A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Manager

Installation and Service Manual

Service Documentation
10/2025

A31003-H34B0-S101-02-0020

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 Wichtige Hinweise

1.1 Zu diesem Handbuch

Dieses Handbuch enthält allgemeine Informationen sowie Installations, Test und Serviceanleitungen für den OpenScape 4000 Manager.

Zum Adressatenkreis für dieses Handbuch zählen alle Installationsexperten, Kundendiensttechniker, Mitarbeiter der Support-Ebene 2, Systemingenieure und Kundenadministratoren, die an der Installation, Wartung, Betreuung und Verwaltung des OpenScape 4000 Managers beteiligt sind.

1.1.1 Voraussetzungen / Vorkenntnisse

Die Person, die den OpenScape 4000 Manager installiert und wartet, muss über Grundkenntnisse in folgenden Bereichen verfügen:

- Telephonie und Trunking
- OpenScape 4000 Systemkenntnisse
- LAN-Kommunikation
- Client/Server-Architektur
- Reparaturmaßnahmen für Workstation- und Server-Hardware

1.1.2 Gliederung

Das vorliegende Handbuch enthält folgende Kapitel:

Kapitel 2, "Einführung" bietet einen Überblick über die Hard- und Software-Komponenten des OpenScape 4000 Managers.

Kapitel 3, "Vorbereitung und Installation des OpenScape 4000 Manager-Servers"beschreibt die Prozeduren, die vor und während der Installation der OpenScape 4000 Manager durchzuführen sind.

Kapitel 4, "Einrichten von Systemen und Benutzern mit OpenScape 4000 Manager"enthält Anleitungen zur Installation der verschiedenen Software-Typen für den OpenScape 4000 Manager-Server.

Kapitel 5, "Bedienung und Wartung des OpenScape 4000 Manager-Servers"beschreibt verschiedene Bedien- und Wartungsprozeduren für den OpenScape 4000 Manager.

Kapitel 6, "OpenScape 4000 SNMP Management"beschreibt die Installation, Konfiguration und Inbetriebnahme des OpenScape 4000 SNMP Proxy Agenten und die speziellen Scripte zur Filterung von Alarmmeldungen.

Darüber hinaus umfasst dieses Handbuch eine Abkürzungsliste und ein Stichwörterverzeichnis.

1.1.3 Schreibweisen und verwendete Symbole

In dem vorliegenden Handbuch gelten folgende Symbole und Konventionen:

Anmerkung: Dieses Symbol weist auf allgemeine Hinweise und erläuternde Informationen hin.

Dieses Symbol weist auf kundenspezifische Hinweise und sehr wichtige Informationen hin.

Sicherheitshinweise: GEFAHR, WARNUNG, VORSICHTDetaillierte Angaben siehe Abschnitt 1.2, "Datenschutz und Datensicherheit".

1.1.4 Verwandte Informationen

Ergänzende Informationen finden Sie in folgenden Handbüchern und Publikationen:

- OpenScape 4000 Manager V10, Batch Generator - Direct Access, Administratordokumentation, P31003-H34A0-M130-xx-76A9
- OpenScape 4000 Manager V10, Configuration Management, Administratordokumentation, P31003-H34A0-M111-xx-76A9
- OpenScape 4000 Manager V10, Leistungsmerkmalbeschreibung, P31003-H34A0-F100-xx-7618
- OpenScape 4000 Manager V10, Import/Export Interface (XIE) API, Servicedokumentation, P31003-H34A0-S100-xx-7620
- OpenScape 4000 Manager V10, License Management Tool - Access Management, Administratordokumentation, P31003-H34A0-M132-xx-76A9
- OpenScape 4000 Manager V10, Performance Planning Tool, Planungsanleitung, P31003-H34A0-P101-xx-76A9
- OpenScape 4000 Manager V10, PM Calculation Rules and Examples, Administratordokumentation, P31003-H34A0-M136-xx-76A9
- OpenScape 4000 Manager V10, Software Activation, Administratordokumentation, P31003-H34A0-M133-xx-76A9
- OpenScape 4000 Manager V10, Webmin Base Administration, Administratordokumentation, P31003-H34A0-M132-xx-76A9
- OpenScape 4000 Manager V10, Datenblatt, P31002-H34A0-D100-xx-7629
- OpenScape 4000 V10, Volume 3, Feature Usage Examples P31003-H31A0-S104-xx-7620

1.1.5 Feedback zur Dokumentation

Bevor Sie anrufen, ist sicherstellen, dass die nachfolgend aufgeführten Information verfügbar sind. Auf diese Weise lässt sich schneller prüfen, mit welchem Dokument Sie Probleme hatten.

- **Titel:** OpenScape 4000 Manager V10, Installation and Service Manual, Servicedokumentation
- **Bestellnummer:** A31003-H34A0-S101-02-7620

1.1.5.1 Nur USA

Sollten Sie ein Problem im Zusammenhang mit diesem Dokument zu berichten haben, wenden Sie sich an den für Sie zuständigen Support:

- Kunden wenden sich bitte an das Customer Support Center (CSC).
- Unify-Mitarbeiter sollten sich an das i-CET (Interactive Customer Engagement Team) wenden oder ein Formular für Feedback zur Dokumentation auf der Seite LiveLink Product Documentation ausfüllen.

1.1.5.2 Andere Länder als die USA

Bitte geben Sie wie folgt Feedback zu dieser Dokumentation:

- Reichen Sie bei ICTS ein Problem-Ticket ein, oder
- Verwenden Sie das Formular für Feedback zur Dokumentation, auf das Sie über die Titelseite der HTML-Version dieser Dokumentation zugreifen können.

1.2 Datenschutz und Datensicherheit

Beim vorliegenden System werden u. a. personenbezogene Daten verarbeitet und genutzt, z. B. bei der Gebührenerfassung, den Displayanzeigen, der Kundendatenerfassung.

In Deutschland gelten für die Verarbeitung und Nutzung solcher personenbezogenen Daten u. a. die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Für andere Länder beachten Sie bitte die jeweiligen entsprechenden Landesgesetze.

Datenschutz hat die Aufgabe, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Ferner hat Datenschutz die Aufgabe, durch den Schutz der Daten vor Missbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.

Der Kunde ist dafür verantwortlich, dass das System in Übereinstimmung mit dem jeweils gültigen Datenschutz-, Arbeits- und Arbeitsschutzrecht installiert, betrieben und gewartet wird.

Die Mitarbeiter unseres Unternehmens sind durch die Arbeitsordnung zur Wahrung von Geschäfts- und Datengeheimnissen verpflichtet.

Um die gesetzlichen Bestimmungen beim Service – ob beim âService vor Ort>oder beim âTeleservice>– konsequent einzuhalten, sollten Sie folgende Regeln unbedingt befolgen. Sie wahren damit nicht nur die Interessen Ihrer/ unserer Kunden, sondern vermeiden dadurch auch persönliche Konsequenzen.

Tragen Sie durch problembewusstes Handeln mit zur Gewährleistung des Datenschutzes und der Datensicherheit bei:

- Achten Sie darauf, dass nur berechtigte Personen Zugriff auf Kundendaten haben.
- Nutzen Sie alle Möglichkeiten der Passwortvergabe konsequent aus; geben Sie keinem Unberechtigten Kenntnis der Passwörter, z. B. per Notizzettel.
- Achten Sie mit darauf, dass kein Unberechtigter in irgendeiner Weise Kundendaten verarbeiten (speichern, verändern, übermitteln, sperren, löschen) oder nutzen kann.

- Verhindern Sie, dass Unbefugte Zugriff auf Datenträger haben, z. B. auf Sicherungs-CDs oder Protokolldrucke. Das gilt sowohl für den Serviceeinsatz, als auch für Lagerung und Transport.
- Sorgen Sie dafür, dass nicht mehr benötigte Datenträger vollständig vernichtet werden. Vergewissern Sie sich, dass keine Papiere allgemein zugänglich zurückbleiben.

Arbeiten Sie mit Ihren Ansprechpartnern beim Kunden zusammen: Das schafft Vertrauen und entlastet Sie selbst.

2 Einführung

Dieses Kapitel bietet einen Überblick über den OpenScape 4000 Manager und die zugehörigen Komponenten.

2.1 Allgemeine Beschreibung

Im Rahmen des OpenScape Managements und der neuen OpenScape/HiPath-Konvergenzarchitektur fungiert der OpenScape 4000 Manager als Netzelement-Manager für die Administration und Serviceability der Kommunikationsplattform OpenScape 4000 IP. Der Einsatz des OpenScape 4000 Managers erfolgt wahlweise im Standalone-Modus (unter der Bezeichnung OpenScape 4000 Assistant) oder im Netzwerkbetrieb mit anderen OpenScape/HiPath 4000 IP Kommunikationsplattformen und den zugehörigen Produkten.

Mit HiPath User Management V3 können zwei verschiedene Manager miteinander verbunden werden

OpenScape 4000 Manager und OpenScape 4000 Assistant unterscheiden sich wie folgt:

- OpenScape 4000 Manager -- Netzwerkversion für kleine, mittlere und größere Netzwerke; die Installation erfolgt auf einem externen Server
- OpenScape 4000 Assistant -- lokale Version, liegt auf dem ADP der Kommunikationsplattform OpenScape 4000 IP vor

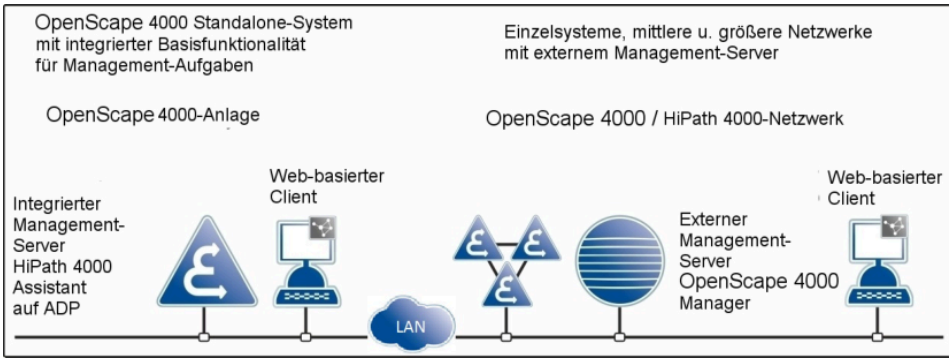


Abbildung 1: OpenScape 4000 Manager vs. OpenScape 4000 Assistant

2.1.1 OpenScape 4000 Manager (Externer Server)

Der OpenScape 4000 Manager bietet eine erweiterte Management-Funktionalität für Standalone-Kommunikationsplattformen des Typs OpenScape 4000 IP sowie Netzwerke auf Basis dieses Plattformtyps. Die Leistungsmerkmale für den OpenScape 4000 Manager stellen zusätzliche Funktionen bereit und vereinfachen bestimmte Aufgaben (oder beides).

Der OpenScape 4000 Manager erfordert einen dedizierten PC, der entweder hardwarebasiert oder virtualisiert (VMware) sein kann. Welches Server-Modell im Einzelfall erforderlich ist, hängt von der Größe des zu verwaltenden Netzwerks ab.

Das OpenScape 4000 Manager-Paket umfasst folgende Applikationen:

- CM-Network

  Dieses Leistungsmerkmal bietet leistungsstarke Funktionen für das Konfigurationsmanagement in kleinen, mittleren und größeren Netzwerken, einschließlich Knoten-zu-Knoten-Umzug und Netzwählplan-Verwaltung. Eine leitungsbezogene Administration ist durch Aufruf der CM-Basic-Applikation in der OpenScape 4000-Anlage möglich (Assistant). Etwa 85 % aller AMOs sind somit über die Web-Schnittstelle zugänglich; auf die übrigen AMOs kann über die integrierte ComWin-Applikation zugegriffen werden.
- PM-Network

  Das Performance Management-Paket für die Netzwerk-Ebene misst und bewertet den Amts- bzw. Leitungsverkehr innerhalb des gesamten Netzwerks. PM-Net ersetzt das Produkt PM-Charts von HDMS.
- PM-Enhanced

  Auf Basis der PM-Network-Ergebnisse misst und bewertet PM-E das Kommunikationsverhalten aller Benutzer und Benutzergruppen. Ferner ermittelt PM-E die Belastung bestimmter Komponenten der OpenScape 4000-Anlagen (mit eingeschränktem Leistungsumfang) netzweit für alle Messobjekte.
- PM-ASC (Attendant Supervisor Console)

  Dieses Leistungsmerkmal wird ausschließlich für die Generierung von ASC-Statistiken an einem Vermittlungsplatz (Attendant Console, AC) genutzt.
- COL-Network

  Bei Installation in einem OpenScape/HiPath 4000-Netzwerk fungiert diese Applikation als zentrale Gebührenerfassungsfunktion (GEB) für das gesamte Netzwerk. Die erfassten Daten stehen für das Accounting Management und das Performance Management zur Verfügung.
- Import/Export API (XIE)

  XIE ist die Schnittstelle für den Datenimport und -export. Diese API ermöglicht es externen Applikationen, auf die Daten des OpenScape 4000 Managers zuzugreifen, und unterstützt ferner den Import und Export von Fremddaten in den OpenScape 4000 Manager.
- SNMP

  Der SNMP-Agent ist eine Gateway-Funktion, die für die Anbindung an Umbrella-Management-Systeme von Drittanbietern benötigt wird.

2.2 OpenScape 4000 Manager Hardware

Der OpenScape4000 Manager wird ähnlich wie das OS4K-System als Hardware/Software-Appliance angeboten. Der OpenScape EcoServer (S30122-K7760-X) kann als Plattform oder alternativ als VM in einer VMware-Umgebung verwendet werden.

Die erforderlichen Ressourcen für VM finden Sie in der Tabelle in Kapitel 5.5.2 "OpenScape 4000 Manager V10R1" von OpenScape-Lösungssatz V10, OpenScape Virtuelle Maschine Ressourcen- und Konfigurationshandbuch, Service-Dokumentation. Die meisten Einstellungen werden festgelegt, wenn die im Installationsmedium enthaltene OVF-Vorlage bereitgestellt wird.

