRAP_ID-Wert wird mit vordefinierten Werten verglichen und muss einem dieser Werte entsprechen. Wenn er keinem dieser Werte entspricht, wird in der Analysedatei ein vordefinierter TRAP-ID-Fehler protokolliert.

NOTE: Die Platzhalter in OID und in MSG unterscheiden sich dadurch, dass in einer OID-Zeichenfolge * verwendet wird, wohingegen in einer MSG-Zeichenfolge .* verwendet werden muss, da . für ein beliebiges Zeichen steht und * für seine Wiederholung.

Sonstige Regeln:

- Bei Schlüsselwörtern, logischen Operatoren, FACILITY- und SEVERITY-Werten wird immer zwischen Groß- und Kleinschreibung unterschieden.
- Bei Zeichenfolgen in Anführungszeichen ist Groß-/Kleinschreibung zu beachten.
- AND und OR besitzen die gleiche Priorität. Verwenden Sie daher Klammern, um die Prioritätsreihenfolge genau festzulegen.
- Klammern können mehrfach verschachtelt werden, z. B. ((...)...(...)...(...(...)...)).
- Logische Operation zwischen Zeilen ist OR.

Korrekte Einträge einer Konfigurationsdatei:

```
(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 mit angegebener
ID muss natürlich existieren
```

Falsche Einträge (jede Zeile enthält mindestens einen Fehler):

Nicht definierte Operation <> und undefiniertes binäres Minus

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

Für FACILITY sind nur die Operatoren = und != zulässig

```
(FACILITY > USER)
```

Vergleichsoperator darf für eine SEVERITY/FACILITY nicht zweimal verwendet werden

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

Falsche Reihenfolge: das Schlüsselwort SEVERITY muss vor dem Vergleichsoperator stehen

Korrekter Ausdruck (SEVERITY > NOTICE)

```
(NOTICE < SEVERITY)
```

Operation wird für OID nicht unterstützt.

```
OID > "127.5.5.4.1"
```

Das Zeichen * darf innerhalb der Zeichenfolge nicht verwendet werden. Es muss am Ende stehen.

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

Fehlende Anführungszeichen.

```
MSG MATCH 1234:
```

Das Zeichen * kann nicht als Platzhalter interpretiert werden.

Platzhalterverhalten kann für TRAP_ID nicht erwartet werden.

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

Wenn die grafische Benutzeroberfläche des Trap-Filters geöffnet wird, erscheint der zuletzt gespeicherte Filter ganz oben.

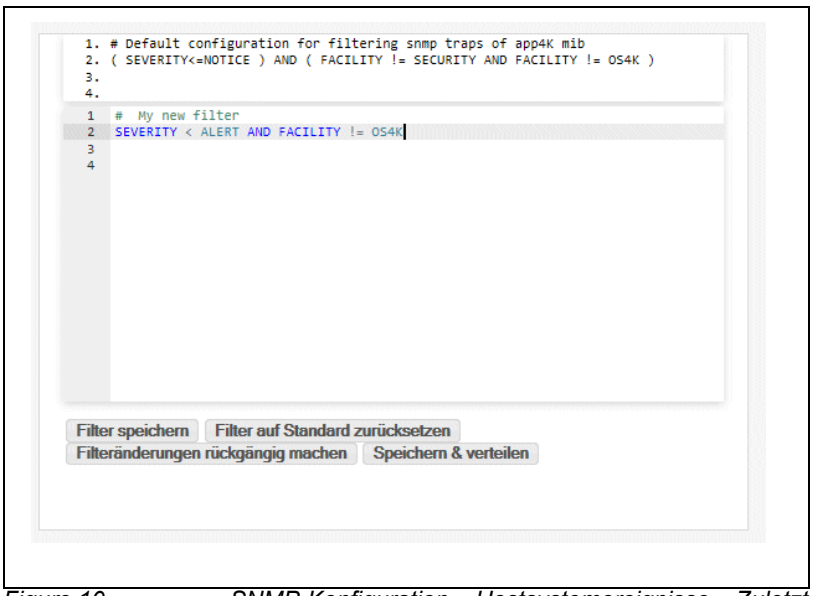


Figure 10 SNMP-Konfiguration – Hostsystemereignisse – Zuletzt gespeicherter Filter

Beschreibung der Aktionsschaltflächen:

- **Filter speichern** – Der Filter wird gespeichert und der Text aus dem bearbeitbaren Bereich wird nach oben kopiert.
- **Filter auf Standard zurücksetzen** – Sie können den Filter auf die Standardeinstellungen zurücksetzen, die während der OS4k-Installation konfiguriert wurden.
- **Filteränderungen rückgängig machen** – Die zuletzt gespeicherte Konfiguration wird wiederhergestellt.
- **Speichern & verteilen** – Der Filter wird gespeichert und die Seite "Konfiguration verteilen" wird geöffnet. Dort können Sie den Filter an alle Hosts im 4k-Bereich verteilen.

Vor Beginn die Verteilung können Sie angeben, welche Daten verteilt werden sollen (**Verteilung an die Hosts**).

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.6 Konfiguration von SNMPv3 auf alle verbundenen Hosts

Über den SNMP-Konfigurator des Assistant können Sie festlegen, ob das vordefinierte SNMPv3-Benutzerprofil mit dem zugehörigen Trap-Ziel auf allen Hosts konfiguriert werden soll.

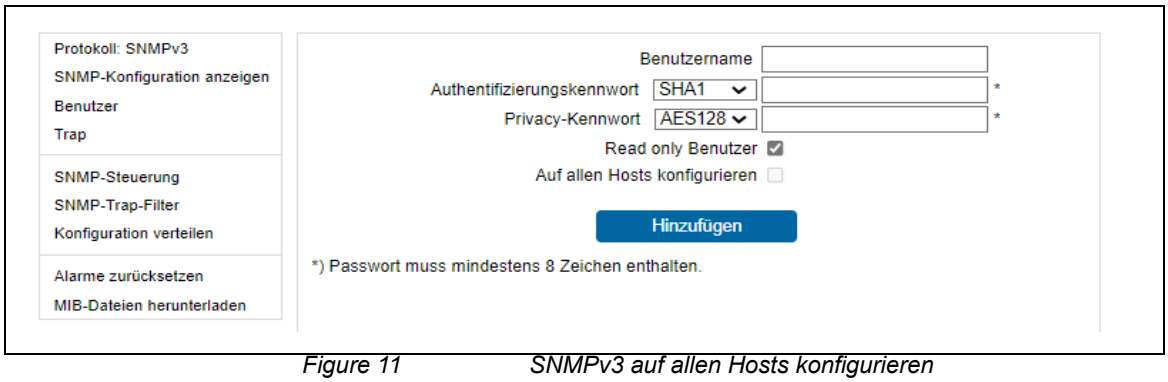


Figure 11 SNMPv3 auf allen Hosts konfigurieren

NOTE: Der Benutzername ist ein alphanumerischer Eintrag ohne Leerzeichen oder Sonderzeichen.
Das Authentifizierungskennwort verwendet den SHA256-Digest-Algorithmus.
Das Privacy-Kennwort verwendet AES128-Verschlüsselung.

Bei der Verteilung der Konfiguration wird dieser Benutzer (einschließlich der diesem Benutzer zugewiesenen Trap-Ziele) auf alle Hostsystemen als schreibgeschützter Benutzer eingerichtet.

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.7 Verteilung an die Hosts

Über den SNMP-Konfigurator des Assistant können Sie festlegen, ob Konfigurationsänderungen auf allen verbundenen Hosts gespeichert werden sollen.

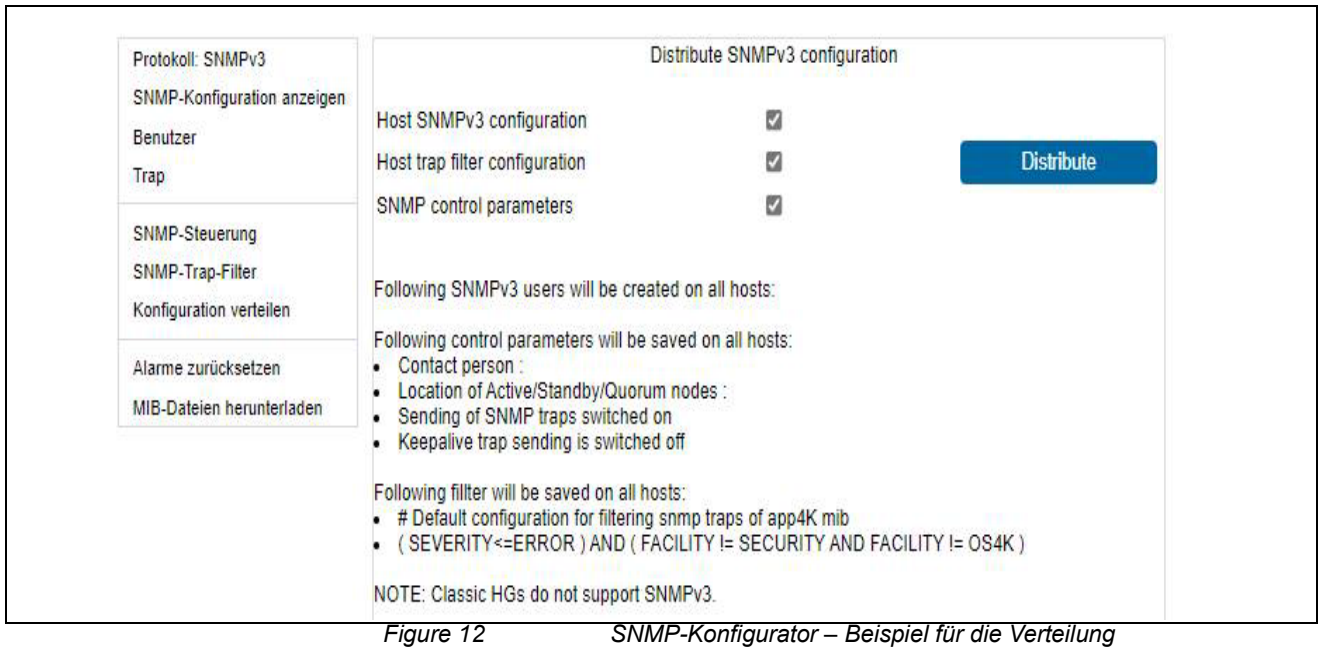


Figure 12 SNMP-Konfigurator – Beispiel für die Verteilung

Folgende Konfigurationsänderungen können auf verbundenen Hosts gespeichert werden:

- SNMPv3-Einstellung
- Host-Filter-Einstellung
- SNMP-Steuerungsparameter

Vor Beginn die Verteilung können Sie angeben, welche Konfiguration an die verbundenen Hosts verteilt werden soll.

Der Verteilungsprozess wird durch Klicken auf die Schaltfläche “Verteilen” gestartet; dies kann einige Sekunden dauern. Bei der Verteilung werden alle ausgewählten Daten konfiguriert und auf allen Knoten im 4k-Bereich gespeichert (außer auf IPDA-basierten APE-Systemen).

NOTE: Für die Verteilung an AP, APEs und STMIX Baugruppen muss zwingend die NGS-IP-Adresse eingerichtet werden.

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.8 Alle Alarme auf dem RMX oder Assistant zurücksetzen

Mit dem SNMP-Konfigurator des Assistant können Sie alle auf dem RMX oder dem Assistant ausgelösten Alarme zurücksetzen (auf den Status "Aus" setzen).

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

MIB-Dateien anzeigen und herunterladen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.9 MIB-Dateien anzeigen und herunterladen

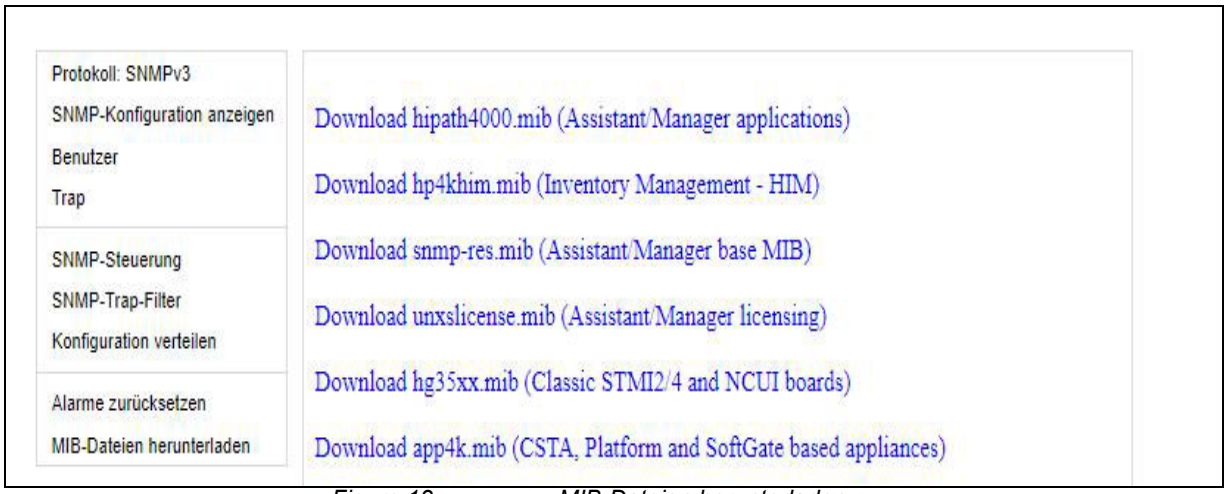


Figure 13 MIB-Dateien herunterladen

So können Sie MIB-Dateien (MIB), mithilfe derer MIB-Strukturen beschrieben werden, anzeigen und herunterladen:

- Klicken Sie auf das Menüfeld **MIB-Dateien herunterladen**.

  Als Nächstes können Sie sich folgende Definitionsdateien anzeigen lassen:

  – OpenScape 4000 MIB,

  – OpenScape/HiPath Inventory Management MIB oder

  – SNMP Research MIB

  – Host 4000 MIB.

  Es wird ein neues Fenster mit der MIB-Beschreibung angezeigt.

Die MIB-Dateien können dann auf der Festplatte gespeichert und später in ein Netzwerkverwaltungssystem importiert werden.

NOTE: Möglicherweise werden die Dateien von Internet Explorer im HTML-Format, d. h. mit HTML-Formatierung, gespeichert. Dadurch wird die Datei für MIB-Browser unlesbar. Vermeiden Sie dies, indem Sie Mozilla Firefox verwenden oder die Datei als Text speichern und sie bei Bedarf in “*.mib” umbenennen.

Verwandte Themen

Benutzeroberfläche

SNMPv1/SNMPv3-Konfiguration anzeigen

Eine Community zur SNMPv1-Konfiguration hinzufügen bzw. von dort entfernen

Benutzer mit Trap-Ziel in SNMPv3-Konfiguration hinzufügen und entfernen, Kennwörter bearbeiten

Trap: Trap-Ziel in SNMPv1/SNMPv3-Konfiguration hinzufügen bzw. entfernen

SNMP-Steuerung: Löschen von Fehlermeldungen konfigurieren

Trap-Filter: Trap-Filter aktivieren bzw. deaktivieren

Konfiguration von SNMPv3 auf alle verbundenen Hosts

Verteilung an die Hosts

Alle Alarme auf dem RMX oder Assistant zurücksetzen

Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Überwachung mittels SNMP-get-Anfragen

3.10 Management von OpenScape 4000-Systemen mit Hilfe der app4K.mib

Die Host 4000 MIB (ASN-1-Syntaxnotation) ist wie folgt aufgebaut:

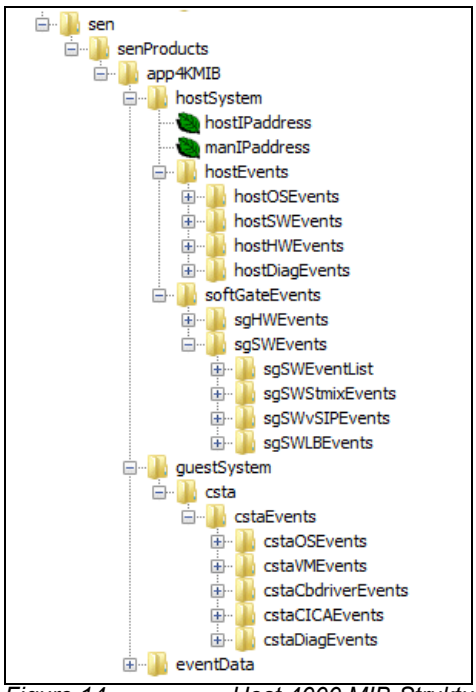


Figure 14 Host 4000 MIB-Struktur

- hostSystem - Hostsystem der OpenScape 4000-Appliance
  - hostEvents - Gruppe von Ereignissen, die von Anwendungen und Überwachungsprozessen generiert werden, die auf der Appliance des OpenScape 4000-Hostsystems ausgeführt werden
    - hostOSEvents - Ereignisse, die vom Betriebssystem des OpenScape 4000 Hostsystems generiert werden
    - hostSWEvents - Ereignisse, die durch Host-Softwareanwendungen und -Daemons generiert werden
    - hostHWEvents – Vom Hostsystem gemeldete Hardware-Ereignisse
    - hostDiagEvents - Für Diagnosezwecke verwendete Ereignisse
  - softGateEvents - Gruppe von Ereignissen, die vom SoftGate-System und SoftGate-relevanter Hardware generiert werden
    - sgHWEvents - Hardwareereignisse, die vom SoftGate-System auf dem Host generiert werden.
    - sgSWEvents – Vom SoftGate-System auf dem Host generierte Softwareereignisse.

- guestSystem – Auf der OpenScape 4000 Host-Appliance laufendes Betriebssystem oder Anwendung
  - csta - Auf der OpenScape 4000 Appliance ausgeführtes CSTA-Gastsystem
    - cstaEvents - Von CSTA generierte Ereignisse
    - cstaOSEvents - Vom Betriebssystem von CSTA generierte Ereignisse
    - cstaVMEvents - Zur VM von CSTA gehörige Ereignisse
    - cstaCbdriverEvents - Zur cbdriver-Software von CSTA gehörige Ereignisse
    - cstaCICAEvents - CICA-bezogene Ereignisse
    - cstaDiagEvents - CSTA-Diagnoseereignisse

Jedes Ereignis bzw. jeder Trap enthält zusätzlich folgende Informationen als Variablenbindungen:

- evSeverity - Schweregrad (Priorität)
- sysDescr – Systembeschreibung aus der MIB2 des Hosts
- sysName – Systemname aus der MIB2 des Hosts
- sysLocation – Systemstandort aus der MIB2 des Hosts
- hostIPaddress – IP-Adresse des Hosts, der den Trap generiert
- manIPaddress – Clan-IP-Adresse des HiPath 4000 Assistant, die für die Verwaltung der SNMP-Einstellung verwendet wird
- eventDateTime – Datum und Uhrzeit für das Auftreten des Ereignisses
- evDescr - Ausführlicher Text der Ereignismeldung

3.10.1 Schweregrad des Ereignisses (evSeverity)

Die Host 4000 MIB verwendet die in syslog-ng (RFC 5424) angegebenen Schweregrade:

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 15 Host 4000 MIB – Schweregrade

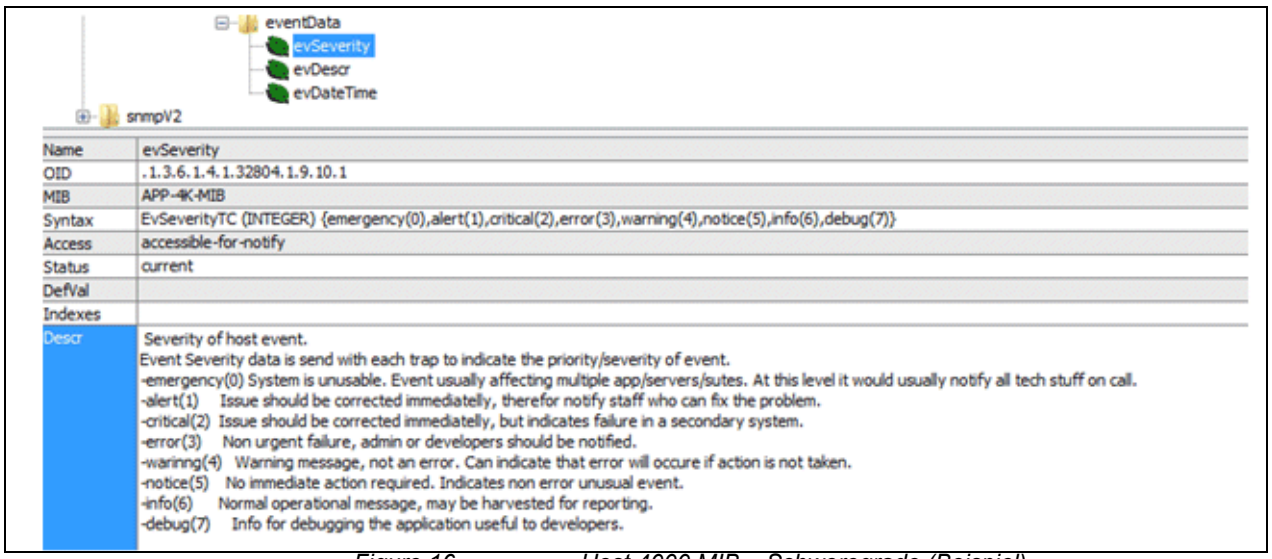


Figure 16 Host 4000 MIB – Schweregrade (Beispiel)

3.10.2 hostOSEvents

Der hostOSEvents-Trap verwendet ein generisches Trap-Modell, d. h. man kann am Trap-Namen nicht erkennen, welche Art von Fehler aufgetreten ist. Jeder Trap beinhaltet eine evDescr-Ereignisbeschreibung als Variablenbindung; diese wird verwendet, um die Ursache des Fehlers zu ermitteln. Am Trap-Namen sind nur der Schweregrad (d. h. die Priorität) des Traps und die Facility (d. h. das OS-Subsystem, das den Trap generiert) erkennbar.

Beispiel: Hier sehen Sie das Protokoll eines Trap-Empfängers beim Empfang eines hostOSSecurityErrEv-Traps, aus dem hervorgeht, dass dieser Fehler vom security-Subsystem des Betriebssystems generiert wurde; um die genaue Fehlerursache zu ermitteln, müssen Sie zusätzlich die evDescr-Variablenbindung überprüfen:

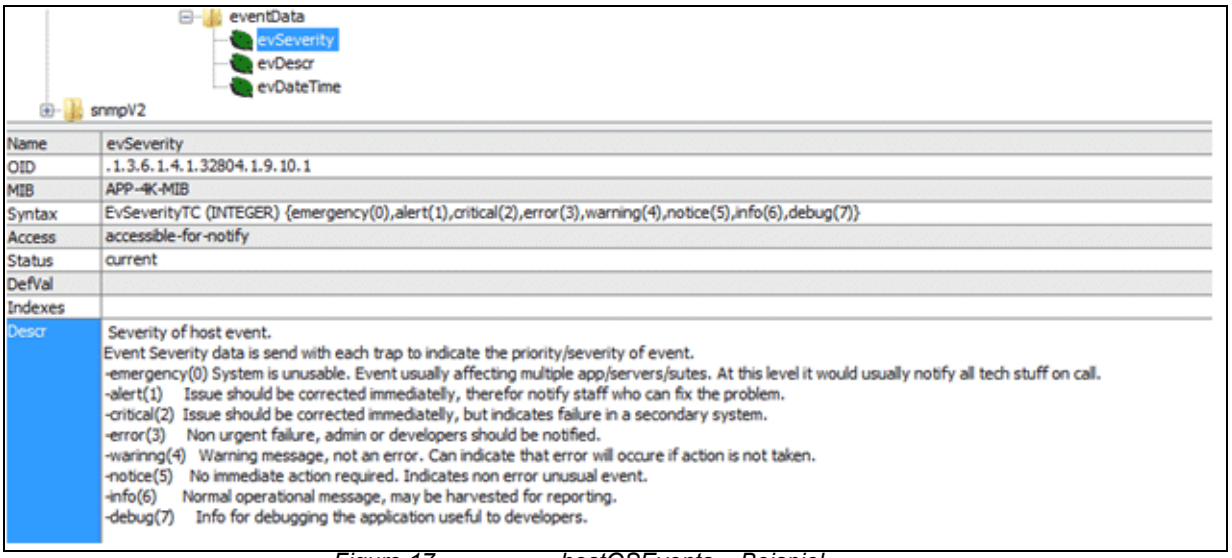


Figure 17 hostOSEvents – Beispiel

Das SNMP-Modul ist standardmäßig so eingestellt, dass vom Betriebssystem nur Trap-Meldungen mit Schweregraden bis "emerg" gesendet werden. Meldungen mit niedriger Priorität werden nicht als SNMP-Traps gesendet.

hostOSEvents umfasst folgende Trap-Kategorien:

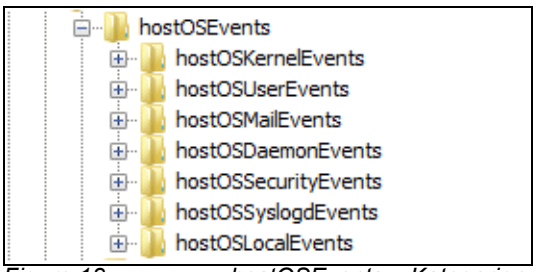


Figure 18 hostOSEvents – Kategorien

- hostOSKernelEvents – Systemkernel-Meldungen des Host-Betriebssystems

- hostOSUserEvents – Anwendungs-/Dienstmeldungen des Host-Betriebssystems
- hostOSMailEvents – E-Mail-Systemmeldungen des Host-Betriebssystems
- hostOSDaemonEvents – Meldungen von System-Daemons des Host-Betriebssystems
- hostOSSecurityEvents - Sicherheits-/Autorisierungsmeldungen des Host-Betriebssystems
- hostOSSyslogdEvents - Intern von syslogd generierte Meldungen des Host-Betriebssystems
- hostOSLocalEvents - Vom Administrator oder von Anwendungen des Host-Betriebssystems generierte Meldungen

3.10.3 hostSWEvents

Nachstehend werden einige Software-basierte Ereignisse, die von OpenScape 4000-Prozessen/Überwachungsanwendungen auf dem Host generiert werden, aufgeführt:

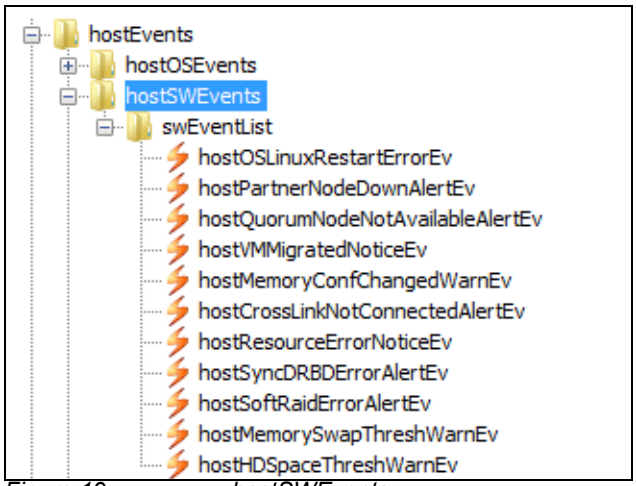


Figure 19 hostSWEvents

- hostOSLinuxRestrtErrorEv - Neustart des Host-Betriebssystems.
- hostPartnerNodeDownAlertEv – Duplex-System: ein Knoten ist außer Betrieb
- hostQuorumNodeNotAvailableAlertEv – Separates Duplex-System: Quorum-Knoten ist nicht verfügbar
- hostVMMigratedNoticeEv – VM wurde über vMotion auf einen anderen physischen Server migriert