Die OpenScape EcoServer-Hardware kann in Kunden-Setups, die die Grenze von 100 OpenScape 4000-Systemen und 30000 Ports überschreiten, an Grenzen stoßen.

Anmerkung: Die Speicherkapazität der Festplatte muss 1 TB betragen.

2.3 OpenScape 4000 Manager Software

Der OpenScape 4000 Manager wird als SW-Appliance bereitgestellt. Diese Appliance enthält das vorgehärtete SLES (Suse Linux Enterprise System) basierte Betriebssystem und alle erforderlichen Manager-SW-Anwendungen. Das ISO-Installationsimage kann entweder auf einen USB-Stick zur Installation auf der OpenScape EcoServer HW-Plattform kopiert oder über die VMware Management-Anwendung gemountet werden.

Die Appliance-Installation erfordert zwei IP-Adressen, eine für die LINUX-Plattform und eine andere für die im Container betriebene Manager-Anwendung.

Der SW-Lebenszyklus wird über Unify SWS, Manager HotFix, Plattform HotFix und RLC (Release Level Complete) für die Fix-Version/Nebenversion/Hauptversion-SW-Updates abgeschlossen. Die SWM-Anwendung ist der zentrale Punkt für die SW-Versorgung.

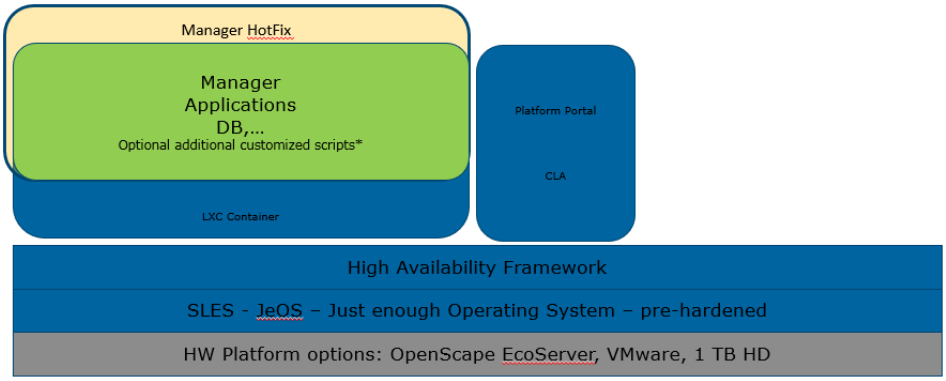


Abbildung 2: OpenScape 4000 Manager-Anwendung-HotFix

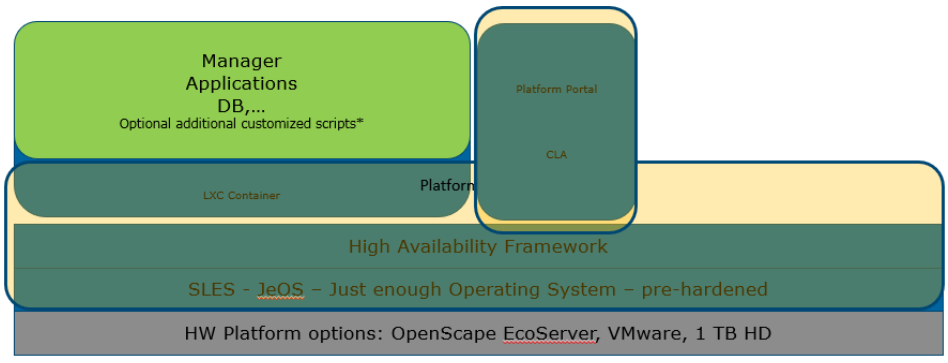


Abbildung 3: OpenScape 4000-Plattform-HotFix

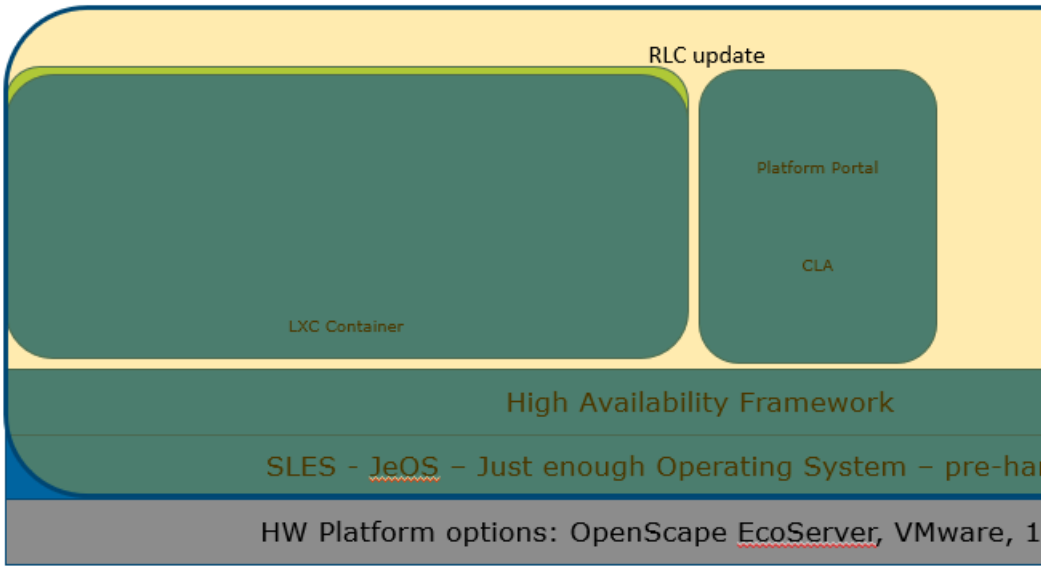


Abbildung 4: OpenScape 4000 RLC Update - einschließlich Hauptversion

2.3.1 Launchpad und Dashboard

Unmittelbar nach Anmeldung beim Manager erscheint links das Launchpad und rechts das Dashboard. Im Launchpad erscheinen alle OpenScape 4000 Manager-Applikationen, für die der momentan angemeldete Benutzer über entsprechende Lizenzen und Zugriffsberechtigungen verfügt. Für den Start dieser Applikationen ist keine weitere Benutzerauthentifizierung erforderlich. Über das Launchpad können außerdem die nativen Management-Applikationen für alle innerhalb des OpenScape 4000 Manager-Netzwerks verwalteten Netzwerk-Objekte gestartet werden (Direktzugang).

Das Launchpad besteht aus folgenden Komponenten: einem Applikationsbaum, über den die einzelnen Applikationen organisiert und gestartet werden können, einer Menüleiste mit Einträgen für die Anpassung des Applikationsbaums, die Übermittlung von Client-Rundsendenachrichten und den Aufruf der Online-Hilfe.

Das Dashboard auf der rechten Seite bietet eine allgemeine Systemstatusübersicht.

Das Launchpad-Dashboard (--> Dashboard) enthält nützliche Informationen zum Systemstatus. Diese Informationen werden nach Informationstyp in die folgenden Gruppen unterteilt:

- Benutzerinfo
- Lizenzverwaltung
- Status Baugruppe
- Configuration Management
- Systemverwaltung
- Systemkomponenten
- Wichtige Hinweise – Komponente, Version, Datum/Uhrzeit des Systemstarts

Der Inhalt des Launchpad-Applikationsbaums hängt von den Registrierungsdaten der einzelnen Applikationen ab und kann je nach Einsatzumgebung differieren. Applikationen, für die eine Interaktion mit einem Netzwerk-Objekt erforderlich ist, erscheinen hier nur, wenn systemseitig

mindestens ein entsprechendes Netzwerk-Objekt (Typ und Version) verfügbar ist.

Blid 2 zeigt das OpenScape 4000 Manager Launchpad mit seinen Standard-Applikationsgruppen.

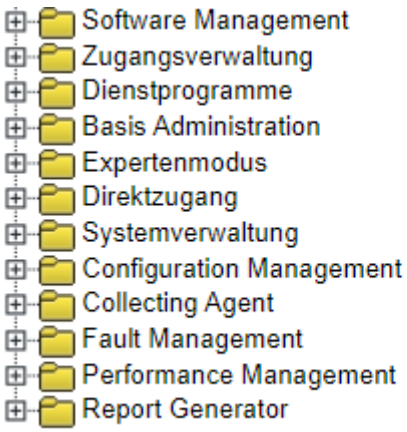


Abbildung 5: Das OpenScape 4000 Manager Launchpad

Blid 3 zeigt das Dashboard des OpenScape 4000 Manager mit dem Status der einzelnen Komponenten.

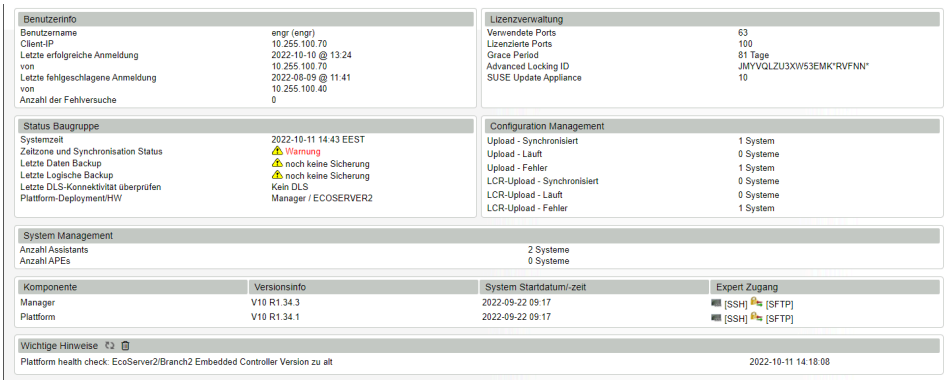


Abbildung 6: Das OpenScape 4000 Manager Dashboard

2.3.2 Softwaremanagement

Softwaremanagement ist die Anwendungsgruppe, die Funktionen zur Installation, Aktivierung, Aktualisierung, Übertragung und Sicherung von Softwareanwendungen und Daten umfasst. Zu den Anwendungen, die im OpenScape 4000 Manager unter Software Management zur Verfügung stehen, gehören Appliance Management (RISO), Backup and Restore (HBR), Software Activation (SWA), Software Manager (SWM).

2.3.2.1 Software-Manager (SWM)

Software-Manager (SWM) ist ein Tool für die LAN-basierte Übermittlung von Software-Komponenten (via TCP/IP) vom Client-PC. Die Software muss zunächst vom Software Supply Server (SWS) auf den Client-PC

heruntergeladen werden; von dort werden die entsprechenden Software-Pakete dann hochgeladen, bevor sie aktiviert werden.

SWM unterstützt das Software Release Management Versioning (SWRM), das ein Herunterladen von Major Release, Minor Release, Fix Release oder HotFix Release ermöglicht.

2.3.2.2 Software-Aktivierung (SWA)

Nachdem ein Major, Minor-, Fix- oder HotFix-Release über SWT (Software-Transfer) an den OpenScape 4000 Manager übertragen wurde, muss es aktiviert werden.

2.3.2.3 Sicherung und Wiederherstellung

Backup and Restore ermöglicht die Erstellung von Sicherungskopien für die Konfigurationsdaten und Software-Komponenten von Manager-Applikationen sowie die Wiederherstellung dieser Daten bei einem eventuellen Anlagenausfall.

Neben den Sicherungs- und Wiederherstellungsfunktionen bietet die Benutzeroberfläche von Backup and Restore dem Benutzer die Möglichkeit, den Inhalt eines oder aller Archive einzusehen, den Status der letzten oder der momentan durchgeführten Backup/Restore-Prozedur abzurufen, externe Geräte wie Bandlaufwerke oder Backup-Server zu verwalten sowie die Backup/Restore-Protokolle zu sichten.

Anmerkung:

Sicherung/Wiederherstellung lehnt alle benutzerdefinierten Dateien oder Unterverzeichnisse im Sicherungsverzeichnis ab. Eine Prüfung warnt den Benutzer, wenn andere Verzeichnisse im Sicherungsordner erstellt werden. Das Verzeichnis, das auf dem Backup-Server für HBR-Sicherungen angegeben ist, und auch das Verzeichnis /.AS/BACKUP/Backup auf der Assistant/Manager-Festplatte müssen nur für HBR-Sicherungen bestimmt sein.

Die Sicherung/Wiederherstellung wird blockiert, wenn sich andere Ordner unter diesem speziellen Verzeichnis befinden.

Am Anfang der Sicherung/Wiederherstellung steht immer der Test des Zielarchivs (Gerät). Der Test des gegebenen Archivs prüft auch, ob es keine unerwarteten Verzeichnisnamen im Archiv gibt.
Wenn die Prüfung fehlschlägt (z. B. weil fremde Verzeichnisse gefunden werden), wird die Sicherung/Wiederherstellung nicht gestartet (schlägt in der Anfangsphase fehl). Das Problem tritt auf, wenn die maximale Anzahl von Sicherungssätzen erreicht ist und ältere Sicherungssätze (die zuvor manuell umbenannt wurden) aktualisiert werden mussten.

2.3.3 Zugangsverwaltung

Die Zugangsverwaltung ist die Zugriffssteuerungszentrale für OpenScape 4000 Manager-Server. Diese Komponente kontrolliert die Benutzerzugriffe auf den Server und bestimmt, welche Applikationen und Leistungsmerkmale den einzelnen Benutzern zur Verfügung stehen.

Über die Zugangsverwaltung können Benutzerkonten angelegt und Passwörter sowie sonstige kontenbezogene Daten verwaltet werden. Ferner ist eine Kontrolle der Benutzerzugriffe über einen Web-Browser, eine Windows Client-Applikation (z. B. ComWin) oder eine Linux-Remote-Shell möglich.

2.3.3.1 Lizenzverwaltung (LicM)

Mithilfe der Anwendung Lizenzverwaltung (LicM) kann der Administrator des OpenScape 4000 Manager-Systems Informationen über die installierte Lizenz anzeigen und den Speicherort des Lizenzagenten des Kunden (Customer License Agent, CLA) konfigurieren. Die Lizenzdaten müssen auf dem konfigurierten CLA installiert und aktiviert werden.

2.3.3.2 OpenScape 4000 License Management Tool (LMT)

Das "Lizenzverwaltungstool" übernimmt die Zuweisung bzw. den Umzug von Software-Lizenzen zwischen den einzelnen OpenScape/HiPath 4000-Knoten in einer Netzwerkumgebung. Dank dieser dynamischen Verschiebung der in LMT-Administrationsgruppen organisierten Lizenzen muss der Kunde beim Umzug/Konfigurieren/Entfernen von Teilnehmern keine Lizenzen zwischen Anlagen verschieben. Die LMT-Funktionalität wird für Einzel-Switches nicht benötigt.

2.3.3.3 Sitzungsverwaltung

Die Sitzungsverwaltungsfunktion unterstützt eine Benutzeroberfläche, über die das Benutzerpasswort bei Bedarf geändert werden kann, sowie einen Web-Sitzungs-Manager, der einen Überblick über alle Web-Sitzungen des aktuellen Benutzers bietet. Benutzer können die Anmelde- und Anbindungsinformationen für alle eigenen Sitzungen einsehen und diese Sitzungen bei Bedarf manuell beenden (deaktivieren).

2.3.3.4 Kontenverwaltung

Die Kontenverwaltungskomponente der Zugangsverwaltung verfügt über Benutzerschnittstellen für die Administration von Benutzer- und Systemkonten sowie die Konfiguration von Zugriffsrechten und Zugriffsrechtegruppen.

2.3.3.5 Verwalten von Web-Server-Zertifikaten

Die Funktion "Verwalten von Webserver-Zertifikaten" beinhaltet Tools zum Erstellen, Importieren und Aktivieren von SSL-Zertifikaten auf dem aktuellen Webserver. Ein Zertifikat kann selbstsigniert sein oder per

Zertifikatsignieranforderung (Certificate Signing Request, CSR) erstellt werden. Die individuelle Stammzertifizierungsstelle wird generiert und zur Signierung des CSR im Certificate Network Management verwendet.

2.3.3.6 Sicherheitsmoduskonfiguration

Die allgemeinen Sicherheitseinstellungen werden über die Sicherheitsmoduskonfiguration verwaltet. Diese Konfiguration deckt auch mögliche Einschränkungen für den Remote-Zugang über SSH-, SecM-, ODBC-, JDBC-Schnittstellen ab. Der Authentifizierungsmodus (Passwort und/oder PKI), die Gateway-Sicherheit sowie die TLS-Protokollauswahl können aktiviert bzw. deaktiviert werden.

2.3.3.7 Konfiguration der PKI-Authentifizierung

Dieses Tool dient zur Verwaltung der Public Key Infrastructure (PKI), die eine Authentifizierung gegenüber dem System mittels PKI-Zertifikat erlaubt. Dieses Tool verwaltet die Konfiguration der PKI-Baumstruktur von Zertifikaten und die Konfiguration des Zertfikatsperrmodus. Zur Überprüfung der Gültigkeit des Client-Zertifikats kann die CRL- oder OCSP-Methode herangezogen werden.

2.3.3.8 Konfiguration der Single Sign-On Authentifizierung

Der OpenScape 4000 Manager oder Assistant unterstützt die Funktion "Single Sign-On" mit Active Directory. Über diese Funktion können sich authentifizierte Domänenbenutzer nahtlos mit einem einzigen Klick am OpenScape 4000 Manager oder Assistant anmelden. Die Authentifizierung basiert auf Kerberos-Anmeldeinformationen (Authentifizierungs-Token), die automatisch vom Client-Webbrowser bereitgestellt werden.

2.3.3.9 Banner auf Anmeldeseite anpassen

Diese Applikation wird verwendet, um kundenindividuelle Text-Banner für die Login-Seite zu entwerfen. Derartige Banner werden beim Anmelden am System über SSH und Web-Browser angezeigt.

2.3.4 Dienstprogramme

Diese Applikationsgruppe umfasst die folgende Applikation: Import/Export API (XIE).

2.3.4.1 Import/Export API (XIE)

Über ein optionales Leistungsmerkmal, dass eine offene Anwendungsprogrammierschnittstelle (Application Programming Interface, API) bereitstellt, unterstützt der OpenScape 4000 Manager den Datenaustausch mit Drittanbieter-Applikationen (Import/Export). Kunden können so bequem und

schnell Informationen (z.B. personengebundene Mitarbeiterdaten) aus der/zur OpenScape 4000 Manager-Datenbank herunterladen/hochladen. Ferner ermöglicht dieser Ansatz unter anderem auch den Export von Feldinhalten aus der Teilnehmerdatenbank an aktuelle oder zukünftige Verzeichnisdienste.

OpenScape 4000 Manager unterstützt eine erweiterte API, die es dem Kunden ermöglicht, Daten mit Hilfe eigener Datenbank-Applikationen aus der OpenScape 4000 Manager-Datenbank auszulesen bzw. dorthin zu schreiben.

Es gibt mehrere Arten der API-Kommunikation mit dem OpenScape 4000 Manager:

1) API C++-Programmierschnittstelle mit API-Klassen-Bibliothek Der Kunde verwendet ein eigenes Applikationsprogramm und programmiert den Datenaustausch selbst.
2) API-Datei-Schnittstelle Der Datenaustausch wird über Linux-Skripts auf CLI-Ebene realisiert (Befehlszeilenschnittstelle).
3) Desktop-Import/Exporttabelle. API-basierter Import/Export-Client (eine Windows-Desktop-Anwendung, die über LAP-XIE heruntergeladen werden kann).
4) Verschlüsselte XIE-Webserver-Schnittstelle. SOAP-basierte Schnittstelle für den Datenaustausch.
5) XIE Webservice: SOAP-basierte HTTPS-Schnittstelle für den Export/Import von Daten aus der/in die OpenScape 4000 Manager-Datenbank. Diese Daten können anschließend in Kundenapplikationen verwendet werden.

2.3.5 Basis Administration

Basis Administration ist eine Applikationsgruppe bestehend aus Webmin Base Administration und Logging Management.

2.3.5.1 Webmin Base Administration

Die Webmin-Basisverwaltung ermöglicht

- LAN-Konfiguration (LAN-Karten, DNS, Hosts, Routen, Dienstzugang)
- WAN-Konfiguration (Firewall)
- Systemverwaltung (Datum/Uhrzeit, Zeitzone, Neustart/Herunterfahren, Anwendungsprozesse)

2.3.5.2 Logging Management

Das Logging Management ist eine Basisapplikation für die zentrale Anmeldung bei anderen Applikationen, die ebenfalls auf der OpenScape 4000 Manager-Plattform eingesetzt werden. Diese Applikationen nutzen gegebenenfalls eigene Einrichtungen für die Aufzeichnung von Detaildaten. Gemeinsam ist jedoch allen Applikationen, dass sie auf das Logging Management zugreifen, um einen Überblick über applikationsspezifische Aktivitäten und Fehlerereignisse zu speichern.

Über das Logging Management können beispielsweise die Aktivitäten einer bestimmten Switch-Einheit, alle Aktivitäten sämtlicher Switches an einem bestimmten Tag oder alle Fehler einer bestimmten Applikation oder eines

bestimmten Prozesses eingesehen werden. Über eine Web-Schnittstelle für umfassende Funktionszugriffe kann der Benutzer Abfragen generieren, modifizieren und speichern, um konkrete Aktivitäten und Fehlerprotokolle aufzuzeichnen. Des weiteren sind Administrationsfunktionen verfügbar, über die Aktivitätsereignisse an andere Plattformen wie beispielsweise Remote-Service-Center weitergeleitet werden können.

2.3.6 Direct Access

Über das Leistungsmerkmal Direktzugang des OpenScape 4000 Managers kann der Benutzer bei Bedarf die native Management-Applikation für ein Netzwerk-Objekt starten. Eine Einzelanmeldung, bei der sich der Benutzer bei dem gewählten Netzwerk-Objekt nicht explizit anzumelden braucht, ist nur möglich, wenn die Anmeldedaten an die betreffende Applikation übergeben werden. Der Benutzer muss in diesem Fall die erforderlichen Anmeldedaten bereitstellen, wenn das Netzwerk-Objekt von der Systemverwaltung generiert wird.

Der OpenScape 4000 Manager unterstützt Web-Applikationen, Windows-Applikationen sowie CLI-basierte Applikationen für den Direktzugang.

2.3.6.1 OpenScape 4000

Mit dieser Funktion können Sie die Funktion Remote Access bzw. File Transfer oder die Applikation des jeweiligen (über die Systemverwaltung) definierten Switches aufrufen. Sie verwendet Single Sign-On (SSO), um die Authentifizierung gegenüber dem Assistant zu umgehen.

2.3.6.2 Batch Generator

Nach der Einrichtung aller Anlagen in der Systemverwaltung und in Configuration Management muss der OpenScape 4000 Manager-Server mit den verwalteten OpenScape/HiPath 4000-Anlagen synchronisiert werden. Diese Datenbanksynchronisierung gewährleistet, dass der OpenScape 4000 Manager-Server stets den aktuellen Anlagenstatus enthält.

Um diese Synchronisierung durchzuführen, führt Configuration Management auf jeder OpenScape/HiPath 4000-Anlage ein Upload durch. OpenScape 4000 Manager Configuration Management stellt eine grafische Benutzeroberfläche (GUI) für die Administration dieser Anlagen bereit.

2.3.7 Systemverwaltung

Die Systemverwaltung ist die Applikation, die zur Einbindung (Hinzufügen/Löschen) von OpenScape 4000-Anlagen in die Verwaltung des OpenScape 4000 Manager verwendet wird.

2.3.8 Configuration Management (CM)

Configuration Management ist der zentrale Einstiegspunkt für die Verwaltung der Teilnehmerdaten. Eine benutzerfreundliche Browser-Schnittstelle ermöglicht Administratoren die Durchführung von sog. MAC-Maßnahmen (Moves, Adds & Changes) zur Verlagerung, Ergänzung oder Änderung von persönlichen Daten und Teilnehmerdaten in OpenScape 4000-Netzwerken. Knotenübergreifende Umzüge sowie die Verwaltung von Netzwählplanen werden ebenfalls unterstützt. Die Netzwerk-Implementierung von Configuration Management (CM-N) unterstützt keine ACD-, Baugruppen-, Leitungssatz- und Wartungsobjekte. Bei Bedarf kann jedoch die lokale CM-Version vom OpenScape 4000 Assistant direkt aufgerufen werden, um diese Leistungsmerkmale nutzen zu können.

2.3.9 Collecting Agent (COL)

Der Collecting Agent (COL), die in den OpenScape 4000 Manager integrierte Hauptkomponente des Account Management (AM), sammelt Abrechnungsdaten für AM sowie Verkehrsmessungsdaten für das Performance Management (PM). Über die web-basierte COL-Benutzeroberfläche kann der Benutzer verschiedene administrative Aufgaben ausführen, beispielsweise Ein- und Ausgabeformate sowie Ausgabezeilen und Filter definieren oder den COL-Status überwachen. Eine von der COL-Startseite aufrufbare Protokollierungsfunktion ermöglicht es, verschiedene Protokolltypen sowie Datums- und Uhrzeitwähler für die Definition des Reportintervalls der Protokollereignisse anzugeben.

2.3.10 J-HPT-Tool

Der Java Husim Phone Tester (J-HPT) for Web ist ein Webtool zur Fernsteuerung von IP-Telefonen. J-HPT Web wird verwendet, die tatsächlichen Einstellungen eines physikalischen Telefons auf einem Web-Inferface abzubilden und vorgenommene Einstellungen an das Telefon zu senden.

2.3.11 Trace Download

Trace Download dient zur Erfassung von Diagnosedaten (sog. Trace-Protokollen) für spezifische Use Cases oder für Komponenten auf der Manager-Seite, um die Diagnose zu vereinfachen. Wenn bei GVS ein Problem-Ticket eingereicht wird, sollten die Diagnosedaten aus dem Trace Download immer angehängt werden.

2.3.12 Alarmkonfigurator

Der "Alarm-Konfigurator" wird für die Verwaltung von Switch-Alarmen sowie die Zuweisung von Alarmen zu bestimmten Teilnehmern oder Leitungssätzen eingesetzt. Ferner ermöglicht dieses Tool eine automatische Alarm-Generierung für Leitungssätze, denen noch keine Alarme zugewiesen wurden. Der Alarm Configurator, der über das OpenScape 4000 Manager Launchpad gestartet wird, unterstützt verschiedene Optionen für die Aktualisierung switch-

spezifischer Alarmdaten, die Verwaltung von Alarmen im Servicemodul sowie die Definition und Prüfung von Alarmzuweisungen für bestimmte Teilnehmer und Leitungssätze.

2.3.13 SNMP-Konfigurator

Der SNMP-Konfigurator wird verwendet, um die SNMP-Protokolleinstellungen auf dem Host anzuzeigen. Die Parameter, die der Benutzer sieht, werden mit OpenScape 4000 Assistant zentral eingestellt.

Weitere Informationen finden Sie in OpenScape 4000 Assistant V10, Simple Network Management Protocol HiPath SNMP, Administratorhandbuch.