- hostMemoryConfChangedWarnEv – Speicherkonfiguration von VM wurde geändert
- hostCrossLinkNotConnectedAlertEv – Querverbindung unterbrochen. Connector und Duplex-Systeme überprüfen.
- hostResourceErrorNoticeEv – Systemanwendungsfehler, nur zur Info – Funktionalität der Ressource überprüfen
- hostSyncDRBDErrorAlertEv – DRBD-Fehler, Duplex-Funktionalität überprüfen
- hostSoftRaidErrorAlertEv – SoftRaid-Fehler– Erstellung der Recovery-HD überprüfen
- hostMemorySwapThreshWarnEv – System swappt – RAM-Auslastung überprüfen
- hostHDSpaceThreshWarnEv – Speicherplatz auf Hard Disk – Schwellwert überschritten

3.10.4 hostHWEvents

Nachstehend werden einige Hardware-basierte Ereignisse, die von OpenScape 4000-Prozessen/Überwachungsanwendungen auf dem Host generiert werden, aufgeführt:

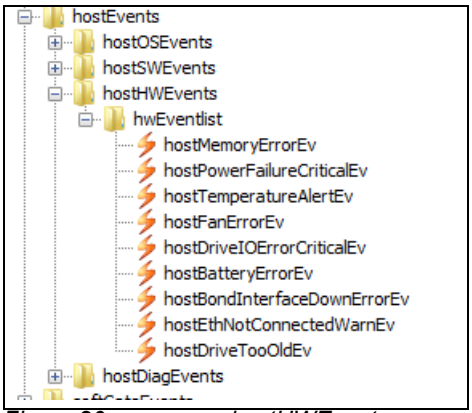


Figure 20 hostHWEvents

- hostMemoryErrorEv – Speicherfehler, Speicher muss ausgetauscht werden
- hostPowerFailureCriticalEv – Stromausfall AC/DC-Netzteil, Netzteil muss ausgetauscht werden
- hostTemperatureAlertEv – CPU-Temperatur hat den Schwellwert überschritten
- hostFanErrorEv – Lüfterfehler – Lüfter muss ausgetauscht werden
- hostDriveIOErrorCriticalEv - I/O-Fehler Festplatte – HD/SSD überprüfen

- hostBateryErrorEv – BIOS-Batterie muss ausgetauscht werden
- hostBondInterfaceDownErrorEv - Bonding-Schnittstellen: redundante Schnittstelle außer Betrieb, Konnektivität überprüfen
- hostEthNotConnectedWarnEv - Ethernet-Schnittstelle konfiguriert, aber nicht verbunden
- hostDriveTooOld - Die Einschaltstunden der Festplatte haben den Standard-Schwellenwert überschritten. Festplatte ersetzen oder auf neuere Hardware wechseln

3.10.5 hostDiagEvents

Die SNMP-Traps können als Diagnostik-Traps verwendet werden. Dies gilt nur für zwei Traps:

Figure 21 hostDiagEvents

- hostKeepAliveInfoEv – Der regelmäßig auf Basis des eingerichteten Keep-Alive-Trap-Intervalls generierte Trap. Wenn das NMS diesen Trap empfängt, bedeutet dies, dass das System funktionsfähig ist.
- hostTestDebugEv– Dieser Trap wird generiert, wenn der Benutzer in der SNMP-Konfiguration des Portals auf die Schaltfläche Testen klickt. Er wird nur verwendet, um zu testen, ob das SNMP-Modul funktioniert, und sendet Traps an vordefinierte Trap-Ziele.

3.10.6 sgHWEvents

Die Hardware-basierten Ereignisse, die vom auf dem Host-Betriebssystem laufenden SoftGate-System generiert werden.

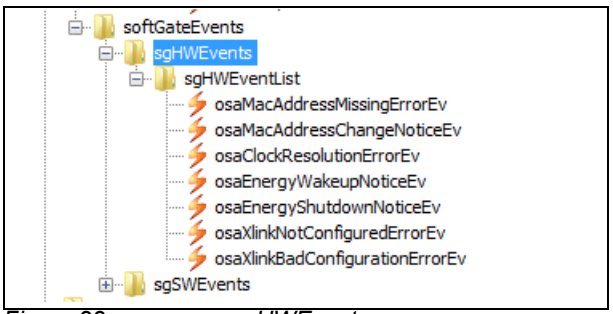


Figure 22 sgHWEvents

- osaMacAddressMissingErrorEv – Konfigurationsproblem beim OSA-Modul – MAC-Adresse fehlt
- osaMacAddressChangeNoticeEv – Konfigurationsproblem beim OSA-Modul – MAC-Adresse geändert
- osaClockResolutionErrorEv – Taktauflösung ungenügend für OSA-Nutzung
- osaEnergyWakeupNoticeEv – Energiesparmodus aktiv: Start nach Aufwachen (Wakeup)
- osaEnergyShutdownNoticeEv – Energiesparmodus aktiv: Herunterfahren gestartet
- osaXlinkNotConfiguredErrorEv – Xlink-LAN-Schnittstelle ist nicht konfiguriert

- osaXlinkBadConfigurationErrorEv – Xlink-Schnittstelle ist identisch mit IPDA Schnittstelle, z. B. Xlink-LAN-Schnittstelle ist nicht konfiguriert oder die IP-Adresse ist ungültig

3.10.7 sgSWEvents

Hardware-basierte Ereignisse, die vom auf dem Host laufenden SoftGate-System generiert werden; diese lassen sich in vier Kategorien unterteilen:

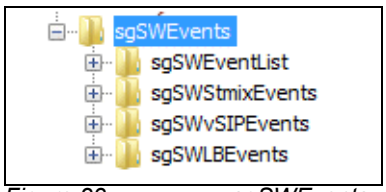


Figure 23 sgSWEvents

- sgSWLBEvents – OpenSIPS-Load-Balancer-Ereignisse
- sgSWvSIPEvents – vHG3500 (SIP)-Ereignisse
- sgSWStmixEvents – STMIX-Ereignisse
- sgSWEventList – Die übrigen vom SoftGate-System generierten Software-Ereignisse

3.10.7.1 sgSWLBEvents

Zu den OpenSIPS-Load-Balancer-Ereignissen gehören u. a. folgende Ereignisse:

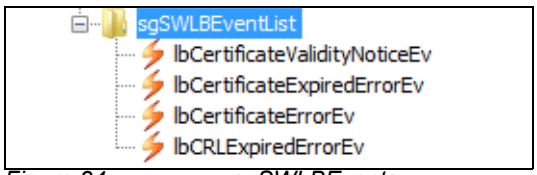


Figure 24 sgSWLBEvents

- lbCertificateValidityNoticeEv – OpenSIPS-Load-Balancer-Sicherheit aktiv und SPE-Zertifikat läuft ab
- lbCertificateExpiredErrorEv – OpenSIPS-Load-Balancer-Sicherheit aktiv und SPE-Zertifikat abgelaufen
- lbCertificateErrorEv – OpenSIPS-Load-Balancer-Sicherheit aktiv und SPE-Zertifikatsprobleme
- lbCRLExpiredErrorEv – OpenSIPS-Load-Balancer-Sicherheit aktiv und Zertifikatssperrliste (CRL) abgelaufen

3.10.7.2 sgSWvSIPEvents

Zu den vHG3500 (SIP)-Ereignissen gehören u. a. folgende Ereignisse:

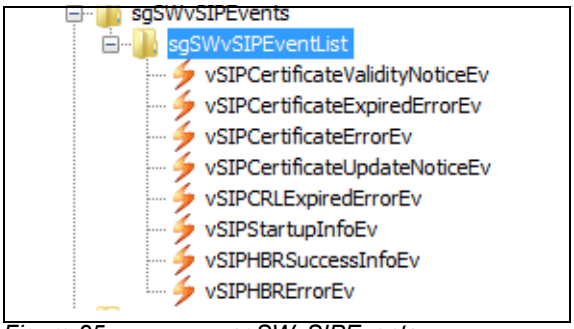


Figure 25 sgSWvSIPEvents

- vSIPCertificateValidityNoticeEv – SPE aktiv und SPE-Zertifikat läuft ab
- vSIPCertificateExpiredErrorEv – SPE aktiv und SPE-Zertifikat abgelaufen
- vSIPCertificateErrorEv – SPE aktiv und SPE-Zertifikatsprobleme
- vSIPCertificateUpdateNoticeEv – SPE aktiv und SPE-Zertifikat wurde verlängert
- vSIPCRLExpiredErrorEv – SPE aktiv und Zertifikatssperrliste (CRL) abgelaufen
- vSIPStartupInfoEv – vHG3500-Startup-Ereignis
- vSIPHBRSuccessInfoEv – HBR-IP-Adresse im AMO konfiguriert. Automatische Wiederherstellung der Konfiguration erfolgreich abgeschlossen
- vSIPHBRErrorEv – HBR-IP-Adresse im AMO konfiguriert, aber ungültige Anmeldeinformationen oder ungültige Adresse. Automatische Wiederherstellung der Konfiguration fehlgeschlagen

3.10.7.3 sgSWStmixEvents

Zu den STMIX-Ereignissen gehören u. a. folgende Ereignisse:

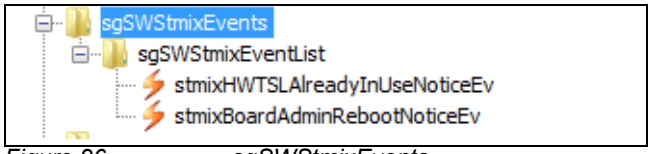


Figure 26 sgSWStmixEvents

- stmixHWTSLAlreadyInUseNoticeEv – Timeslot wird bereits verwendet und im SG oder STMIX von RTO automatisch gelöscht
- stmixBoardAdminRebootNoticeEv – Baugruppe wird gezielt neu gestartet

3.10.7.4 sgSWEventList

Die verbleibenden vom SoftGate generierten Softwareereignisse, die nicht baugruppenspezifisch sind:

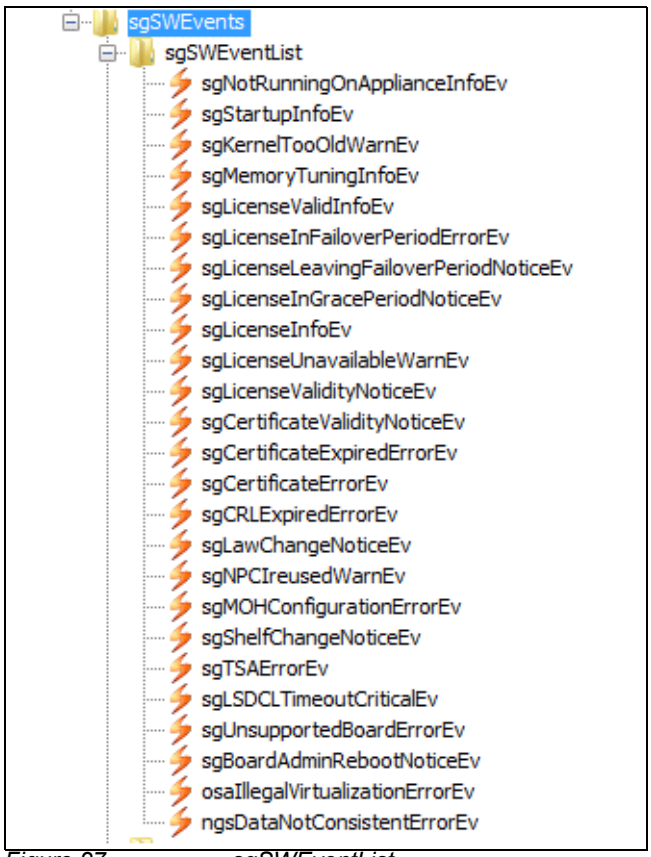


Figure 27 sgSWEventList

- sgNotRunningOnApplianceInfoEv – SoftGate läuft nicht auf einer Appliance

- sgStartupInfoEv – Informationen über die Plattform, die beim Hochfahren angezeigt werden. SG auf VM,UNKNOWNVM,HPA500A,HPA500I,DSCXL2,COTS oder unbekannt.
- sgKernelTooOldWarnEv – Kernel ist zu alt für die SG-Nutzung
- sgMemoryTuningInfoEv – Auf SoftGate-HW mit 4 GB Speicher wird der Webservice automatisch nach 7 Tagen deaktiviert, um den Speicherverbrauch zu reduzieren.
- sgLicenseValidInfoEv – SoftGate-Lizenz ist gültig.
- sgLicenseInFailoverPeriodErrorEv – CLA-Lizenzierungsserver wahrscheinlich nicht erreichbar.
- sgLicenseLeavingFailoverPeriodNoticeEv – CLA-Lizenzierungsserver wieder erreichbar.
- sgLicenseInGracePeriodNoticeEv – SoftGate-Lizenz befindet sich in der Grace Period.
- sgLicenseInfoEv – Meldung von CsCM.
- sgLicenseUnavailableWarnEv – SoftGate-Lizenz nicht verfügbar
- sgLicenseValidityNoticeEv – Gültigkeitsdauer der SoftGate-Lizenz.
- sgCertificateValidityNoticeEv – SPE aktiv und SPE-Zertifikat läuft ab.
- sgCertificateExpiredErrorEv – SPE aktiv und SPE-Zertifikat abgelaufen
- sgCertificateErrorEv – SPE aktiv und SPE-Zertifikatsprobleme
- sgCRLExpiredErrorEv – SPE aktiv und Zertifikatssperrliste (CRL) abgelaufen
- sgLawChangeNoticeEv – Law-Konfiguration für Slot (EBT) geändert.
- sgNPCIreusedWarnEv – IPDA-Port wird wiederverwendet.
- sgMOHConfigurationErrorEv – Konfigurationsproblem bei Wartemusik (MOH).
- sgShelfChangeNoticeEv – Typ oder Konfiguration des SoftGate-Baugruppenrahmens wurde geändert; SoftGate wird automatisch neu gestartet.
- sgTSAErrorEv – TSA-Fehler
- sgLSDCLTimeoutCriticalEv – Neustart von SoftGate wegen Zeitüberschreitung des nativen lsdcl.
- sgUnsupportedBoardErrorEv – Baugruppentyp wird in SoftGate nicht unterstützt (ist aber einfach per AMO konfigurierbar).
- sgBoardAdminRebootNoticeEv – Baugruppe wird gezielt neu gestartet

- osaIllegalVirtualizationErrorEv – Illegale Virtualisierung für Baugruppe oder Modul.
- ngsDataNotConsistentErrorEv – NGS-Adresse ist konfiguriert und NCUI-Payload-IP der RMX-Baugruppendaten unterscheidet sich von der IP in der NGS-Datenbank.