2.3.14 Performance Management (PM)

Die Anwendung Performance Management (PM) dient primär zur Verarbeitung von Verkehrsmessungsdaten. Die meisten Daten für PM stammen aus den vom Collecting Agent (COL) erfassten CDR-Datensätzen, ZAUSL-Dateien und CMI-Dateien. Über eine web-basierte Benutzeroberfläche kann der PM-Benutzer vereinbaren, welche Telefonie-Positionen (Nebenstellen, Sammelanschlüsse, Vermittlungsplätze, VPL-Gruppen, Leitungssätze, Leitungsbündel und Schnurlos-Konzentratoren) von der Messfunktion erfasst werden sollen. Es besteht ferner die Möglichkeit, Berichte bzw. Berichtgruppen zu generieren, anzupassen und auszuführen, und bei Bedarf können individuelle Filterkriterien definiert und auf diese Berichte angewendet werden.

2.3.15 Report Generator

Der Report Generator ist eine zur OpenScape 4000 Manager-Plattform zählende Anwendung, die die Reporting-Aufgaben anderer OpenScape 4000-Anwendungen vereinfacht. Dieses Leistungsmerkmal gestattet die Erzeugung flexibler benutzerdefinierter Reporte anhand neu erstellter oder vordefinierter Muster, die bestimmten Anwendungen und Reportobjekten entsprechend modifiziert werden können. Es stehen diverse Optionen für das Anzeigen, Drucken und Exportieren von Reporten zur Verfügung.

Eine E-Mail-Benachrichtungsfunktion ermöglicht das Definieren automatisch zu versendender E-Mails mit oder ohne Exportdateien als Anlage im HTML-, PDF-, CSV- oder XML-Format, nachdem ein Report erzeugt wurde.

3 Vorbereitung und Installation des OpenScape 4000 Manager-Servers

Dieses Kapitel enthält Verfahren, die vor und während der Installation des OpenScape 4000 Manager-Servers durchgeführt werden müssen.

3.1 Vorbereitung

Führen Sie die folgenden Schritte aus, um die Installation des Managers vorzubereiten:

1) Erfassen Sie die MAC-Adresse einer beliebigen LAN-Schnittstelle der zu installierenden Hardware.

2) Füllen Sie die XML-Konfigurationsdatei aus.

Anmerkung: Weitere Informationen zur XML-Datei finden Sie im Dokument OpenScape 4000 Installation, Konfiguration und Migration, Kapitel "XML-Konfigurationsdatei".

Anmerkung: Vorlagen und Beispiele für verschiedene XML-Konfigurationsdateien für alle Bereitstellungstypen sind auf dem ISO/Installations-Stick im Verzeichnis \Documentation verfügbar (z. B. firstinst-netw-xml_examples_v4.zip).

---

3) Kopieren Sie die XML-Datei(en) in den Ordner **config** auf dem Installationsmedium.

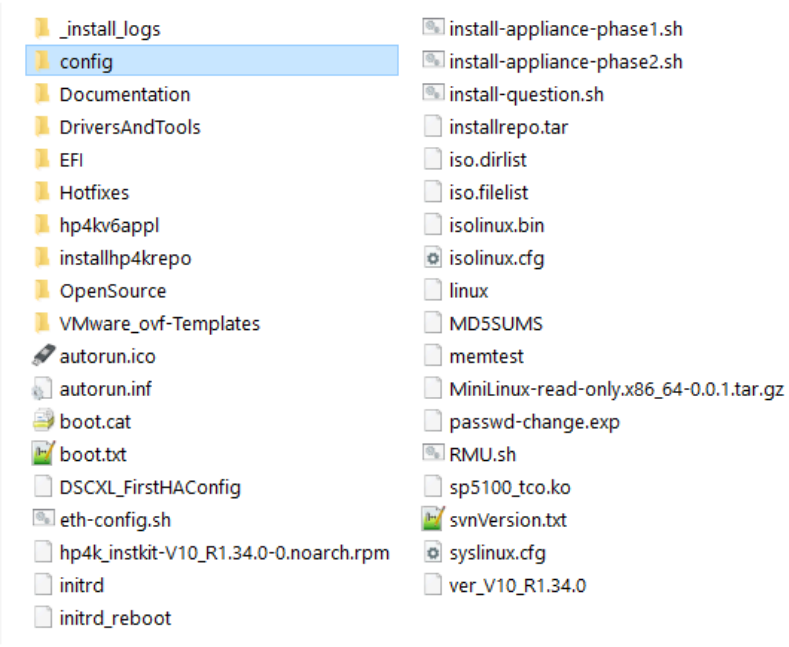


Abbildung 7: Speicherort der XML-Datei auf dem Installationsmedium

---

Anmerkung:

Es ist möglich, mehrere XML-Konfigurationsdateien für mehrere Systeme in den Ordner **config** zu kopieren, wenn diesen unterschiedliche MAC-Adressen zugewiesen sind.

3.2 Installationsvorgang mit Monitor/Tastatur

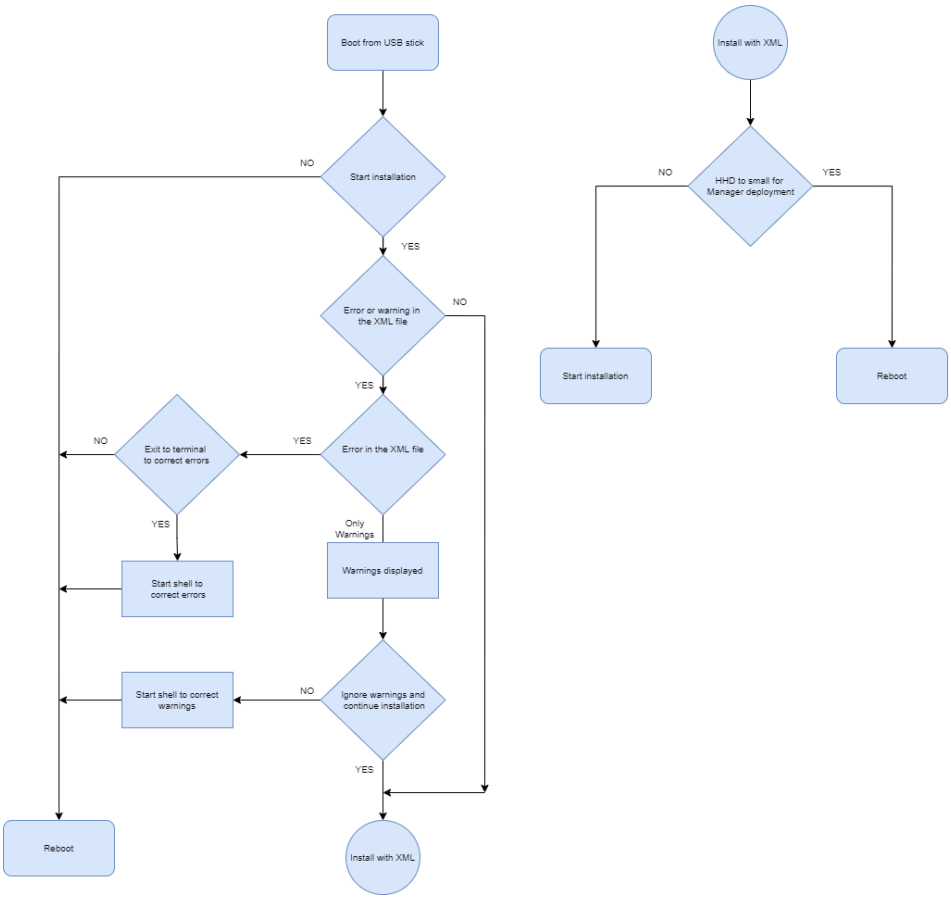


Abbildung 8: Übersicht über den Installationsvorgang

Führen Sie die folgenden Schritte aus, um die Installation des Managers über Monitor/Tastatur durchzuführen:

1) Rufen Sie das Startmenü auf und wählen Sie das Boot-Gerät aus:

EcoServer/Branch: F11 direkt, F11 Konsole

2) Bitte beachten Sie, dass das verwendete USB-Gerät zweimal angezeigt werden kann (einmal mit und einmal ohne UEFI-Präfix), wenn Sie F11 zur

Auswahl des Boot-Geräts im BIOS verwenden. Es sollte das Boot-Gerät ohne UEFI-Präfix ausgewählt werden.

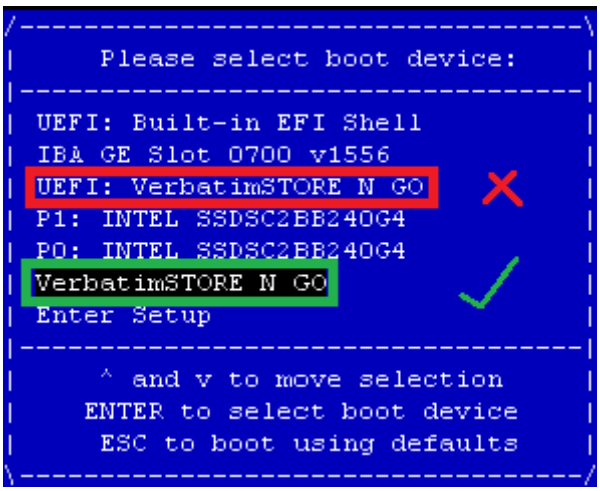


Abbildung 9: BIOS-Boot-Geräteauswahl

3) Booten Sie den Computer vom Installationsmedium (USB-Stick). Sie werden aufgefordert, die Installation zu starten oder neu zu starten.

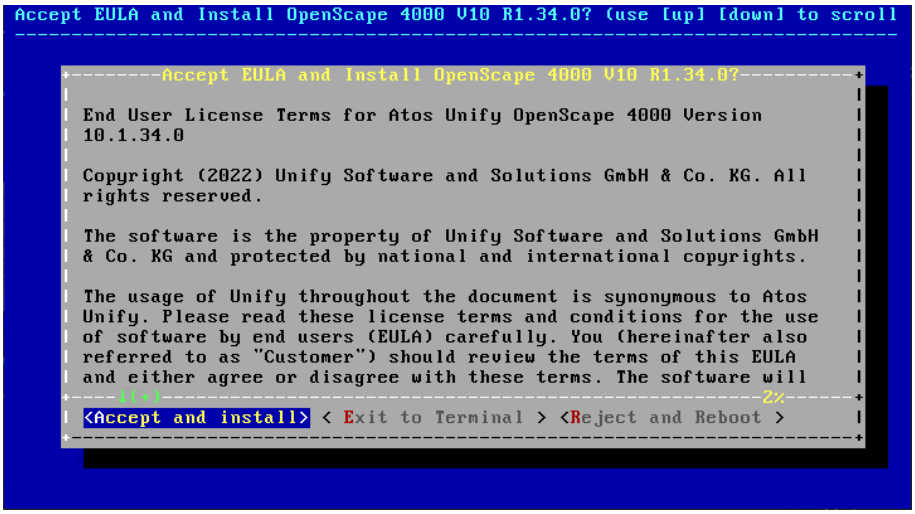


Abbildung 10: Computer vom Installationsmedium booten

4) Prüfen Sie, ob eine kompatible XML-Konfigurationsdatei vorhanden ist.

Wenn Sie Ja (Installation starten) wählen, wird auf dem Installationsmedium (im Ordner config) geprüft, ob eine kompatible XML-Konfigurationsdatei für die Hardware vorhanden ist.

Für diesen Schritt gibt es mehrere Möglichkeiten:

- **Fall 1**: Es wird eine XML-Konfigurationsdatei gefunden.

  Wenn eine XML-Konfigurationsdatei gefunden wird, die eine MAC-Adresse von einer der Systemschnittstellen enthält, wird die Datei auf Fehler bezüglich der Linux-Konfigurationsdaten geprüft.

  a) Fall 1.1: Die XML-Konfigurationsdatei enthält keine Fehler/ Warnungen

  Der Installationsvorgang prüft den verfügbaren Speicherplatz auf der Festplatte und stellt fest, ob die Bereitstellung mit dem Speicherplatz auf der Festplatte übereinstimmt.

  Weitere Informationen finden Sie in Schritt 5.

  b) Fall 1.2: Die XML-Konfigurationsdatei enthält Fehler

  Wenn die XML-Konfigurationsdatei Fehler enthält, wird die Installation mit Fehlermeldungen abgebrochen. Die Fehlerprotokolle werden auf dem Installationsmedium in den Ordner **_install_logs** geschrieben.

  Beispiele:

  – Mehr als eine XML-Konfigurationsdatei entspricht einer MAC-Adresse dieses Servers:

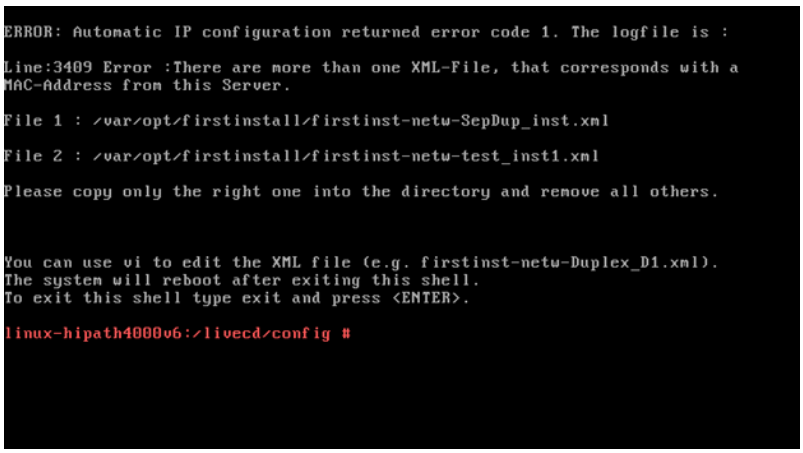


  Abbildung 11: Erstinstallation - Protokolldatei für eine XML-Konfigurationsdatei mit Fehlermeldungen

  – Falsche Bereitstellung in der XML-Konfigurationsdatei

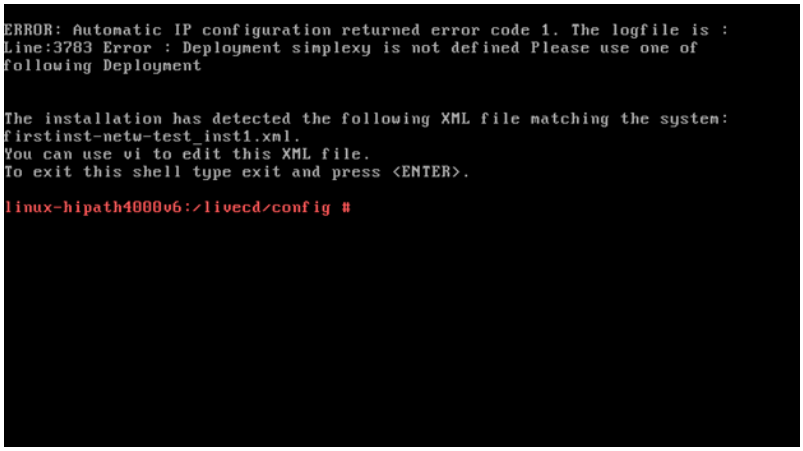


Abbildung 12: Erstinstallation - Protokolldatei für eine XML-Konfigurationsdatei mit Fehlermeldungen

c) Fall 1.3: Die XML-Konfigurationsdatei enthält Warnungen

Wenn in der XML-Konfigurationsdatei nur Warnungen gefunden werden, werden diese angezeigt.

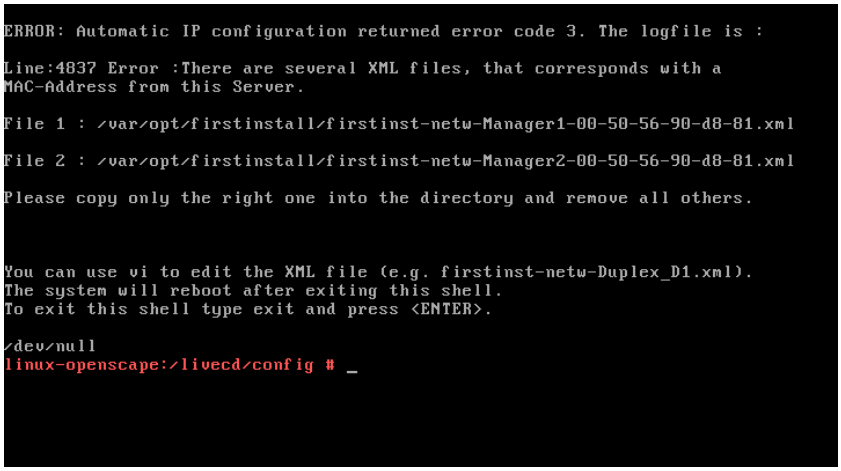


Abbildung 13: Erstinstallation - XML-Konfigurationsdatei mit Warnungen

Drücken Sie **Weiter**. Der folgende Bildschirm wird angezeigt:

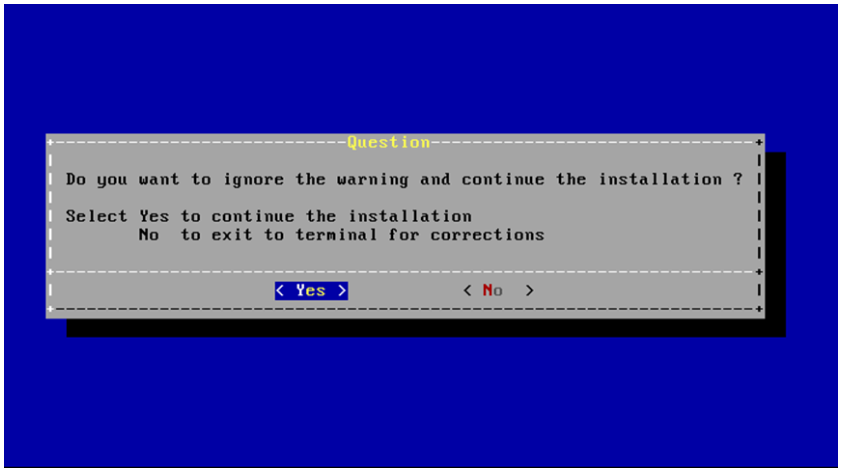


Abbildung 14: Erstinstallation - XML-Konfigurationsdatei mit Warnungen

Im Menü links können Sie folgende Aktionen auswählen:

– **Ja** , um die Warnungen zu ignorieren und den Installationsvorgang fortzusetzen.

oder

– **Nein** , um die Installation zu beenden und eine Terminalsitzung zur Durchführung der entsprechenden Korrekturen zu öffnen.

Wenn Sie **Ja** wählen, prüft der Installationsvorgang den verfügbaren Speicherplatz auf der Festplatte, um festzustellen, ob die Bereitstellung mit dem erforderlichen Festplattenspeicherplatz übereinstimmt. Weitere Informationen finden Sie in Schritt 5.

Wenn Sie **Nein** wählen, wird der folgende Bildschirm angezeigt:

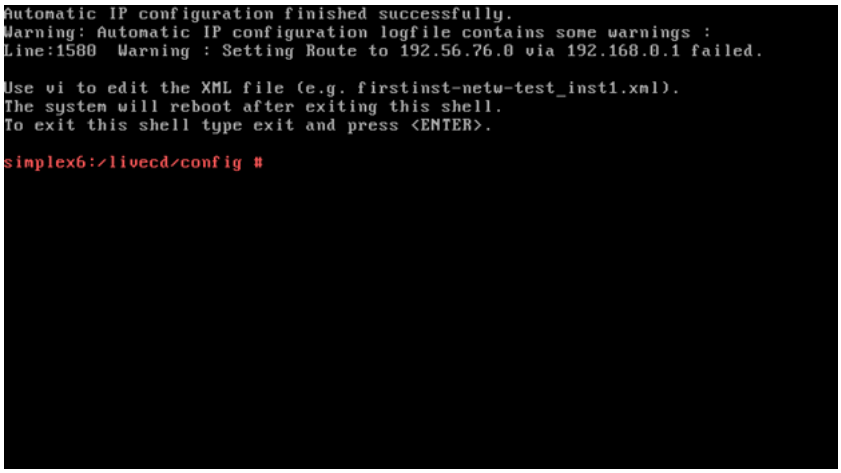


Abbildung 15: Erstinstallation - Protokolldatei für eine XML-Konfigurationsdatei mit Warnungen

- **Fall 2: Keine XML-Konfigurationsdatei gefunden**

  Wenn keine XML-Konfigurationsdatei gefunden wird, die die MAC-Adresse der Hardware enthält, auf der die Installation gerade läuft,

können Sie die Installation mit einer Standardkonfiguration fortsetzen oder eine Shell-Sitzung starten, um einige Korrekturen vorzunehmen.

Im Falle eines falschen *.xml-Dateinamens wird eine Warnmeldung angezeigt: "Keine entsprechende XML-Datei...". Der Dateiname muss mit **firstinst-netw-*.xml** beginnen.

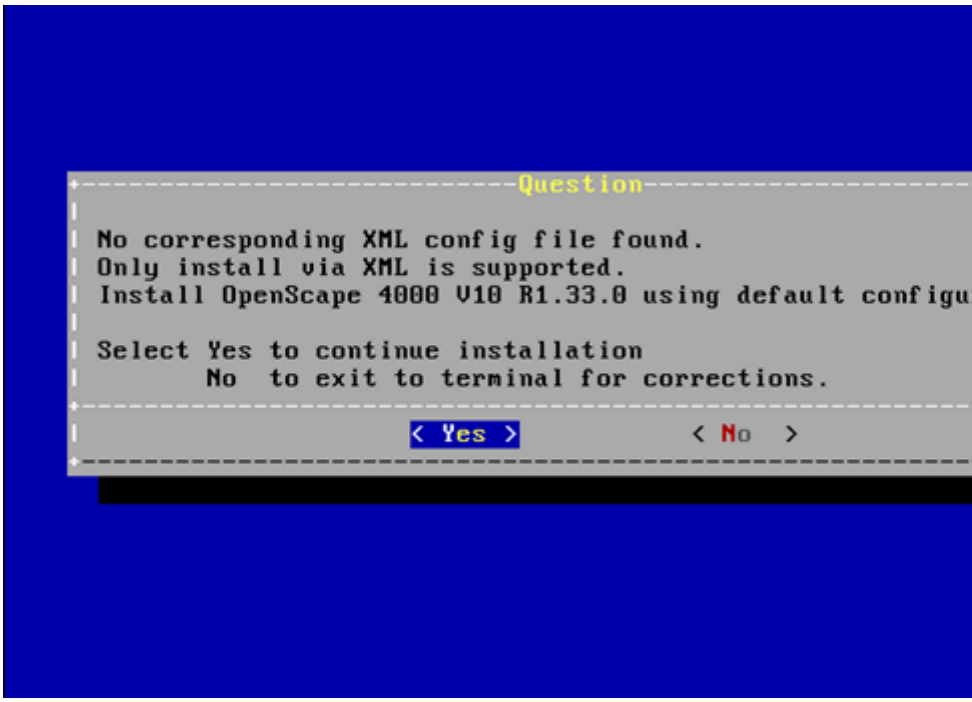


Abbildung 16: Erstinstallation - XML-Konfigurationsdatei nicht gefunden

a) Fall 2.1: Installation mit Standardkonfiguration

Wenn Sie **Ja** wählen, wird die Installation gestartet, aber für eth0 wird eine Standard-IP-Adresse konfiguriert (IP-Adresse 192.168.0.2 /24).

In diesem Fall empfiehlt es sich, die Installation mit einer korrekt konfigurierten XML-Datei zu wiederholen.

Bei der Installation wird der verfügbare Speicherplatz auf der Festplatte geprüft und die möglichen Bereitstellungen ermittelt. Weitere Informationen finden Sie in Schritt 5.

b) Fall 2.2: Shell starten und Korrekturen vornehmen

Wenn Sie **Nein** wählen, wird die folgende Warnung angezeigt und Sie haben die Möglichkeit, den Fehler zu korrigieren.

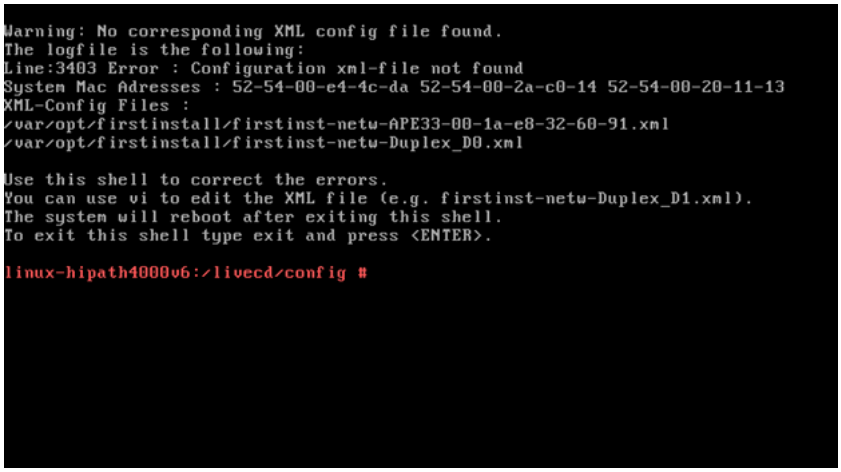


Abbildung 17: Erstinstallation - Warnung, dass keine entsprechende XML-Konfigurationsdatei gefunden wurde

---

Anmerkung: Prüfen Sie, ob sich die .xml-Datei im richtigen Pfad befindet, und wenn ja, prüfen Sie auch, ob sie die richtige MAC-Adresse des Knotens enthält. Um die .xml-Datei zu bearbeiten, können Sie den vi-Editor verwenden.

---

5) Überprüfen Sie den verfügbaren Speicherplatz.

Für diesen Schritt gibt es zwei Möglichkeiten:

- **Fall 1: Die Bereitstellung entspricht der Festplattengröße**

  Wenn die Festplatte für die Bereitstellung der XML-Konfigurationsdatei geeignet ist, wird geprüft, ob es sich bei der aktuellen Bereitstellung um eine Duplex- oder eine getrennte Duplex-Bereitstellung handelt. Weitere Informationen finden Sie in Schritt 6.

6) Wenn die Installation erfolgreich abgeschlossen ist, wird eine Meldung angezeigt und Sie werden aufgefordert, das Installationsmedium zu entfernen und OK zu drücken, um das System neu zu starten.

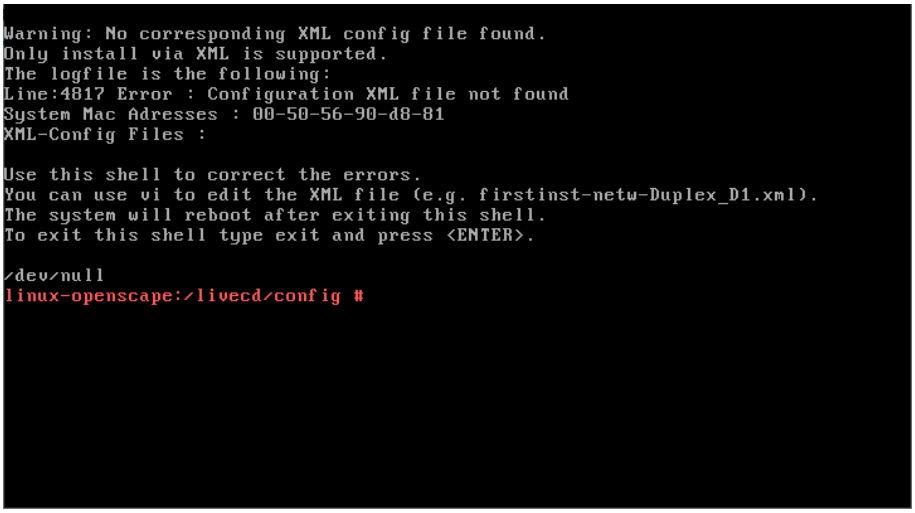


Abbildung 18: Installation erfolgreich abgeschlossen

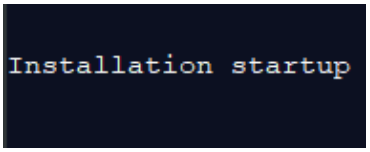
7) Nach dem Neustart startet das System mit der installierten Software auf der Festplatte und kann über jede konfigurierte IP-Adresse der angeschlossenen LAN-Schnittstellen erreicht werden.