3.10.8 cstaEvents

Die auf dem aktiven Knoten von OpenScape 4000 laufende CSTA sendet auch SNMPv3-Traps von ihrem Betriebssystem und ihren CSTA-Prozessen.

3.10.8.1 cstaOSEvents

Der cstaOSEvents-Trap verwendet ein generisches Trap-Modell, d. h. man kann am Trap-Namen nicht erkennen, welche Art von Fehler aufgetreten ist. Jeder Trap beinhaltet eine evDescr-Ereignisbeschreibung als Variablenbindung; diese wird verwendet, um die Ursache des Fehlers zu ermitteln. Am Trap-Namen sind nur der Schweregrad (d. h. die Priorität) des Traps und die Facility (d. h. das OS-Subsystem, das den Trap generiert) erkennbar.

Das SNMP-Modul ist standardmäßig so eingestellt, dass vom Betriebssystem nur Trap-Meldungen mit Schweregraden bis "emerg" gesendet werden. Meldungen mit niedriger Priorität werden nicht als SNMP-Traps gesendet.

cstaOSEvents umfasst folgende Trap-Kategorien:

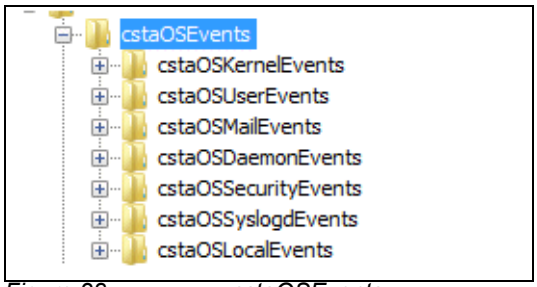


Figure 28 cstaOSEvents

- cstaOSKernelEvents – Kernel-Meldungen des CSTA-Betriebssystems
- cstaOSUserEvents – Anwendungs-/Dienstmeldungen des CSTA-Betriebssystems
- cstaOSMailEvents – E-Mail-Systemmeldungen des CSTA-Betriebssystems
- cstaOSDaemonEvents – Meldungen von System-Daemons des CSTA-Betriebssystems
- cstaOSSecurityEvents – Sicherheits-/Autorisierungsmeldungen des CSTA-Betriebssystems

- cstaOSSyslogdEvents – Intern von syslogd generierte Meldungen des CSTA-Betriebssystems
- cstaOSLocalEvents - Vom Administrator oder von Anwendungen des CSTA-Betriebssystems generierte Meldungen

3.10.8.2 cstaVMEvents

Ereignisse im Zusammenhang mit der Überwachung und Prozessen der virtuellen Maschine von CSTA umfassen u. a.:

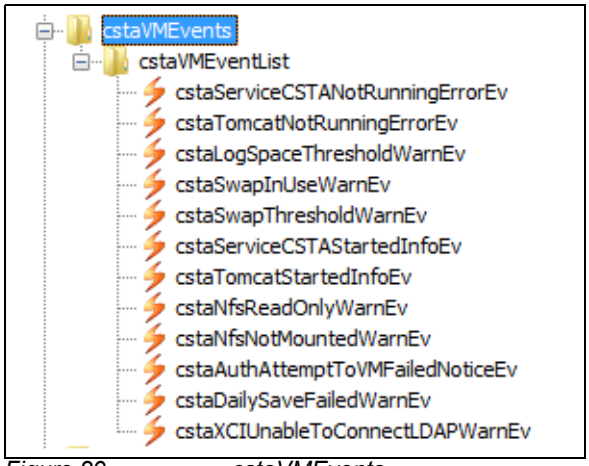


Figure 29 cstaVMEvents

- cstaServiceCSTANotRunningErrorEv – CSTA-Dienst wird nicht ausgeführt
- cstaTomcatNotRunningErrorEv – Tomcat-Dienst wird nicht ausgeführt
- cstaLogSpaceThresholdWarnEv – Log-Partition voll/Schwellwert überschritten
- cstaSwapInUseWarnEv – System swappt
- cstaSwapThresholdWarnEv – Swap-Volume voll/Schwellwert überschritten
- cstaServiceCSTAStartedInfoEv – CSTA-Dienst gestartet
- cstaTomcatStartedInfoEv – Tomcat-Server gestartet
- cstaNfsReadOnlyWarnEv – NFS schreibgeschützt gemountet
- cstaNfsNotMountedWarnEv - NFS nicht gemountet
- cstaAuthAttemptToVMFailedNoticeEv – Fehlgeschlagener Authentifizierungsversuch auf VM
- cstaDailySaveFailedWarnEv – Tägliche automatische Sicherung für Neuinstallation fehlgeschlagen
- cstaXCIUnableToConnectLDAPWarnEv – XCI kann keine Verbindung zu LDAP herstellen

3.10.8.3 cstaCdbDriverEvents

Zur cbdriver-Software von CSTA gehörige Ereignisse umfassen u. a.:

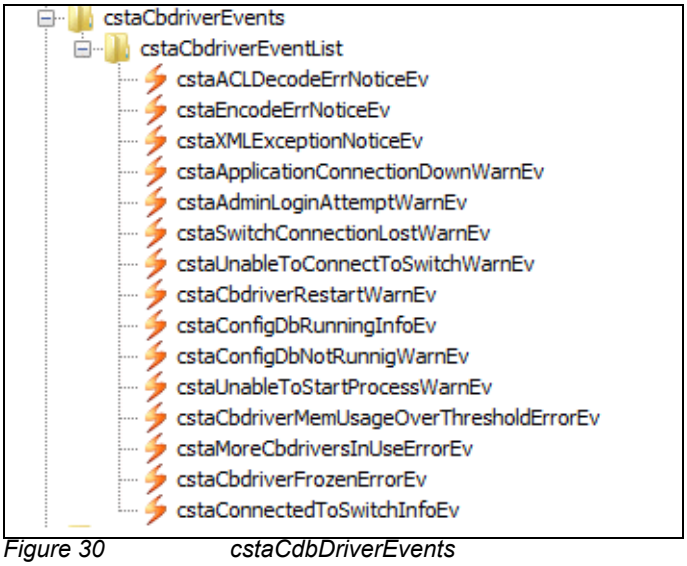


Figure 30 cstaCdbDriverEvents

- cstaACLDecodeErrNoticeEv – ACL-Decodierungsfehler
- cstaEncodeErrNoticeEv – CSTA-Codierungsfehler
- cstaXMLExceptionNoticeEv – XML-Ausnahmefehler
- cstaApplicationConnectionDownWarnEv – Anwendungsverbindung unterbrochen
- cstaAdminLoginAttemptWarnEv – Login-Versuch mit Admin
- cstaSwitchConnectionLostWarnEv – Verbindung zur Anlage unterbrochen
- cstaUnableToConnectToSwitchWarnEv – Verbindungsaufbau zur Anlage nicht möglich, AMO-Konfiguration überprüfen
- cstaCbdriverRestartWarnEv – cbdriver wurde mit <Fehler> angehalten – neu gestartet
- cstaConfigDbRunningInfoEv – Configdb wird ausgeführt
- cstaConfigDbNotRunnigWarnEv - Configdb wird nicht ausgeführt
- cstaUnableToStartProcessWarnEv - Prozess kann nicht gestartet werden – siehe evDescr (Ereignisbeschreibung) des Traps
- cstaCbdriverMemUsageOverThresholdErrorEv – cbdriver-Speicherauslastung liegt über dem Schwellwert; Treiber neu starten
- cstaMoreCbdriversInUseErrorEv – Mehr als N cbdrivers im Einsatz

- cstaCbdriverFrozenErrorEv – cbdriver-Prozess hängt im Speicher; Prozess manuell killen
- cstaConnectedToSwitchInfoEv – CSTA-Verbindung zur Anlage hergestellt

3.10.8.4 cstaCICAEvents

CICA-Ereignisse umfassen u. a.:

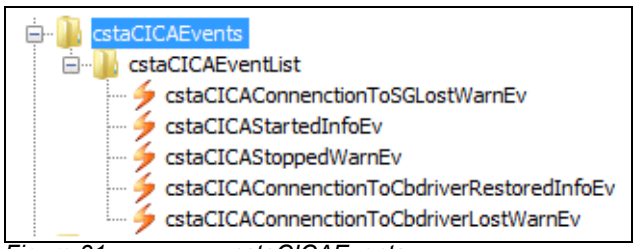


Figure 31 cstaCICAEvents

- cstaCICAConnenctionToSGLostWarnEv – CICA-Verbindung zu SG unterbrochen
- cstaCICAStartedInfoEv – CICA gestartet
- cstaCICAStoppedWarnEv – CICA gestoppt
- cstaCICAConnenctionToCbdriverRestoredInfoEv – CICA-Verbindung zu cbdriver wiederhergestellt
- cstaCICAConnenctionToCbdriverLostWarnEv – CICA-Verbindung zu cbdriver unterbrochen

3.10.8.5 cstaDiagEvents

Ereignisse, die für CSTA-Diagnosezwecke verwendet werden, umfassen u. a.:

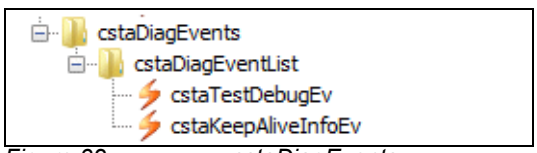


Figure 32 cstaDiagEvents

- cstaTestDebugEv – Ereignis, das zum Testen der SNMP-Funktionalität von CSTA verwendet wird.
- cstaKeepAliveInfoEv – Von der CSTA-Software gesendetes Keep-Alive-Ereignis

3.11 Überwachung mittels SNMP-get-Anfragen

Der auf jedem Host von beliebigen 4k-Systemen aktive Net-SNMP-Agent stellt über das SNMP-Protokoll eine Vielzahl von Leistungsinformationen bereit.

Darüber hinaus kann der Agent auf Anfrage auch eine Liste der auf dem System installierten RPM-Pakete generieren, eine Liste der aktuell auf dem System laufenden Prozesse oder die Netzwerk-Konfiguration des Systems.

Dieser Abschnitt enthält eine kurze Übersicht über die in der SNMP-Host-Ressourcen-MIB, USDAVIS MIB (UCD-SNMP-MIB, UCD-DISKIO-MIB) und IF-MIB verfügbaren Daten.

3.11.1 UCD-SNMP-MIB

Der Großteil der systemspezifischen Leistungsdaten befindet sich in der UCD-SNMP-MIB.

3.11.1.1 Überwachung der Prozessorauslastung

Die systemStats-OID stellt eine Reihe von Zählern für die Prozessorauslastung zur Verfügung:

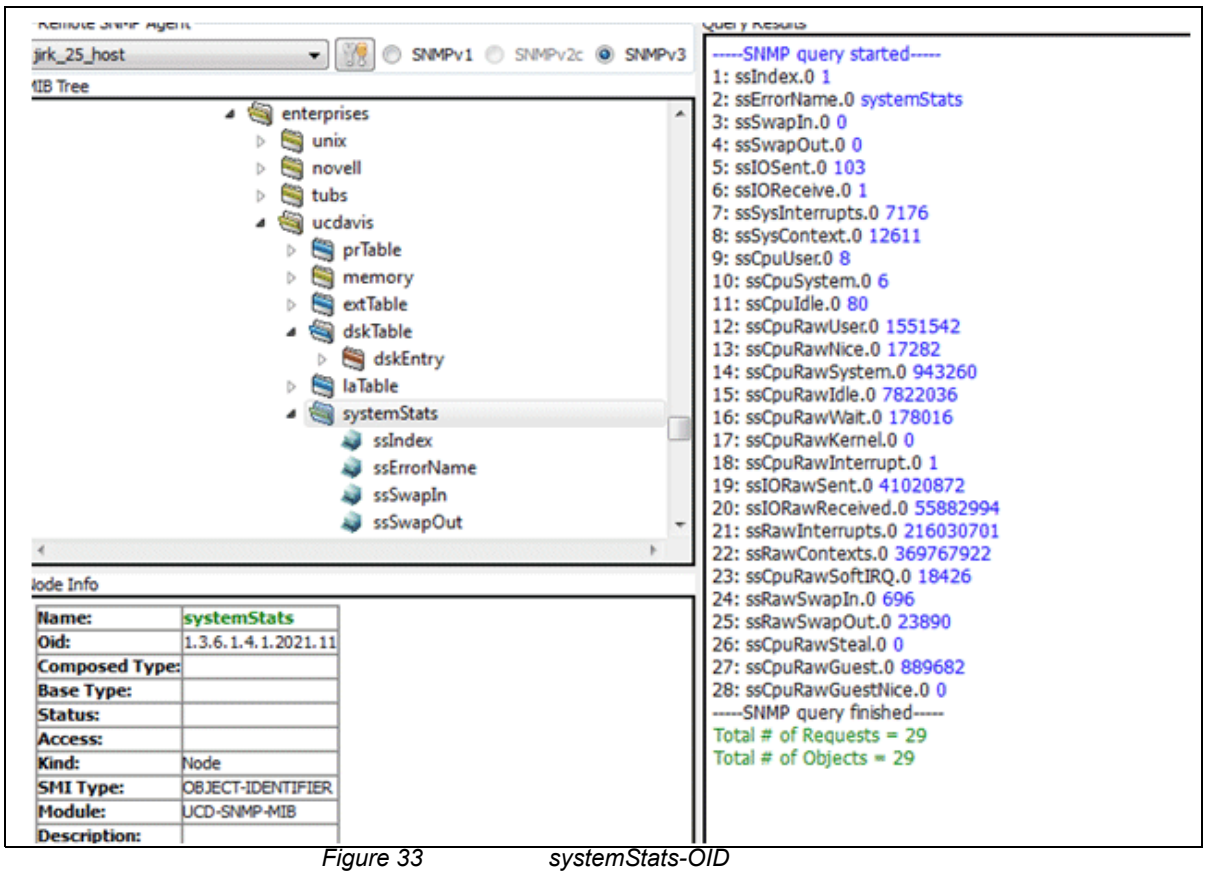


Figure 33 systemStats-OID

Insbesondere die OIDs ssCpuRawUser, ssCpuRawSystem, ssCpuRawWait und ssCpuRawIdle OIDs stellen Zähler bereit, anhand derer ermittelt werden kann, ob ein System den Großteil seiner Prozessorzeit im Kernel-Space, User-Space oder I/O-Space verbringt. ssRawSwapIn und ssRawSwapOut sind hilfreich, wenn es darum geht zu ermitteln, ob ein System nicht mehr über genügend Arbeitsspeicher verfügt.

3.11.1.2 Überwachung der Speicherauslastung

Speicherinformationen sind verfügbar unter der UCD-SNMP-MIB::memory-OID, die ähnliche Daten bereitstellt wie das Befehlzeilenkommando:

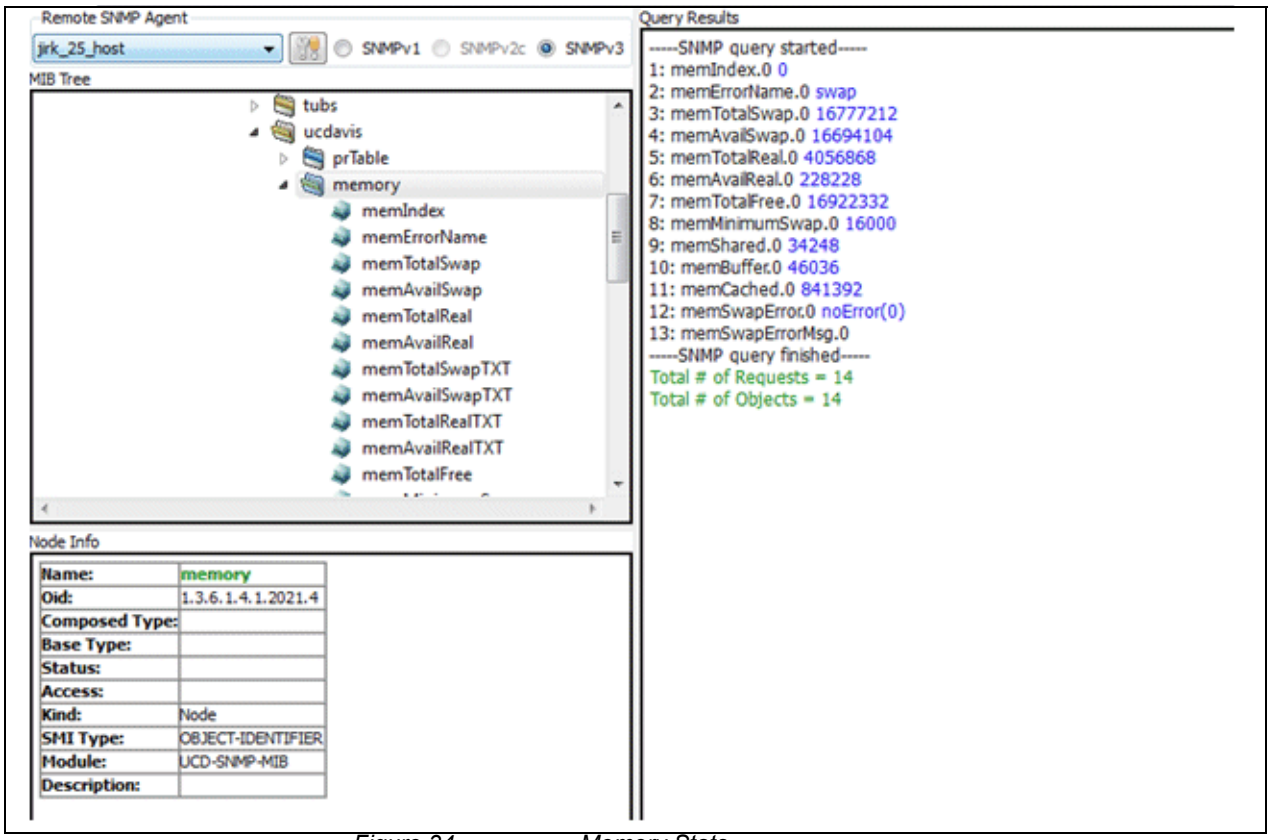


Figure 34 Memory Stats

Die durchschnittliche Auslastung ist ebenfalls in der UCD-SNMP-MIB erkennbar. Die SNMP-Tabelle UCD-SNMP-MIB::laTable enthält eine Liste mit den durchschnittlichen Auslastungswerten für 1, 5 und 15 Minuten:

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 35 Durchschnittliche Auslastung

3.11.2 Host-Ressourcen-MIB

Die in Net-SNMP enthaltene Host-Ressourcen-MIB zeigt Informationen über die aktuelle Hardware- und Software-Konfiguration eines Hosts an. Die folgenden OIDs stehen unter dieser MIB zur Verfügung:

- HOST-RESOURCES-MIB::hrSystem – enthält allgemeine Systeminformationen wie Betriebszeit, Anzahl der Benutzer und Anzahl der laufenden Prozesse

- HOST-RESOURCES-MIB::hrStorage – enthält Daten zur Verwendung des Arbeitsspeichers und des Dateisystems
- HOST-RESOURCES-MIB::hrDevices – enthält eine Liste mit allen Prozessoren, Netzwerkgeräten und Dateisystemen
- HOST-RESOURCES-MIB::hrSWRun – enthält eine Liste aller laufenden Prozessen
- HOST-RESOURCES-MIB::hrSWRunPerf – enthält Speicher- und CPU-Statistiken zur Prozesstabelle von HOST-RESOURCES-MIB::hrSWRun
- HOST-RESOURCES-MIB::hrSWInstalled – enthält eine Auflistung der RPM-Datenbank

3.11.2.1 Allgemeine Systeminformationen (hrSystem)

Die hrSystem-OID der HOST-RESOURCES-MIB stellt allgemeine Informationen über das System bereit:

Figure 36 hrSystem

3.11.2.2 Dateisystem und Datenträgerinformationen (hrStorage)

Die Host-Ressourcen-MIB enthält Informationen zur Größe und Verwendung der Dateisysteme. Jedes Dateisystem (und auch jeder Speicherpool) verfügt über einen Eintrag in der Tabelle HOST-RESOURCES-MIB::hrStorageTable:

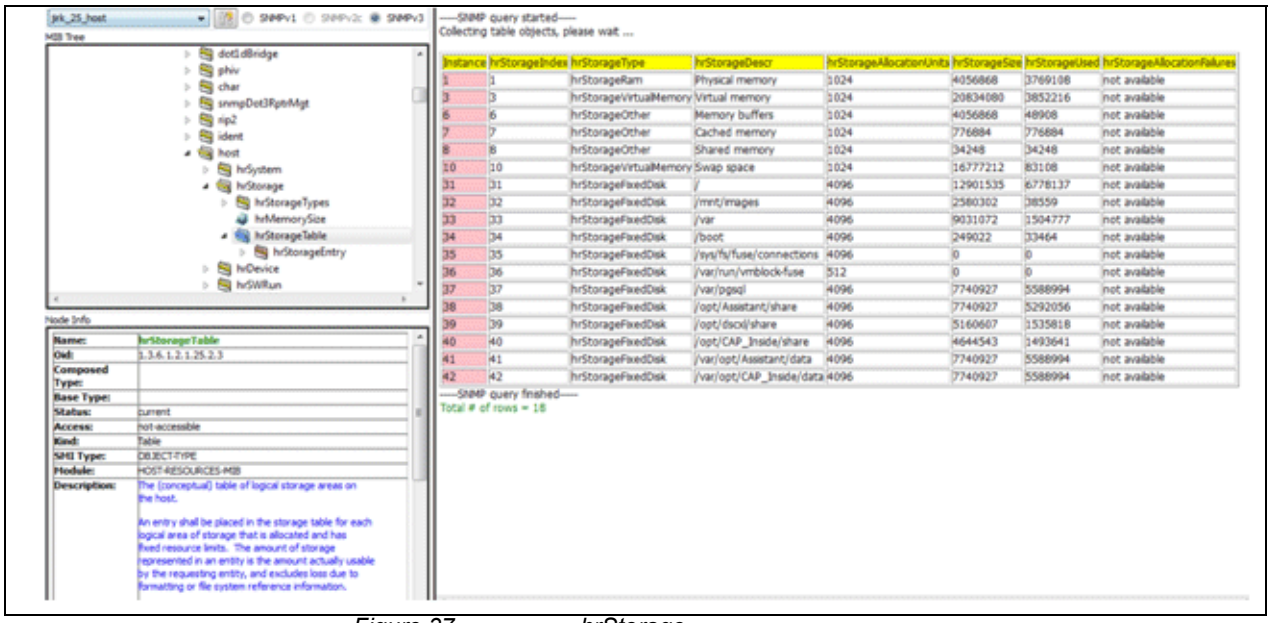


Figure 37 hrStorage

Die OIDs unter HOST-RESOURCES-MIB::hrStorageSize und HOST-RESOURCES-MIB::hrStorageUsed können verwendet werden, um die verbleibende Kapazität jedes gemounteten Dateisystems zu berechnen.

I/O-Daten sind sowohl in der UCD-SNMP-MIB::systemStats (ssIORawSent.0 und ssIORawRecieved.0) als auch in der UCD-DISKIO-MIB::diskIOTable verfügbar. Letztere stellt weitaus genauere Daten bereit. In dieser Tabelle finden Sie OIDs für diskIONReadX und diskIONWrittenX mit Zählern für die Anzahl der Bytes, die seit dem letzten Systemneustart vom Blockgerät gelesen und dorthin geschrieben wurden:

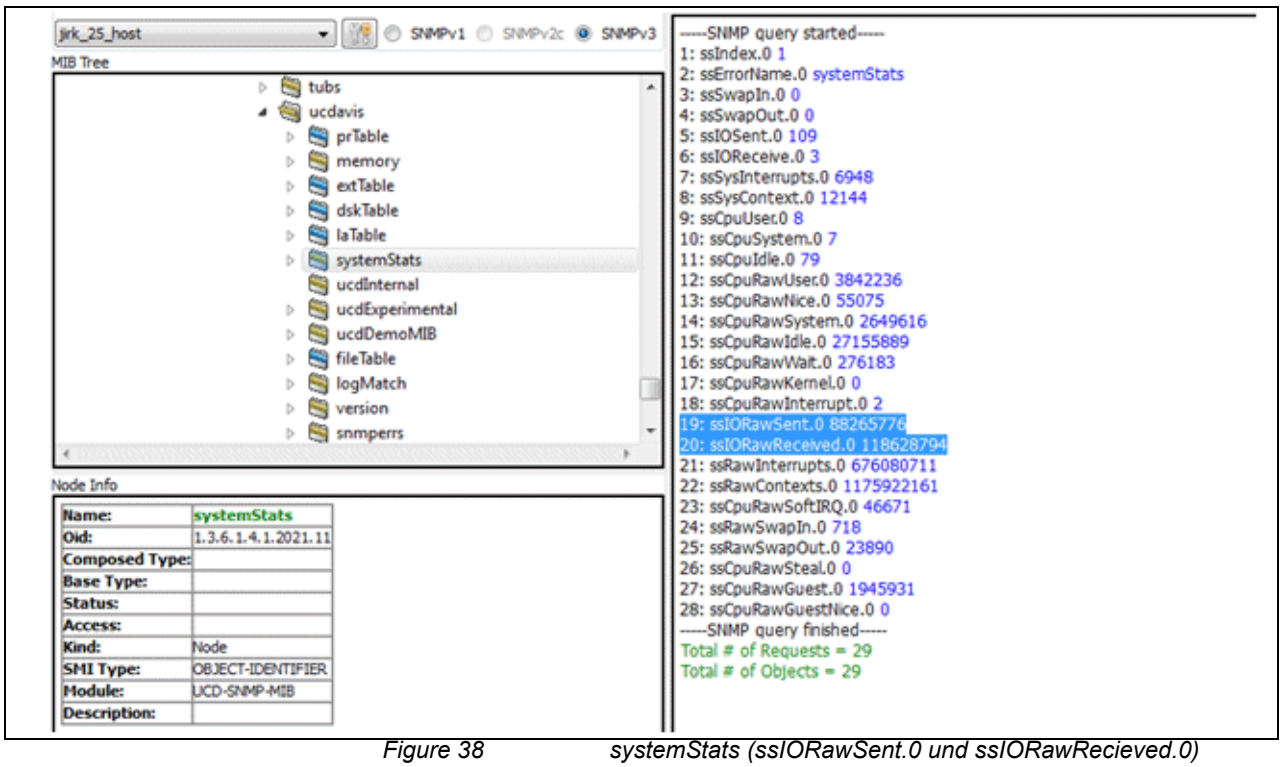


Figure 38 systemStats (ssIORawSent.0 und ssIORawRecieved.0)