3.3 Installation nur über das OLED-Display und die "ON"-Taste

Ab V8 R1.19 kann die OpenScape 4000-Installation auf dem EcoServer nur noch über das OLED-Display und die "ON"-Taste auf der linken Seite durchgeführt werden. Es ist nicht notwendig, einen Monitor oder eine Tastatur anzuschließen, da die notwendigen Installationsschritte über die Taste bestätigt werden. Diese Methode kann nun auch für die Manager-Bereitstellung verwendet werden.

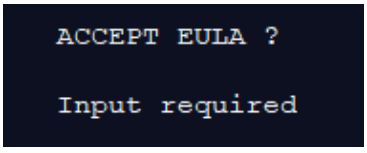
Führen Sie die folgenden Schritte aus, um die Installation mit dem OLED-Display durchzuführen:

1) Stecken Sie den USB-Stick ein, entfernen Sie alle HGs/SSDs und schalten Sie den EcoServer ein. Warten Sie etwa 2-3 Minuten, bis die Installation abgeschlossen ist. Das System zeigt die Meldung "Installation Startup" an.

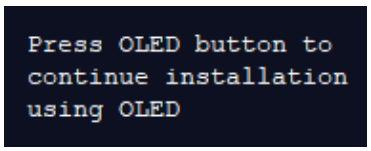


Um das DSCXL2 aus- und wieder einzuschalten, verwenden Sie die Schaltfläche **HW Reset.**

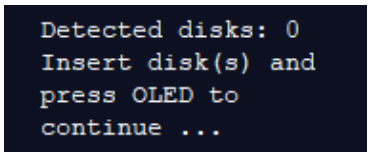
2) Anschließend wird auf dem OLED-Display die Meldung „EULA akzeptieren?“angezeigt. Drücken Sie die Taste **ON**.



3) Warten Sie, bis die nächste Aufforderung angezeigt wird. Sie werden aufgefordert, die Installation mit OLED fortzusetzen.

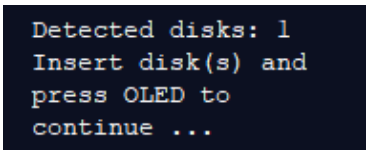


Drücken Sie die Taste **ON** und warten Sie, bis die folgende Meldung auf dem OLED angezeigt wird:



4) Legen Sie nun je nach Einsatzmodell eine oder zwei Festplatten/SSDs ein und warten Sie, bis die richtige Anzahl von Festplatten auf dem OLED-Display angezeigt wird.

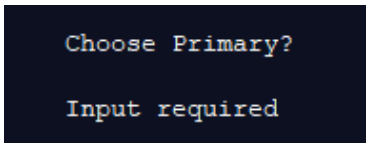
Drücken Sie die Taste **ON** , um die Installation fortzusetzen.



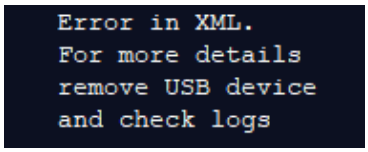
Anmerkung: Die Anzeige wird alle 30 Sekunden automatisch aktualisiert.

Anmerkung: Im Falle von Duplex- oder GSD-Systemen muss der im XML als primär konfigurierte Knoten bestätigt werden.

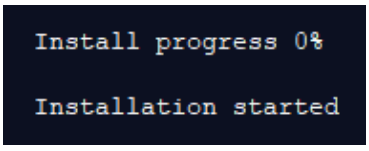
Drücken Sie zur Bestätigung die Taste **ON** .



Anmerkung: Falls ein Fehler in der XML-Datei festgestellt wurde (z. B. fehlende obligatorische Parameter), wird die folgende Meldung angezeigt:

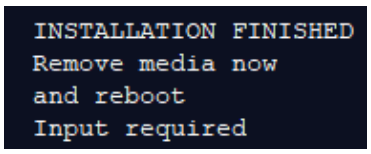


Während die Installation von OpenScape 4000 läuft, zeigt das OLED folgende Meldung an:

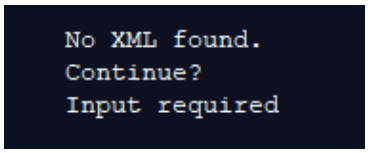


5) Nachdem die Installation abgeschlossen ist, entfernen Sie das USB-Laufwerk und drücken Sie ein weiteres Mal die Taste **ON**, um das

OpenScape4000-System neu zu starten und zum ersten Mal in Betrieb zu nehmen.

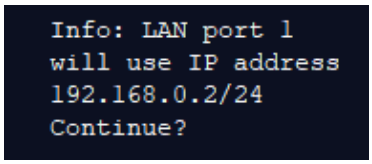


Wenn eine Installation ohne XML durchgeführt wird, zeigt das OLED die folgende Meldung an:



Drücken Sie die Taste **ON**, um die Installation ohne XML fortzusetzen.

Im Falle einer Installation ohne XML zeigt das OLED die IP-Adresse an, die der ersten physikalischen LAN-Schnittstelle des DSCXL2/Eco Servers/Zweigstelle zugewiesen wird. Sie können die erste physische LAN-Schnittstelle mit einem Netzwerk verbinden, in dem ein DHCP-Server läuft, und der DSCXL2/Eco-Server/Branch wird dann versuchen, eine IP-Adresse zu erhalten. Dies wird auf dem OLED-Display zur Überprüfung angezeigt. Fahren Sie fort, indem Sie erneut die Taste **ON** drücken. Am Ende der Installation ist das OpenScape4000 Platform Portal über diese IP-Adresse erreichbar. Falls keine DHCP-Antwort empfangen wird, wird die Standard-IP-Adresse/Netzmaske auf 192.168.0.2/255.255.255.0 gesetzt.



Anmerkung: Sollten Fehler auftreten, entfernen Sie den USB-Stick, überprüfen Sie die Protokolle im Verzeichnis "<usb_stick_root>/_install_logs", beheben Sie die Probleme und beginnen Sie erneut bei Schritt 1.

Es wird empfohlen, den ECO-Server/Branch vor Schritt 1 auszuschalten. Beim DSCXL2 wird außerdem empfohlen, alle Festplatten zu entfernen, den USB-Stick anzuschließen und mit der HW-Reset-Taste zu Schritt 1 zurückzukehren.

3.4 OpenScape 4000-Installation auf einem Hypervisor

Bitte beachten Sie die OpenScape Virtual Machine Resourcing and Configuration Guide für die Dimensionierung der für die jeweilige Bereitstellung erforderlichen Ressourcen.

Benötigte Informationen vom Kunden

- Netzwerkidentifikationsnamen, z. B.: Management, Sprache, Atlantik.

- Erstinstallationsdatei firstinst-netw-XXXXX.xml (einschließlich der Konfigurationsdaten für OpenScape 4000 Softgate, sofern diese verfügbar sind).
- Freie IP-Adresse aus dem Kundenadressbereich für den Service-PC.
- MAC-Adresse.

Service PC

Der Service PC wird für die folgenden Aufgaben benutzt:

- Zugriff auf den OpenScape 4000 Assistant nach der Erstinstallation.
- Zugriff auf die OpenScape 4000 mit Hilfe von OpenScape 4000 Expert Access (=Comwin) nach der Erstinstallation.
- Verwendung der VMware-Umgebung.
- Erzeugen und Anpassen der Konfigurationsdateien.
- Ändern der OpenScape 4000 ISO-Datei.

Vorbereitungen auf dem Service PC

- Tragen Sie eine freie Kunden IP-Adresse und Netzmaske auf der LAN-Karte des Service PC ein.

Konsole > **Start** > **Systemsteuerung** > **Netzwerk und Internet** > **Netzwerkverbindung** > **LanAdapter** > Rechter Mausklick auf **Eigenschaften** > **TCP / ipV4** > **Eigenschaften …**

Wählen Sie das **Optionsfeld Folgende IP-Adresse verwenden** und bestätigen Sie mit **OK**.

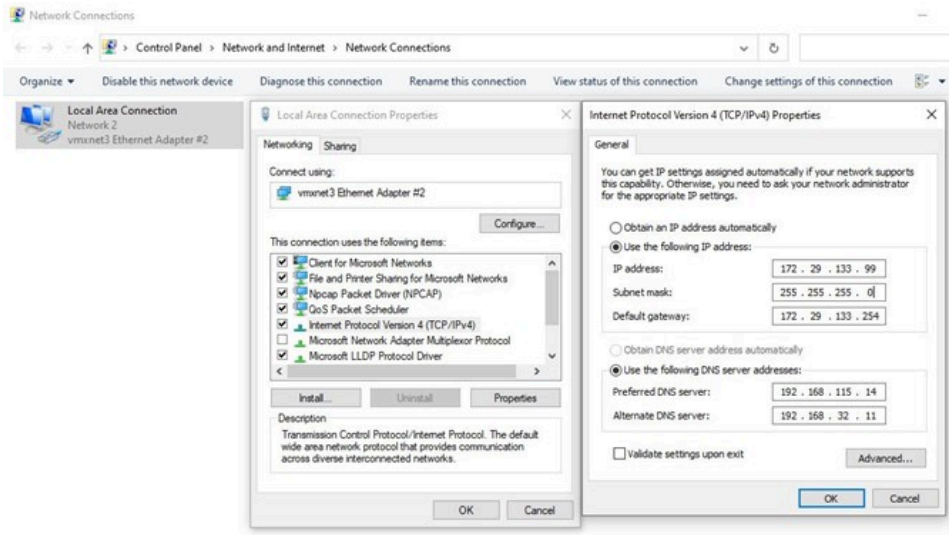


Abbildung 19: Beispiel für IP-Adresse und Netzmaske für den Service-PC

- Erzeugen Sie auf dem PC einen Arbeitspfad für:
  - XML-Datei,
  - ISO-Editor-Software (z. B. AnyBurn),
  - Hotfixes.
- Kopieren Sie die Installations-ISO-Datei an einen Ort, auf den der Hypervisor Client zugreifen kann (z. B. Datenspeicher).

Vorbereiten der OpenScape 4000 ISO-Datei

Für die .ISO-Bearbeitung kann der {{user}} seine bevorzugte Bearbeitung wählen, wobei AnyBurn erfolgreich verifiziert wurde.

Die Erstellung einer benutzerdefinierten .ISO-Datei mit der obligatorischen Konfigurationsdatei und optionalen Hotfixes ermöglicht es dem {{user}}, OpenScape 4000 ohne die Verwendung von zusätzlichen FLP- und HF-Images zu installieren.

Wichtig:

- AnyBurn-Werkzeug. Die im Labor geprüfte Mindestversion war V5.9.
- Die XML-Konfigurationsdatei, die mit dem XML Config File Generator (im Lieferumfang von HiPath 4000 Expert Access enthalten) generiert wurde, sollte unter /config auf das ISO kopiert werden.
- Hotfixes für die Installation mit dem ISO sollten nach /hotfixes kopiert und die Aktivierung im XML Config File Generator konfiguriert werden, falls erforderlich.

Anmerkung: Die frühere Installationsmethode mit FLP und dem HF-Image funktioniert im Legacy-Modus. Für diese Methode wird kein Support angeboten. Die benötigten Ressourcen befinden sich auf dem Installationsmedium unter `\DriversAndTools\VMware_Installation_Resources_Legacy_V10`

Hotfix Installation vorbereiten

Bei der Erstinstallation können Hotfixes aktiviert werden. Zu diesem Zweck können die benötigten HFs direkt vor der Installation in den Ordner`\Hotfixes` dem ISO hinzugefügt werden.

3.4.1 OpenScape 4000 Installation auf VMware ESXi

Openscape 4000 Manager ist eine der Openscape 4000 Implementierungen und die Installation ist ähnlich wie bei jeder Openscape 4000 Implementierung.

Einzelheiten zur ovf-Bereitstellung und Installation auf VMWare finden Sie in Kapitel 3.1 des OpenScape 4000, Installation, Konfiguration und Migration, Installationshandbuch.

3.4.2 OpenScape 4000-Installation auf Microsoft Hyper-V

Openscape 4000 Manager ist eine der Openscape 4000 Implementierungen und die Installation ist ähnlich wie bei jeder Openscape 4000 Implementierung.

Details zur Erstellung einer Virtuellen Maschine und zur Installation auf Hyper-V finden Sie in Kapitel 3.2 des OpenScape 4000, Installation, Konfiguration und Migration, Installationshandbuch.

3.4.3 OpenScape 4000-Installation auf KVM

Openscape 4000 Manager ist eine der Openscape 4000 Implementierungen und die Installation ist ähnlich wie bei jeder Openscape 4000 Implementierung.

Details zur Erstellung einer Virtuellen Maschine und zur Installation auf KVM finden Sie in Kapitel 3.3 des OpenScape 4000, Installation, Konfiguration und Migration, Installationshandbuch.

3.4.3.1 OpenScape 4000-Installation auf Proxmox VE

Openscape 4000 Manager ist eine der Openscape 4000 Implementierungen und die Installation ist ähnlich wie bei jeder Openscape 4000 Implementierung.

Details zur Erstellung einer Virtuellen Maschine und zur Installation auf KVM finden Sie in Kapitel 3.3 des OpenScape 4000, Installation, Konfiguration und Migration, Installationshandbuch.

3.5 Kompatibilität von OpenScape/HiPath 4000-Systemen

Dieser Abschnitt beschreibt die OpenScape/HiPath 4000-Systeme, die vom OpenScape 4000 Manager V10 unterstützt werden.

3.5.1 Unterstützte OpenScape/HiPath 4000-Anlagen

Der OpenScape 4000 Manager V10R0 unterstützt die folgenden OpenScape/HiPath 4000-Anlagen:

- OpenScape 4000 V10
- OpenScape 4000 V8
- OpenScape 4000 V7
- HiPath 4000 V6
- HiPath 4000 V5
- HiPath 4000 V4
- HiPath 4000 V3.0, V3.1
- HiPath 4000 V2.0
- HiPath 4300
- HiPath 4500

Der OpenScape 4000 Manager V10R1 unterstützt die folgenden OpenScape/HiPath 4000-Anlagen:

- OpenScape 4000 V10
- OpenScape 4000 V8
- OpenScape 4000 V7
- HiPath 4000 V6

Anmerkung: Für die Administration von OpenScape/HiPath 4000-Netzwerken mittels OpenScape 4000 Manager muss auf dem OpenScape 4000 Manager ein Release verwendet werden,

das dem höchsten Release auf den Assistants beim Kunden entspricht bzw. höher als dieses ist.

Anmerkung: Bei gemischten Bereitstellungen (OpenScape/HiPath 4000 und CMP/UC) müssen alle Upgrades in der vorgegebenen Reihenfolge durchgeführt werden: zuerst UC und dann OpenScape/HiPath 4000. Wenn die Aktualisierung in umgekehrter Reihenfolge erfolgt (erst OpenScape/HiPath 4000 und dann UC), gibt es zwischen dem OpenScape/HiPath 4000-Upgrade und dem UC-Upgrade eine Phase, in der die Kommunikation zwischen den beiden Produkten unterbrochen ist!

3.5.2 Aktuelle UPLO2-Versionen für ältere HiPath 4000-Varianten

Verwenden Sie bitte die aktuellsten Releases von HiPath 4000-Varianten.

3.6 Anschluss an OpenScape 4000

OpenScape/HiPath 4000-Anlagen können nur über LAN an den OpenScape 4000 Manager angeschlossen werden.

3.6.1 Port-Tabellen

Die aktuellen Port-Tabellen für OpenScape 4000 Manager und Assistant sind in der Interface Management Datenbank (IFMDB) enthalten. Diese finden Sie hier:

im Unify-Partnerportal (https://unify.com/en/partners/partner-portal)

im Intranet unter folgender URL: https://apps.g-dms.com:9090/ifm/php/php_ifmdb/login.php

3.7 Überprüfen des erfolgreichen Starts von Prozessen und Komponenten

Während der Hochlaufphase des OpenScape 4000 Managers (Boot-Vorgang) werden automatisch eine ganze Reihe von abhängigen und unabhängigen Prozessen gestartet. Treten beim Start dieser Prozesse Probleme auf, kann der OpenScape 4000 Manager möglicherweise keine Verbindung zu den verwalteten Anlagen herstellen. Prüfen Sie nach dem Hochfahren des OpenScape 4000 Manager-Servers wie folgt, ob alle Prozesse erfolgreich gestartet wurden:

1) Rufen Sie die Webmin-Seite mit den **Anwendungsprozessen** auf.

   Auf dieser Seite sehen Sie den aktuellen Status der meisten Anwendungsprozesse

   Siehe Bild 42.

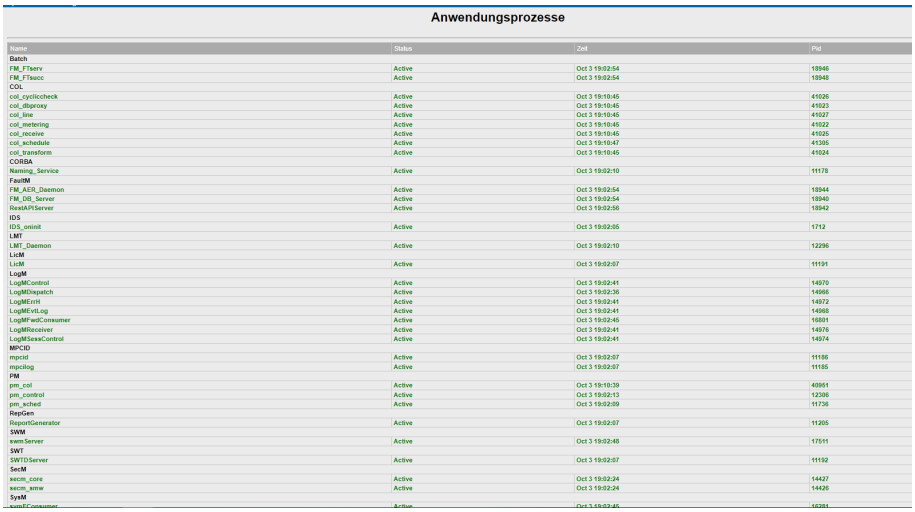


Abbildung 20: Webmin-Prozessliste

2) Wenn sich Prozesse im Zustand Nicht aktiv befinden, sollten Sie sich an die nächsthöhere Support-Ebene wenden.

3.8 CHD-Links-Update für Manager V10R1

Bei einem Upgrade von V6, V7, V8 auf V10 ist es NICHT erforderlich, die in diesem Kapitel beschriebenen Schritte durchzuführen. Bei einem Upgrade auf OpenScape 4000 Manager V10R1 müssen alle CPTP-Einträge auf bereits vorhandenen OpenScape 4000-Systemen angepasst werden. Andernfalls funktionieren die Funktionen zur Dateiübertragung, Alarm- und Fehlermeldung am OpenScape 4000 Manager V10R1 nicht.

Mit einem Upgrade auf OpenScape 4000 Manager V10R1 wurde der HLB-Modus abgeschafft und alle Switches müssen in den HLO-Modus migriert werden. Dies geschieht automatisch in der CM-Datenbank während der HBR-Wiederherstellung der früheren Managerdaten. Die CPTP-Einträge auf bereits vorhandenen OpenScape 4000-Systemen müssen ebenfalls mit Hilfe der unten stehenden Anleitung angepasst werden.

3.9 Vorbereiten des OpenScape 4000 Manager-Client

Um den vollen Leistungsumfang des OpenScape 4000 Managers nutzen zu können, müssen Sie zunächst die erforderliche Software-Umgebung für den Client-PC schaffen.

3.9.1 Client-Vorbereitung über die öffentlich zugängliche Seite des OpenScape 4000 Manager-Servers

Wenn Sie sich schrittweise durch den gesamten Installationsvorgang führen lassen wollen (geführte Tour), gehen Sie folgendermaßen vor:

1) Öffnen Sie einen Browser und führen Sie eine der folgenden Aktionen aus:
   a) Geben Sie die neu zugewiesene LAN-Adresse ein:
   `https://<address>/common/cltprep/install/`

   oder
   b) Navigieren Sie zum Abschnitt **Dienstprogramme** von OpenScape 4000 Manager und wählen Sie die **Client-Vorbereitung**.
2) Folgen Sie den Anweisungen auf dem Bildschirm (empfohlen für neue Benutzer), um mit der Installation zu beginnen.

3.9.2 Verbindung zum OpenScape 4000 Manager

3.9.2.1 Verbinden über SSH / SFTP

Der SSH/SFTP-Dienst wird von Linux OS bereitgestellt und kann verwendet werden für

- Zugang zum Dienst,
- Zugang zur XIE-Dateischnittstelle

Anmerkung: Nur der Zugriff auf den Manager-Linux-Container ist erlaubt, nicht aber auf das Betriebssystem der Plattform.

Nur Benutzer mit dem Sicherheitsprofil engr, rsta oder rsca oder Benutzer, denen das Zugriffsrecht „Zugriffsverwaltung - Linux-Dateisystem“ zugewiesen wurde, können über SSH oder SFTP auf Manager zugreifen.

Weitere Informationen finden Sie unter Abschnitt 4.6, „Benutzerverwaltung - Erstellen von Benutzernamen und Zuweisen von Anwendungen“.

3.9.3 Generieren und Aktivieren eines individuellen Zertifikats

Ohne individuelles Zertifikat kann Ihr Browser Meldungen anzeigen, dass das Zertifikat ungültig ist, und eine Sicherheitswarnung ausgeben. Daher sollte das vorinstallierte SSL-Zertifikat durch ein individuelles Zertifikat ersetzt werden.

Wenn Sie ein individuelles Zertifikat generieren und aktivieren möchten, müssen Sie eine der folgenden drei Optionen wählen:

- selbstsigniertes Zertifikat (weiter mit Abschnitt 3.9.3.1, "Selbstsigniertes Zertifikat") oder
- importiertes, durch eine CA signiertes Zertifikat (weiter mit Abschnitt 3.9.3.2, "Importiertes, von einer CA signiertes Zertifikat") oder

- von einer offiziellen CA signiertes und über CSR generiertes Zertifikat (weiter mit Abschnitt 3.9.3.3, "Von einer offiziellen CA signiertes und über CSR generiertes Zertifikat").

3.9.3.1 Selbstsigniertes Zertifikat

Schritt A: Zertifikat generieren

1) Wechseln Sie auf der **Startseite** von **OpenScape 4000 Manager** zu **Access Management –> Manage Web Server Certificates –> Certificates for this Web Server**.
2) Klicken Sie auf **Generate**.
3) Geben Sie die erforderlichen Daten im Dialog **Generate Server Certificate (self signed)** ein, und klicken Sie auf **Continue**.
4) Überprüfen Sie die Daten im Dialog **Display Certificate**. Klicken Sie auf **Continue**.
5) Das Programm wechselt zum Dialog **Activate Server Certificate**.

Schritt B: Generiertes Zertifikat aktivieren

1) Wählen Sie das generierte Zertifikat in der Liste **Overview of all certificates that can be activated** aus.
2) Klicken Sie auf **Activate selected certificate**.
3) Falls erforderlich, geben Sie ein Passwort für den privaten Schlüssel ein, und klicken Sie auf **Activate Certificate**.
4) Klicken Sie im eingeblendeten Meldungsfenster auf **OK**, und befolgen Sie die Anweisungen auf dem Bildschirm.

3.9.3.2 Importiertes, von einer CA signiertes Zertifikat

Anmerkung: Das Zertifikat der signierenden CA muss in den Speicher vertrauenswürdiger Stamm-CAs des Webbrowsers importiert werden, da dies nicht bei der Vorbereitung des OpenScape 4000 Manager-Clients geschieht.

Schritt A: Zertifikat importieren

1) Wechseln Sie auf der **Startseite** von **OpenScape 4000 Manager** zu **Access Management –> Manage Web Server Certificates –> Certificates for this Web Server**.
2) Klicken Sie auf **Import**.
3) Geben Sie den entsprechenden Dateinamen ein.
4) Geben Sie ein Passwort für den privaten Schlüssel ein.
5) Klicken Sie auf **Import Certificate**.
6) Das Programm wechselt zum Dialog **Activate Server Certificate**.

Schritt B: Importiertes Zertifikat aktivieren

1) Wählen Sie das importierte Zertifikat in der Liste **Overview of all certificates that can be activated** aus.
2) Klicken Sie auf **Activate selected certificate**.

3) Falls erforderlich, geben Sie ein Passwort für den privaten Schlüssel ein, und klicken Sie auf **Activate Certificate**.
4) Klicken Sie im eingeblendeten Meldungsfenster auf **OK**, und befolgen Sie die Anweisungen auf dem Bildschirm.

3.9.3.3 Von einer offiziellen CA signiertes und über CSR generiertes Zertifikat

Schritt A: Zertifikat generieren

1) Wechseln Sie auf der **Startseite** von **OpenScape 4000 Manager** zu **Access Management –> Manage Web Server Certificates –> Certificates for this Web Server**.
2) Klicken Sie auf **Generate via CSR**.
3) Klicken Sie auf die Schaltfläche **Generate New Certificate Request**.
4) Geben Sie alle erforderlichen Daten im Dialog **Generate Certificate via CSR** ein, und klicken Sie dann auf **Continue**.
5) Überprüfen Sie die Daten im Dialog **Display Certificate**. Klicken Sie auf **Continue**.

Schritt B: Generiertes selbstsigniertes Zertifikat testen

1) Klicken Sie auf das Symbol **Test** in der Spalte **Action** der im Dialog **Generate Certificate via CSR** angezeigten Tabelle.
2) Aktivieren Sie das generierte Zertifikat im Dialog **Activate Server Certificate**.

Schritt C: Zertifikat exportieren

1) Öffnen Sie den Dialog **Generate Certificate via CSR**.
2) Klicken Sie auf das Symbol **Export** in der Spalte **Action**.
3) Kopieren Sie das CSR per Kopieren und Einfügen, oder exportieren Sie es in eine Datei.

Schritt D: Exportiertes CSR zwecks Signierung an Ihre Zertifizierungsstelle senden

Schritt E: Signiertes Zertifikat importieren

1) Öffnen Sie den Dialog **Generate Certificate via CSR**.
2) Klicken Sie auf das Symbol **Import** in der Spalte **Action**.
3) Kopieren Sie den Inhalt des signierten Zertifikats per Kopieren und Einfügen, oder importieren Sie das signierte Zertifikat aus einer Datei.
4) Geben Sie ein Passwort für den privaten Schlüssel ein, und klicken Sie auf **Continue**.

Schritt F: Signiertes Zertifikat aktivieren

1) Öffnen Sie den Dialog **Generate Certificate via CSR**.
2) Klicken Sie auf das Symbol **Activate** in der Spalte **Action**.
3) Sobald Sie auf das Symbol **Activate** klicken, wird der Webserver automatisch neu gestartet.

3.10 Überprüfen der Lizenzen

Die Zuweisung der Lizenzen erfolgt im Rahmen der Staging-Phase. Vergewissern Sie sich wie folgt, dass die Lizenzierungsmaßnahme ordnungsgemäß durchgeführt wurde:

1) Wählen Sie im OpenScape 4000 Manager Launchpad die Position Zugangsverwaltung und aktivieren Sie die Applikation Lizenzverwaltung durch Anklicken der entsprechenden Menüposition (siehe Bild 47).