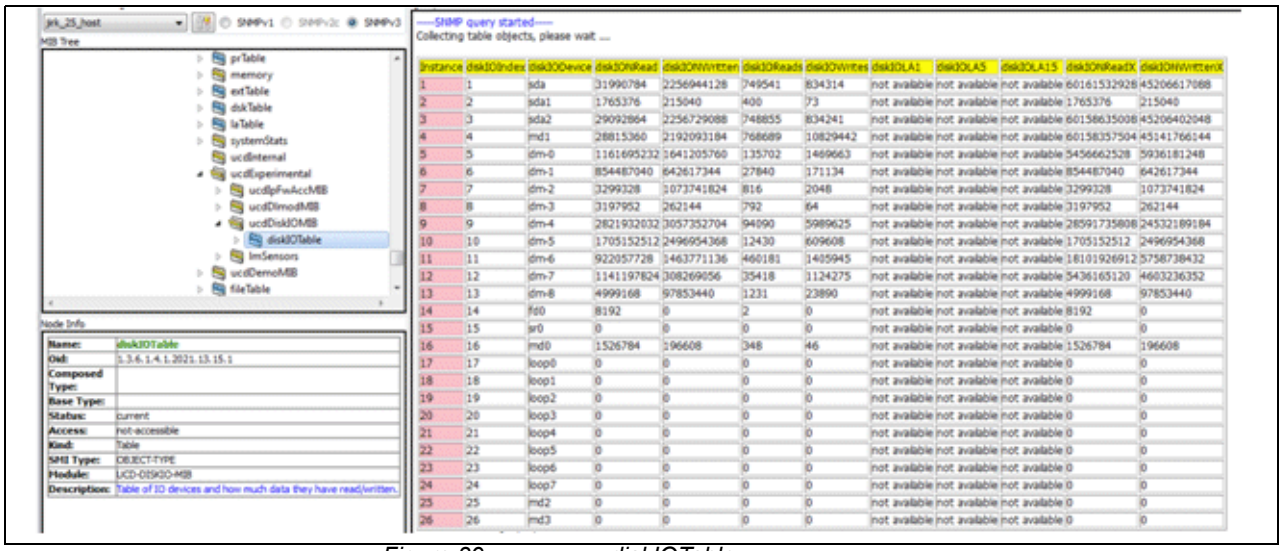


Figure 39 diskIOTable

3.11.2.3 Netzwerkinformationen

Die Schnittstellen-MIB enthält Informationen über die Netzwerkgeräte. IF-MIB::ifTable enthält eine SNMP-Tabelle mit einem Eintrag für jede Systemschnittstelle, die Schnittstellenkonfiguration sowie verschiedene

Paketzähler für die Schnittstelle. Das folgende Beispiel zeigt eine ifTable auf einem OpenScape 4000-System mit aktivem Simplex-Knoten, das auf einer VM läuft:

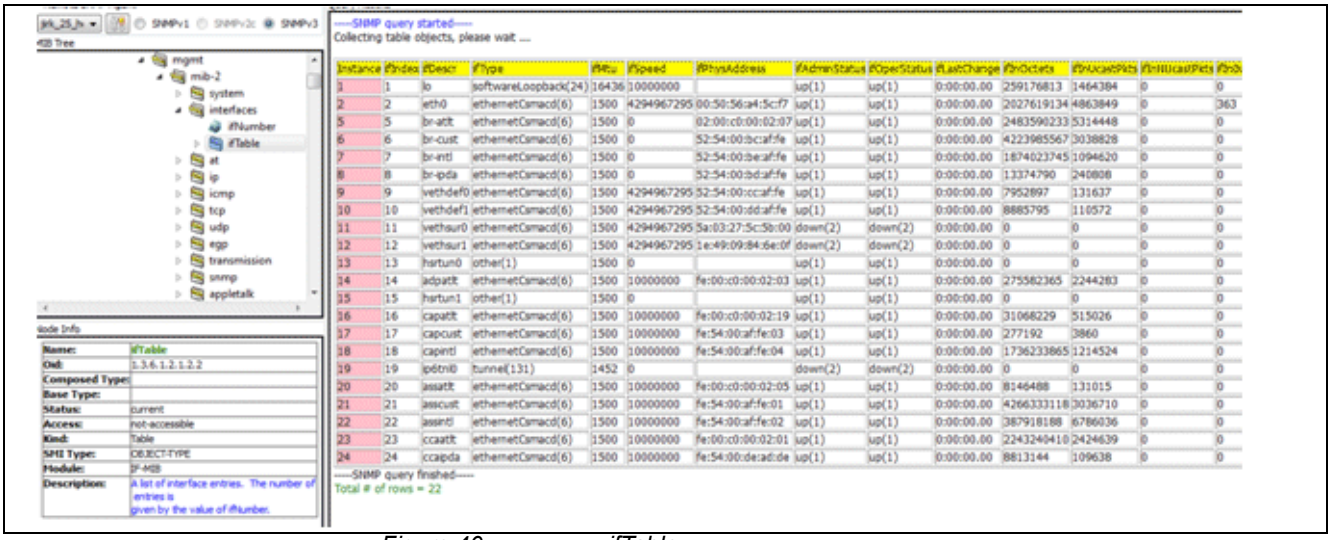


Figure 40 ifTable

Wie Sie sehen können, hat die Netzwerkgeschwindigkeit (ifSpeed) bereits den maximalen Wert erreicht, sodass keine Netzwerküberwachung der OpenScape 4000-Schnittstellen möglich ist.

Sie müssen die IF-MIB:ifXTable, eine Erweiterung der ifTable, verwenden.

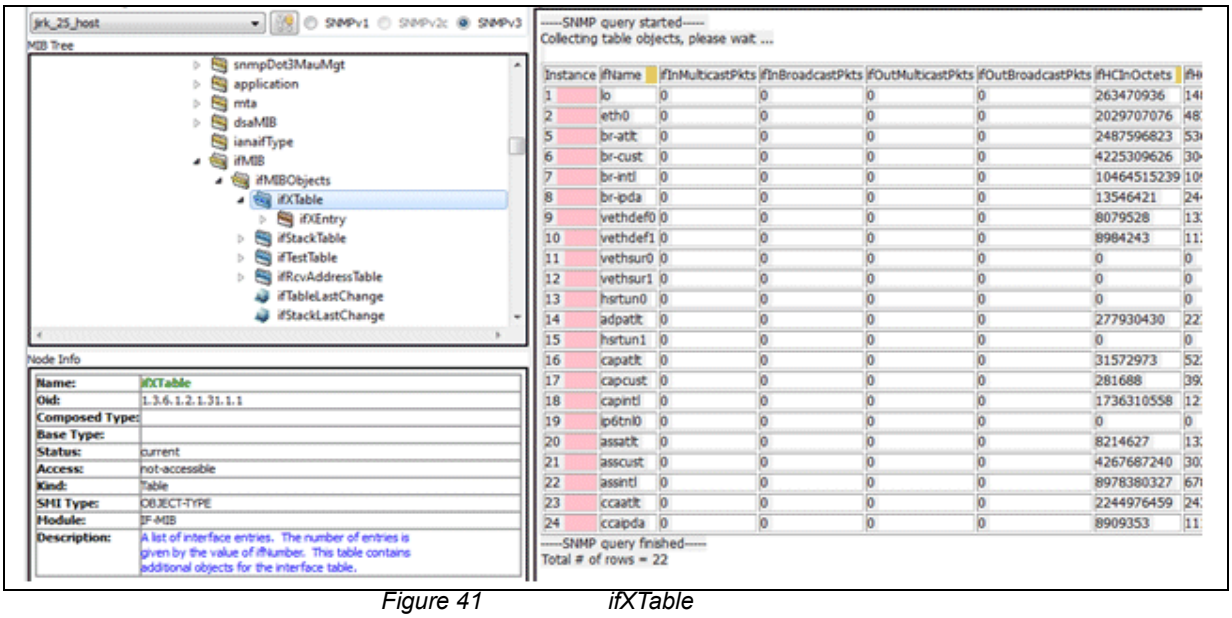
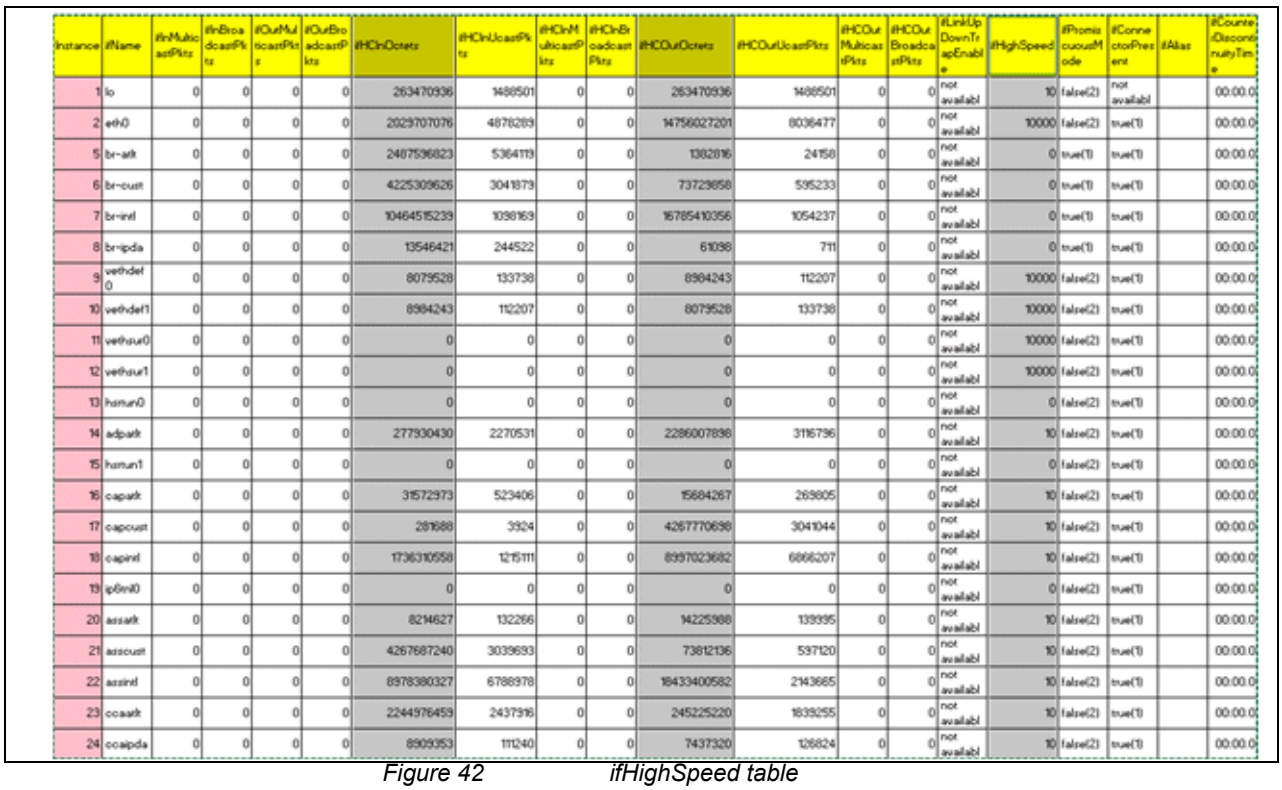


Figure 41 ifXTable

Suchen Sie hier nach dem Wert ifHighSpeed; dieser gibt die richtige Schnittstellengeschwindigkeit an:



Instance	#Name	#InMulticastPkts	#InBroadcastPkts	#OutMulticastPkts	#OutBroadcastPkts	#HCInOctets	#HCInUcastPkts	#HCInMulticastPkts	#HCInBroadcastPkts	#HCOutOctets	#HCOutUcastPkts	#HCOutMulticastPkts	#HCOutBroadcastPkts	#LinkUpDownTrapEnable	#HighSpeed	#PromiscuousMode	#ConnectorPresent	#Alias	#CounterDiscontinuityTime
1	lo	0	0	0	0	263470936	1486501	0	0	263470936	1486501	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-adt	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	3041879	0	0	73723658	595233	0	0	not availabl	0	true(1)	true(1)		00:00.0
7	br-intl	0	0	0	0	10464515239	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	8384243	112207	0	0	not availabl	10000	false(2)	true(1)		00:00.0
10	vethdef1	0	0	0	0	8384243	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	adpadt	0	0	0	0	277330430	2270531	0	0	2286007898	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	capadt	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	4267770638	3041044	0	0	not availabl	10	false(2)	true(1)		00:00.0
18	capintl	0	0	0	0	1736310558	1215111	0	0	8997023682	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	assadt	0	0	0	0	8214627	132266	0	0	14225988	139995	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	ccadt	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 42 ifHighSpeed table

Der Verkehrswert ist unter den OIDs IF-MIB::ifHCOutOctets und IF-MIB::ifHCInOctets ablesbar. An den dort angegebenen Werten für zwei aufeinander folgende Anrufe können Sie die Auslastung der Schnittstelle erkennen.

3.11.2.4 Softwareinformationen

- Informationen über installierte rpm-Softwarepakete, laufende Prozesse und zugehörige Leistungsstatistiken (CPU-/Speicherauslastung) werden in den folgenden drei OIDs bereitgestellt:
- HOST-RESOURCES-MIB::hrSWRun – enthält eine Liste aller laufenden Prozessen
- HOST-RESOURCES-MIB::hrSWRunPerf – enthält Speicher- und CPU-Statistiken zur Prozesstabelle von HOST-RESOURCES-MIB::hrSWRun
- HOST-RESOURCES-MIB::hrSWInstalled – enthält eine Auflistung der RPM-Datenbank

Laufende Softwareprozesse

HOST-RESOURCES-MIB::hrSWRun – enthält eine Liste aller auf einem OpenScape 4000-Hostsystem laufenden Prozesse:

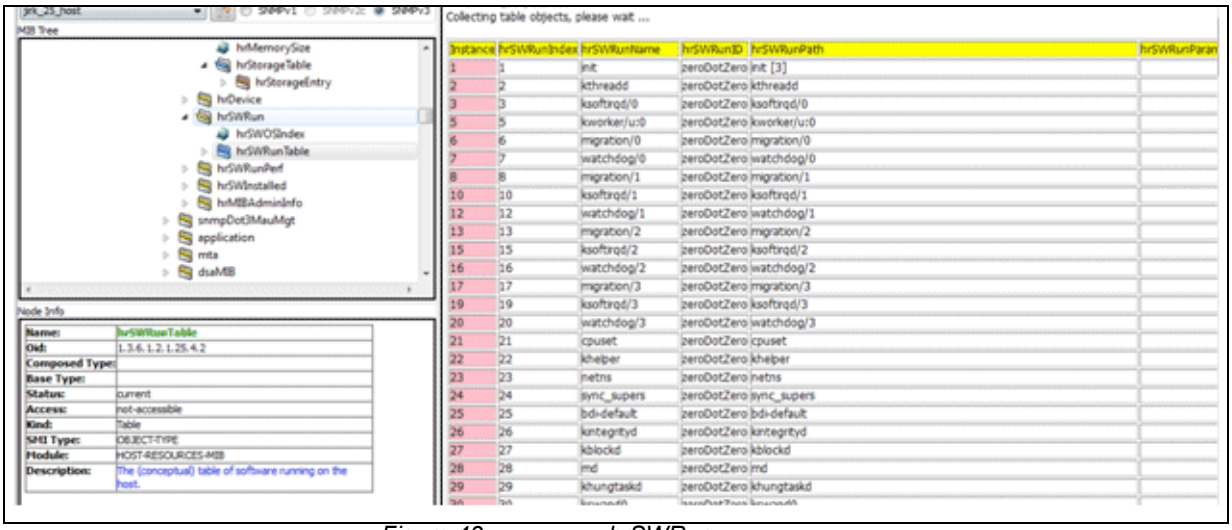


Figure 43 hrSWRun

Leistung der installierten Software

HOST-RESOURCES-MIB::hrSWRunPerf – enthält Speicher- und CPU-Statistiken zur Prozesstabelle von HOST-RESOURCES-MIB::hrSWRun:

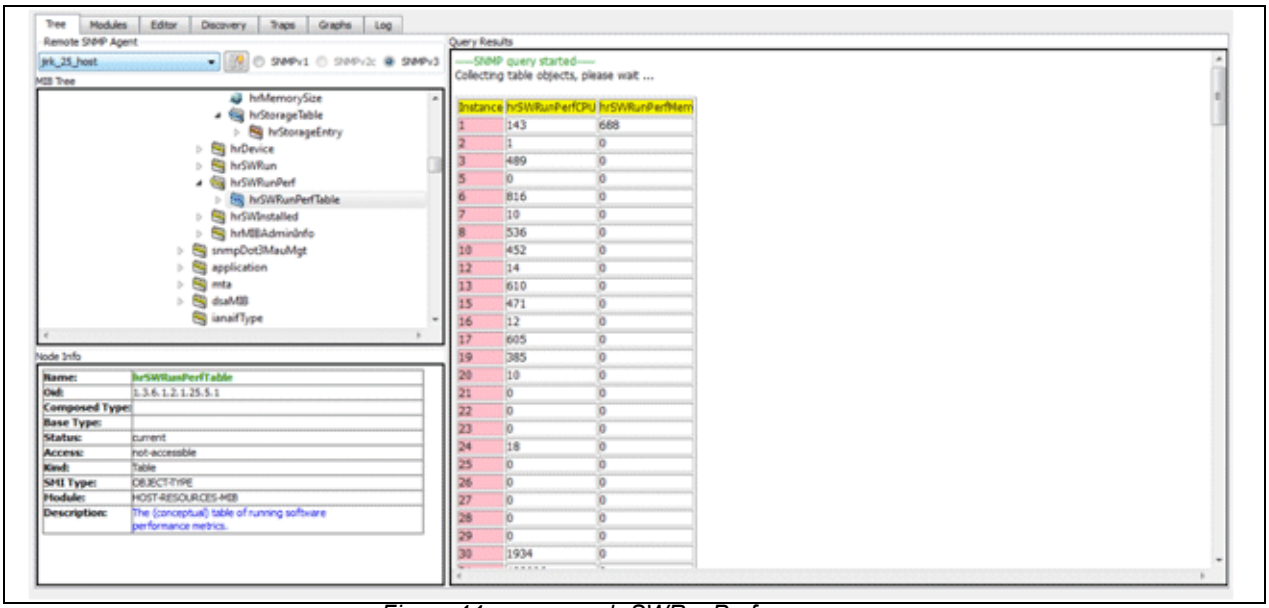


Figure 44 hrSWRunPerf

Installierte Softwarepakete

Die Tabelle hrSWInstalledTable des HOST-RESOURCES-MIB::hrSWInstalled-Teils der MIB dient zum Sammeln von Informationen über die auf dem OpenScape4000-Hostsystem installierten rpm-Pakete:

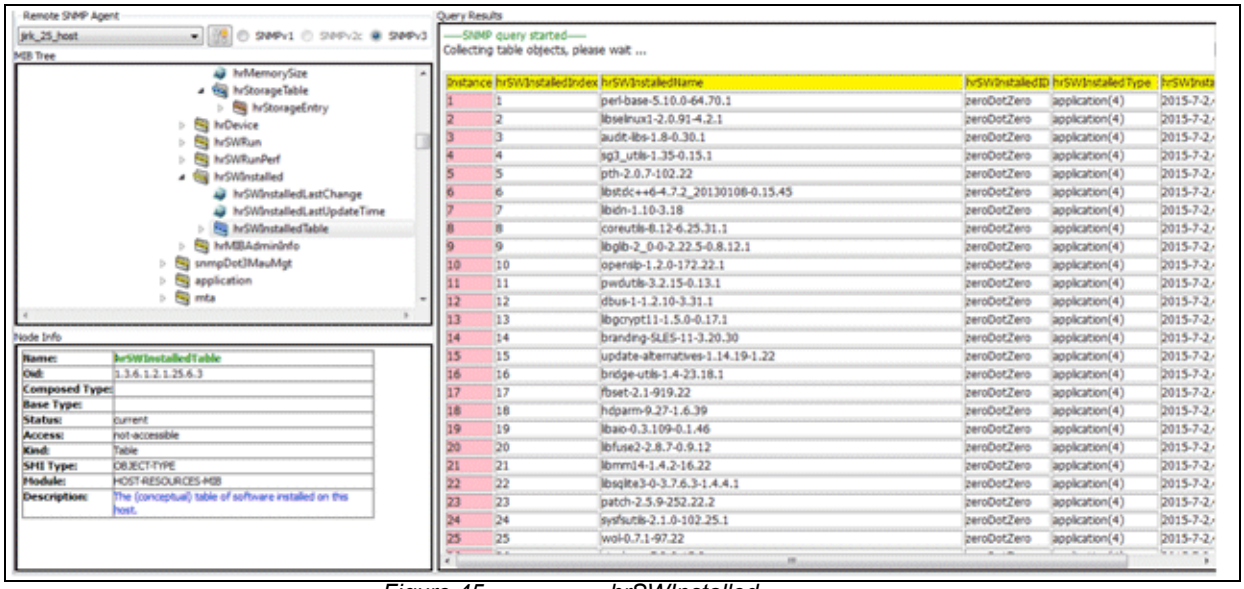


Figure 45 hrSWInstalled

4 Problembehebung

Informationen zur Behebung möglicher Fehler finden Sie unter:

Allgemeine Fehlermeldungen

Diese Fehlermeldung weist darauf hin, dass ein serverseitiges Skript fehlt. Kontaktieren Sie den Kunden-Support.

4.1 Allgemeine Fehlermeldungen

Es gibt drei Arten von allgemeinen Fehlermeldungen:

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

   Diese Fehlermeldung (Fehler 500 - Interner Serverfehler) wird in der Regel angezeigt, wenn ein oder mehrere serverseitige Skripts im System fehlen oder die Zugriffsrechte für diese Skripts falsch eingerichtet wurden. Darüber hinaus tritt er bei Fehlern in serverseitigen Skripts auf. Kontaktieren Sie den Kunden-Support.

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

   Diese Fehlermeldung (Interner Serverfehler. Daten möglicherweise beschädigt) wird bei Datenbankinkonsistenzen angezeigt, oder bei durch falsche Benutzereingaben verursachten Datenbankfehlern. Kontaktieren Sie den Kunden-Support.

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

   Diese Fehlermeldung weist darauf hin, dass ein serverseitiges Skript fehlt. Kontaktieren Sie den Kunden-Support.

5 OpenScape 4000-Alarme

Im Grunde genommen funktioniert die Alarmberichterstattung in OpenScape wie folgt:

- Bei der Netzwerkverwaltung (mit dem OpenScape 4000 Manager) werden vom OpenScape 4000 RMX (vom AFR2-Prozess auf RMX – je nach CPTP-, AFR-, SIGNL-, ... RMX-Konfiguration) empfangene Fehler (Fxxxx) bzw. Alarme (Axxxx) direkt an den SNMP-Dienst des OpenScape 4000 Manager übergeben, wo sie anschließend gefiltert oder als SNMP-hicomAlarm bzw. hicomError-Trap-Nachrichten übermittelt werden.
- Bei Nichtverwendung des OpenScape 4000-Manager wird der AFR3-Prozess auf dem RMX so konfiguriert, dass die Alarm-/Fehlermeldungen an den lokalen OpenScape 4000-Assistant gesendet werden, wo sie dann gefiltert oder als SNMP-hicomAlarm bzw. hicomError-Trap-Nachrichten übermittelt werden.

Jede Alarm-Trap-Nachricht (hicomAlarmOnMajor, hicomAlarmOnMinor, …) enthält die folgenden Parameter:

- **hicomSysPabxId**: Index des Systems in der chdmain-Tabelle (grundsätzlich nur bei der Netzwerkverwaltung nutzbar); dieser Parameter gibt den Knoten an, an dem der Alarm aufgetreten ist.
- **hicomSysMnemonic**: Mnemonik des in SysM konfigurieren Systems (Textdarstellung von hicomSysPabxId); dieser Parameter gibt den Knoten an, an dem der Alarm aufgetreten ist.
- **hicomAlGroup**: Alarmgruppe für folgende Alarmtypen
  - Central (Zentral) (1),
  - SWU Peripheral (SWU Peripherie) (2),
  - SWU Logical (SWU logisch) (3 und 4),
  - SM Peripheral (SM Peripherie) (5),
  - Manager/Assistant (7)
- **hicomAlSubId**: Alarmnummer innerhalb der Gruppe (siehe Tabelle unten)
- **hicomAlPriority**: Priorität des Alarms: 0 = Nebenalarm, 1 = Hauptalarm, 2 = Gerät (bei diesem Trap stets 1)
- **hicomAlAbsMod**: Alarm-generierendes Modul, z. B. BPA, NM
- **hicomAlStatus**: 0 = Alarm aus, 1 = Alarm ein
- **hicomAlTimDat**: Alarmzeitpunkt in Sekunden seit dem 01.01.1970
- **hicomAlName**: Alarmname, z. B. CC RESTARTS (CC-Neustart); LTU FAILURE (LTU-Ausfall); …

Informationen zu den Alarmen der Gruppen 1 bis 5 finden Sie in den AMOs VADSU und VADSM. Diese Alarme werden von RMX generiert und von dort an das SNMP-System des OpenScape 4000 Manager oder OpenScape 4000 Assistant übermittelt.

Neben den vom OpenScape RMX generierten Alarmmeldungen kann es auch vom Manager oder vom Assistant generierte Alarmmeldungen geben. Diese Alarme gehören zur Alarmgruppe **hicomAlGroup 7 (NM)**.

Nachstehend eine Liste dieser zur Alarmgruppe 7 gehörenden vordefinierten Alarme:

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
1	RETRY EXCEEDED (Max. Anz. Wiederholungen erreicht)	Haupt	Col konnte CDR-Datei nicht abrufen
2	NOT ENOUGH SPACE (Nicht genügend Speicherplatz)	Haupt	Speicherplatz für Performance Management reicht nicht aus
3	SWITCH ACCESS FAILING (Fehler bei Zugriff auf Switch)	Haupt	OpenScape-Abfrage fehlgeschlagen (Aktivierung projektspezifisch)
4	PM-DB FULL (PM-DB voll)	Haupt	Informix-Datenbank hat die Obergrenze erreicht
5	INFORMIX	Haupt	Allgemeine Datenbankprobleme
6	DISK FULL (Datenträger ist voll)	Haupt	Nicht genügend Speicherplatz
7	AFR FILE COUNT (Anzahl der AFR-Dateien)	Haupt	Anzahl der von RMX empfangenen Fehlermeldungen ist zu hoch -> Systemüberlastung durch zu viele Fehler
8	AFR DB SPACE	Haupt	Datenbank-Schwellwert erreicht: Hinzufügen weiterer Fehlermeldungen in die Datenbanktabelle “lerror” wurde angehalten
9	AFR STOPPED (AFR gestoppt)	Haupt	Es können keine Alarm- und Fehlermeldungen mehr empfangen werden, da AFR auf der RMX-Seite angehalten wurde
10	AFR FAULT (AFR-Fehler)	Haupt	Bei der Analyse der empfangenen AFR-Nachricht ist ein Fehler aufgetreten
11	AUTOLCK:	Haupt	Das Benutzerkonto wurde automatisch gesperrt
12	BACKUP FAILED (Backup fehlgeschlagen)	Haupt	Bei der RMX-Datensicherung ist ein Fehler aufgetreten
13	RESTORE FAILED (Wiederherstellung fehlgeschlagen)	Haupt	Bei der Wiederherstellung der RMX-Daten ist ein Fehler aufgetreten
14	DISK FULL (Datenträger ist voll)	Haupt	Beim Festplattenspeicher wurde der Schwellwert erreicht

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
15	THRESH. EXCEEDED (Schwellwert überschritten)	Haupt	Bei der PM-Datenbank wurde der Schwellwert erreicht
16	LMT_CDW_UPDATE (Aktualisierung LMT-Codewort)	Neben	Fehler bei der Aktualisierung des Codeworts am Switch durch das License Management Tool (LMT)
17	LMT_LICENSE_REDUCTION (LMT-Lizenz-reduzierung)	Haupt	Die Anzahl der Lizenzen im License Management Tool wurde reduziert
18	LMT_GLOBAL_ALARM_ THRESHOLD (Schwellwert für globalen LMT-Alarm)	Neben	Der Schwellwertalarm wurde in einer der Admin-Gruppen im License Management Tool (LMT) eingestellt
19	LMT_GLOBAL_ALARM (Globaler LMT-Alarm)	Haupt	Der Alarm wurde in einer der Admin-Gruppen im License Management Tool eingestellt; Codewörter für Systeme in dieser Admin-Gruppe wurden nicht aktualisiert
20	LMT_GLOBAL_WARNING_ THRESHOLD (Schwellwert für globale LMT-Warnung)	Neben	Die Schwellwertwarnung wurde in einer der Admin-Gruppen im Lizenz-Management-Tool eingestellt
21	LMT_GLOBAL_WARNING (Globale LMT-Warnung)	Neben	Die Warnung wurde in einer der Admin-Gruppen im License Management Tool eingestellt; Codewörter für Systeme in dieser Admin-Gruppe wurden nicht aktualisiert
22	PROCM_PM_CONTROL	Haupt	Der System-Daemon pm_control des Perfor-mance Management wurde unerwartet beendet
23	PROCM_PM_COL	Haupt	Der System-Daemon pm_col des Performance Management wurde unerwartet beendet
24	PROCM_PM_SCHED	Haupt	Der System-Daemon pm_sched des Performance Management wurde unerwartet beendet
25	PROCM_COL_SCHEDULE	Haupt	Der System-Daemon col_schedule des Collecting Agent wurde unerwartet beendet
26	PROCM_COL_TRANSFORM	Haupt	Der System-Daemon col_transform des Collecting Agent wurde unerwartet beendet
27	PROCM_COL_CYCLICCHECK	Haupt	Der System-Daemon col_cycliccheck des Collecting Agent wurde unerwartet beendet
28	PROCM_COL_LINE	Haupt	Der System-Daemon col_line des Collecting Agent wurde unerwartet beendet
29	PROCM_COL_DB_PROXY	Haupt	Der System-Daemon col_db_proxy des Collecting Agent wurde unerwartet beendet
30	PROCM_COL_RECEIVE	Haupt	Der System-Daemon col_receive des Collecting Agent wurde unerwartet beendet

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
31	PROCM_COL_METERING	Haupt	Der System-Daemon col_metering des Collecting Agent wurde unerwartet beendet
32	PROCM_FTW_TRANSFER_ CONTROL	Haupt	Der System-Daemon FTW_Transfer_Control des FlagTrace Watchdog wurde unerwartet beendet
33	PROCM_IDS_ONINIT	Haupt	Der Systemdatenbank-Daemon IDS_oninit der Informix-Datenbank wurde unerwartet beendet
34	PROCM_LMT_DAEMON	Haupt	Der System-Daemon lmtd des License Management Tools wurde unerwartet beendet
35	PROCM_SWTD_SERVER	Haupt	Der System-Daemon SWTDServer von Software Transfer wurde unerwartet beendet
36	PROCM_HTTP_USSW	Haupt	Der Apache-Server-Daemon wurde unerwartet beendet
37	PROCM_HTTP_TOMCAT	Haupt	Der Tomcat-Server-Daemon wurde unerwartet beendet
38	PROCM_LOGMEVTLOG	Haupt	Der System-Daemon LogMEvtLog des Logging Management wurde unerwartet beendet
39	PROCM_LOGMRECEIVER	Haupt	Der System-Daemon LogMReceiver des Logging Management wurde unerwartet beendet
40	PROCM_LOGMERRH	Haupt	Der System-Daemon LogMErrH des Logging Management wurde unerwartet beendet
41	PROCM_LOGMCONTROL	Haupt	Der System-Daemon LogMControl des Logging Management wurde unerwartet beendet
42	PROCM_LOGMDISPATCH	Haupt	Der System-Daemon LogMDispatch des Logging Management wurde unerwartet beendet
43	PROCM_LOGMSESS CONTROL	Haupt	Der System-Daemon LogMSessControl des Logging Management wurde unerwartet beendet
44	PROCM_SECM_SMW	Haupt	Der System-Daemon secm_smw des Security Management wurde unerwartet beendet
45	PROCM_SECM_CORE	Haupt	Der System-Daemon secm_core des Security Management wurde unerwartet beendet
46	PROCM_SYMUPLOAD CONTROL	Haupt	Der System-Daemon symUploadControl des System Management (Systemverwaltung) wurde unerwartet beendet
47	PROCM_SYMSERVICE	Haupt	Der System-Daemon symService des System Management (Systemverwaltung) wurde unerwartet beendet
48	PROCM_CMPROC_DOM_ UXBPROC	Haupt	Der System-Daemon cmproc_dom_uxbproc des Configuration Management (Konfigurationsma-nagement) wurde unerwartet beendet

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
49	PROCM_CMPROC_DOM_ UXLMAIN	Haupt	Der System-Daemon cmproc_dom_uxlmain des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
50	PROCM_CMPROC_CCS	Haupt	Der System-Daemon cmproc_ccs des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
51	PROCM_CMPROC_SUB_ UXSDBSYN	Haupt	Der System-Daemon cmproc_sub_unxsdbsyn des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
52	PROCM_CMPROC_DOM_ CSERVER	Haupt	Der System-Daemon cmproc_dom_cserver des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
53	PROCM_CMPROC_DOM_ CMIPSA	Haupt	Der System-Daemon cmproc_dom_cmipsa des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
54	PROCM_CMPROC_DOM_ CONVBJOB	Haupt	Der System-Daemon cmproc_dom_convbjob des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
55	PROCM_CMPROC_DOM_ CDBSERVER	Haupt	Der System-Daemon cmproc_dom_cdbserver des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
56	PROCM_CMPROC_SUB_ ICPROCESSING	Haupt	Der System-Daemon cmproc_sub_icprocessing des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
57	PROCM_CMPROC_SUB_ CSERVER	Haupt	Der System-Daemon cmproc_sub_cserver des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
58	PROCM_CMPROC_DOM_ UMPROC	Haupt	Der System-Daemon cmproc_dom_umproc des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
59	PROCM_CMPROC_DOM_ UXSDBSYN	Haupt	Der System-Daemon cmproc_dom_uxsdbsyn des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
60	PROCM_CMPROC_DOM_ UXSFILED	Haupt	Der System-Daemon cmproc_dom_uxsfiled des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
61	PROCM_CMPROC_DOM_ DLSPROXY	Haupt	Der System-Daemon cmproc_dom_dlsproxy des Configuration Management (Konfigurationsmanagement) wurde unerwartet beendet
62	PROCM_FM_AER_DAEMON	Haupt	Der System-Daemon AER_Daemon des Fault Management wurde unerwartet beendet

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
63	PROCM_FM_DB_SERVER	Haupt	Der System-Daemon FM_DB_Server des Fault Management wurde unerwartet beendet
64	PROCM_NAMING_SERVICE	Haupt	Der System-Daemon NamingService des CORBA-Kommunikations-Frameworks wurde unerwartet beendet
65	PROCM_FM_FTSERV	Haupt	Der System-Daemon ftserv des Batch Generator wurde unerwartet beendet
66	PROCM_FM_FTSUCC	Haupt	Der System-Daemon ftsucc des Batch Generator wurde unerwartet beendet
67	PROCM_MPCID	Haupt	Der für die Kommunikation mit RMX verwendete System-Daemon mpcid des Multi-Purpose Client Interface wurde unerwartet beendet
68	PROCM_MPCIDLOG	Haupt	Der für die Kommunikation mit RMX verwendete System-Daemon mpcidlog des Multi-Purpose Client Interface wurde unerwartet beendet
69	PROCM_HISPAD	Haupt	Der System-Daemon hispad von HiSPA 4000 wurde unerwartet beendet
70	PROCM_REPORTGENERATOR	Haupt	Der System-Daemon ReportGenerator des Report Generator wurde unerwartet beendet
71	PROCM_REPGENREADY	Haupt	Der System-Daemon RepgenReady des Report Generator wurde unerwartet beendet
72	PROCM_DMSIED	Haupt	Der System-Daemon dmsied der Export/Import-Schnittstelle (XIE) wurde unerwartet beendet
73	PROCM_XIESERVER	Haupt	Der System-Daemon xieserver der Export/Import-Schnittstelle (XIE) wurde unerwartet beendet
74	PROCM_COMWINACCESS	Haupt	Der System-Daemon comwinaccess von Expert Access wurde unerwartet beendet
75	LOGM_ACTIVITY_TABLE_ THRESHOLD (Schwellwert der LOGM-Aktivitätstabelle)	Neben	Bei der Aktivitätstabelle des Logging Management wurde der Schwellwert erreicht
76	LOGM_ERROR_TABLE_ THRESHOLD (Schwellwert der LOGM-Fehlertabelle)	Neben	Bei der Fehlertabelle des Logging Management wurde der Schwellwert erreicht
77	LICM_LICENSE_EXCEEDED	Haupt	Die OpenScape 4000 Management-Lizenz ist abgelaufen
78	HBR_DATA_BACKUP	Haupt	Die Datensicherung ist fehlgeschlagen
79	HBR_LOGICAL_ABD	Haupt	Die logische Sicherung der ABD-Einheit ist fehlgeschlagen
80	HBR_LOGICAL_BUM	Haupt	Die logische Sicherung der BUM-Einheit ist fehlgeschlagen

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
81	HBR_LOGICAL_CDB	Haupt	Die logische Sicherung der CDB-Einheit ist fehlgeschlagen
82	HBR_LOGICAL_CHD	Haupt	Die logische Sicherung der CHD-Einheit ist fehlgeschlagen
83	HBR_LOGICAL_COMWIN	Haupt	Die logische Sicherung der COMWIN-Einheit ist fehlgeschlagen
84	HBR_LOGICAL_HBR	Haupt	Die logische Sicherung der HBR-Einheit ist fehlgeschlagen
85	HBR_LOGICAL_HBR_MPCID	Haupt	Die logische Sicherung der MPCID-Einheit ist fehlgeschlagen
86	HBR_LOGICAL_HBR_TSYNC	Haupt	Die logische Sicherung der TSYNC-Einheit ist fehlgeschlagen
87	HBR_LOGICAL_LAP2	Haupt	Die logische Sicherung der LAP2-Einheit ist fehlgeschlagen
88	HBR_LOGICAL_LOGM	Haupt	Die logische Sicherung der LOGM-Einheit ist fehlgeschlagen
89	HBR_LOGICAL_SSO	Haupt	Die logische Sicherung der SSO-Einheit ist fehlgeschlagen
90	HBR_LOGICAL_SECM	Haupt	Die logische Sicherung der SECM-Einheit ist fehlgeschlagen
91	HBR_LOGICAL_UBA	Haupt	Die logische Sicherung der UBA-Einheit ist fehlgeschlagen
92	HBR_LOGICAL_WEBMIN	Haupt	Die logische Sicherung der WEBMIN-Einheit ist fehlgeschlagen
93	FM_COMANDFILE_SEND	Neben	Der Batch Generator kann den AMO-Job nicht an die Anlage übergeben
94	PM_DATABASE_THRESHOLD	Neben	Bei der PM-Datenbank wurde der Schwellwert erreicht
95	PM_REPORT	Haupt	Die zeitgesteuerte Berichterstellung durch Performance Management war nicht erfolgreich.
96	COL_FETCH	Haupt	Abruf von der Anlage (fetch-Anforderung) im Collecting Agent schlug fehl
97	COL_RECEIVE	Haupt	Konvertierung (transform-Anforderung) der empfangenen Datei im Collecting Agent schlug fehl
98	COL_OUTPUT_FILE_PROD	Neben	Erstellung der Ausgabedatei im Collecting Agent schlug fehl

hicomAl-SubID	hicomAlName	hicom AlarmOn (Major (Haupt-alarm) / Minor (Neben-alarm))	Kurzbeschreibung
99	COL_PARTITION_FILLED	Haupt	Abruf (fetch-Anforderung) im Collecting Agent wurde deaktiviert, da das COL-Backup-Verzeichnis voll ist
100	CM_DB_SYNCH	Neben	Die Synchronisierung der Datenbank mit der Anlage im Configuration Management war nicht erfolgreich
101	SWA_ACTIVATION_FAILED	Haupt	Die Software-Aktivierung des Major/Minor/FixRelease oder des Hotfix schlug fehl
102	DISK_SATURATION_ THRESHOLD	Neben	Auf einer der überwachten Systempartitionen wurde der Schwellwert erreicht
103	SSO_REPLICATION	Haupt	Die Replikation während des Smart Switchover (SSO) war nicht erfolgreich
104	LICM_H300_PORTCOUNT_ WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von H300-Ports in der Lizenzverwaltung wurde erreicht.
105	LICM_HP4K_V1_PORT-COUNT_WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von OpenScape4000 V1-Ports in der Lizenzverwaltung wurde erreicht.
106	LICM_HP4K_V2_PORT-COUNT_WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von OpenScape4000 V2-Ports in der Lizenzverwaltung wurde erreicht.
107	LICM_HP4K_V3_PORT-COUNT_WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von OpenScape4000 V3-Ports in der Lizenzverwaltung wurde erreicht.
108	LICM_HP4K_V4_PORT-COUNT_WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von OpenScape4000 V4-Ports in der Lizenzverwaltung wurde erreicht.
109	LICM_HP4K_V5_PORT-COUNT_WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von OpenScape4000 V5-Ports in der Lizenzverwaltung wurde erreicht.
110	LICM_PORTCOUNT_ EXCEEDED	Haupt	Der Schwellwert für die max. Anzahl von Ports für OpenScape4000-Lizenzen in der Lizenzverwaltung wurde überschritten.
111	LICM_HP4K_V6_PORT-COUNT_WARN_REACHED	Neben	Der Schwellwert für die max. Anzahl von OpenScape4000 V6-Ports in der Lizenzverwaltung wurde erreicht.
112	LICM_SLES_UPDATE_ PROTECTION	Haupt	Das System verfügt nicht über genügend Lizenzen für den SLES-Upgrade-Schutz. Es kann sein, dass RLC/Minor/Major-Updates blockiert werden.

Weitere Informationen zu Fault Management, Alarmen und SNMP finden Sie in Kapitel 6 “OpenScape 4000 SNMP Management” des Installations- und Servicehandbuchs.

Index

T

U

Z