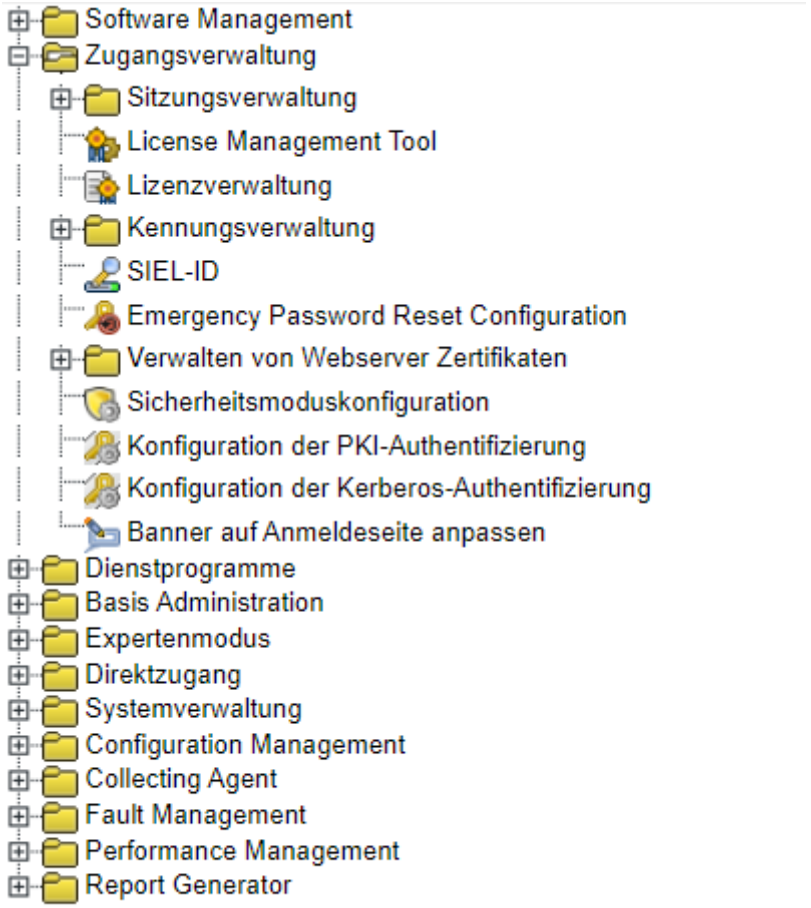


Abbildung 21: Lizenzverwaltung für Überprüfung der Server-Lizenzen aufrufen

2) Führen Sie auf der Startseite Lizenzverwaltung die folgenden Schritte aus (siehe Bild 48)

=> Klicken Sie auf Installierte Lizenzdaten anzeigen, um die im Rahmen der Staging-Phase installierten Lizenzen einzusehen.

=> Klicken Sie auf **CLA IP-Adresse/DNS Name anzeigen**, um die Adresse des konfigurierten Customer License Agent anzuzeigen.

Abbildung 22: Startseite "Lizenzverwaltung"

Anmerkung: Ist noch keine Lizenzierung erfolgt, sollten Sie Abschnitt 5.8, "Lizenzen des OpenScape 4000 Manager-Servers verwalten" lesen. Sie finden hier ausführliche Anleitungen zur Installation der Lizenzdaten.

3.11 Konfigurieren eines externen Backup-Servers

Um OpenScape 4000 Manager Backup-Sets remote speichern zu können, muss ein kompatibler SFTP- oder NFS-Server im Kunden-LAN installiert werden. Das FTP-Übertragungsprotokoll wird von der Funktion Backup/Restore im OpenScape Manager und im Assistant V8 nicht unterstützt, da es unsicher ist. Nur SFTP wird unterstützt.

Auf die Konfiguration des SFTP-Servers wird in diesem Handbuch nicht näher eingegangen. Beachten Sie hierzu bitte die Anweisungen im Handbuch des jeweiligen SFTP-Server-Herstellers.

OpenScape 4000 Manager und Assistant nutzen das SFTP-Client-Modul. Entsprechende Tests haben ergeben, dass dieses Modul zum SSH File Transfer Protocol (SFTP) Version 3 der IETF kompatibel ist. Demzufolge können alle SFTP-Server, die diese Protokollversion unterstützen, als SFTP-Backup-Server eingesetzt werden. Wir bitten um Ihr Verständnis, dass wir bei

direkten Problemen mit der SFTP-Server-Software oder bei Nichteinhaltung der SFTP-Protokoll-Definition keinen Support leisten können.

Folgende SFTP-Server wurden erfolgreich mit Backup & Restore getestet:

- Linux:
  - OpenSSH
- Windows:
  - OpenSSH basierend auf cygwin
  - SilverSHielD SSH/SFTP-Server
  - FreeFTPd-basierter SFTP-Server

Anmerkung: Bitte beachten Sie, dass wir keinen Support bieten für Probleme, die durch die SFTP-Server-Software selbst verursacht werden.

---

4 Einrichten von Systemen und Benutzern mit OpenScape 4000 Manager

Dieses Kapitel enthält Anweisungen zur Einrichtung der Software OpenScape 4000 Manager-Systemverwaltung.

4.1 Systemverwaltung – Überblick

Die Systemverwaltung (System Management) ist eine Applikation für die Verwaltung von Netzwerk-Objekten im OpenScape 4000 Manager. Anders ausgedrückt: Der OpenScape 4000 Manager kann als Netzelement-Manager für OpenScape/HiPath 4000-Kommunikationsserver betrachtet werden. Daher liegt der Schwerpunkt der Systemverwaltung auf der Administration von Anlagen des Typs OpenScape/HiPath 4000. SNS-Produkte (System and Network Solutions) werden nicht mehr unterstützt. Dennoch unterstützt die Systemverwaltung eine vordefinierte Gruppe von Netzwerk-Objekt-Typen einschließlich OpenScape/HiPath 4000 und Netzwerk-Management-Server.

Die Systemverwaltung ist Eigentümer von allgemeinen Systemdaten sowie von Kommunikationsparametern. Applikationsspezifische Daten (beispielsweise Performance Management, Collecting Agent oder Zugangsverwaltung) werden zwar in der Systemverwaltung angezeigt, die Verwaltung dieser Daten erfolgt jedoch in der jeweiligen Applikation selbst.

Alle Netzwerk-Objekte, die vom OpenScape 4000 Manager verwaltet werden sollen, müssen zunächst in der Systemverwaltung eingerichtet werden. Die Benutzeroberfläche der Systemverwaltung verfügt über Funktionen zum Hinzufügen, Modifizieren und Löschen von Netzwerk-Objekten.

Die Systemverwaltung kann über das Launchpad (Applikationsbaum oder Menüleiste) gestartet werden. Nach erfolgreichem Aufruf der Systemverwaltung (siehe Bild 49) erscheint für jede verwaltete Anlage ein Datensatz.

Applikationsbaum der Systemverwaltung

4.2 Systemverwaltung – Hinzufügen von OpenScape/HiPath 4000-Anlagen

Anmerkung: Zusätzliche Informationen zu den Fenstern und Feldern der Systemverwaltung sowie weitere Anweisungen zur Erzeugung des in diesem Abschnitt beschriebenen Objekts finden Sie in den Mouseover-Texten und in der Online-Hilfe.

Führen Sie die nachfolgend beschriebenen Schritte aus, um eine neue OpenScape/HiPath 4000-Anlage im OpenScape 4000 Manager-Server hinzuzufügen:

1) Rufen Sie das OpenScape 4000 Manager Launchpad auf und klicken Sie hier auf Systemverwaltung.
2) Klicken Sie auf OpenScape 4000 Administration (siehe Bild 50).

Abbildung 23: OpenScape/HiPath 4000-Anlage in der Systemverwaltung einrichten

3) Öffnen Sie im Fenster OpenScape 4000 Administration das Menü Objekt und wählen Sie die Option Neu (siehe Bild 51).

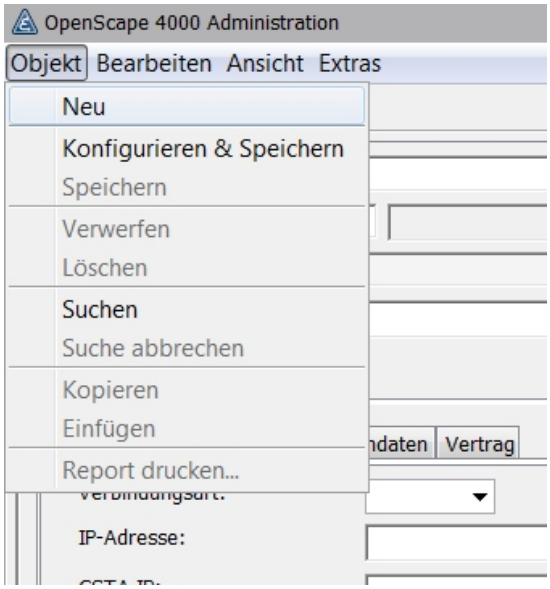


Abbildung 24: Das Menü Objekt>im Fenster OpenScape 4000 Administration

4) Klicken Sie auf den Eintrag Neu im Menu Objekt oder in die untere rechte Ecke des Dialogs "Systemverwaltung", um das Fenster Neues Objekt zu öffnen. Wenn die Daten eines vorhandenen Netzwerk-Objekts bereits vor dem Öffnen des Fensters Neues Objekt angezeigt wurden, wird der Inhalt von bestimmten Feldern nicht gelöscht, sondern wird vom zuvor angezeigten Objekt übernommen, um die Erstellung des nächsten/neuen Objekts zu erleichtern.

   Die folgenden Felder werden nicht gelöscht und enthalten nach wie vor die Daten eines zuvor angezeigten Objekts:

   - Version
   - Typ (HLO / HLB)
   - Kundenname (auf der Registerkarte Kundendaten)
   - Verbindungsart (Registerkarte Verbindung)
   - Domain (Registerkarte Systemdaten)
   - Knotennummer (Registerkarte Systemdaten)

   Unter der gleichnamigen Schaltfläche gibt es eine Funktion namens Daten abrufen mit der alle möglichen OpenScape 4000-Informationen (Assistant, ADP, ...) von der angegebenen Assistant-Adresse abrufbar sind.

5) Bitte geben Sie die IP-Adresse ein und klicken Sie auf die Schaltfläche Daten abrufen. Für den automatischen Datenabruf per Assistant wird das Standard-Assistant-Konto nsl-engr verwendet; dieses sollte daher zwischen dem Manager und dem Assistant synchron gehalten werden. Sie haben aber dennoch die Möglichkeit, die Assistant-Anmeldeinformationen manuell eingeben, wenn der automatische Verbindungsaufbau fehlschlägt.

6) Die folgenden Felder werden abgerufen, sofern verfügbar: Manager-IP-Adresse im CPTP, AFR-Nummer, Version, Systemnummer, Access Point System (ebenfalls mit der APE-Nummer), AMO-Sprache, Domain,

Knotennummer, Zeitzone (funktioniert nur mit neuestem Hotfix für Assistant V7R0 und neuere Releases), Vertragsnummer.

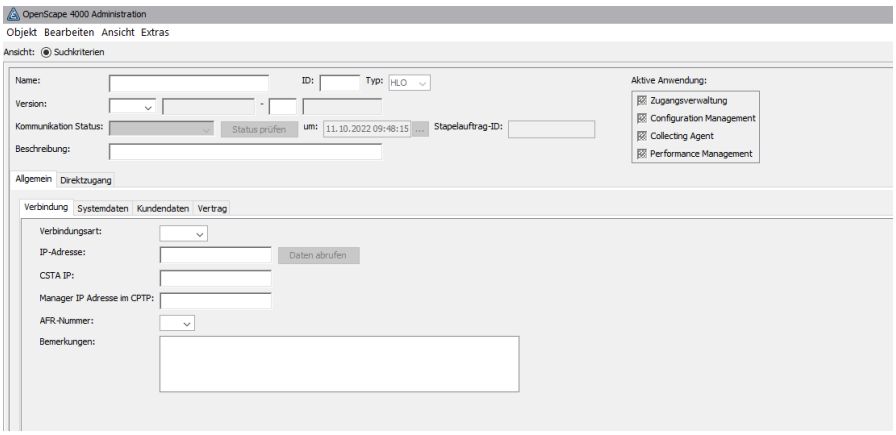
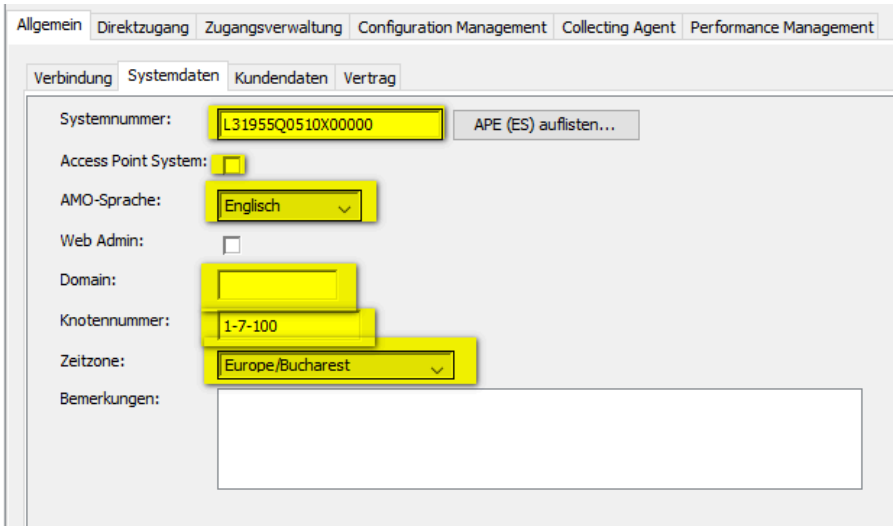
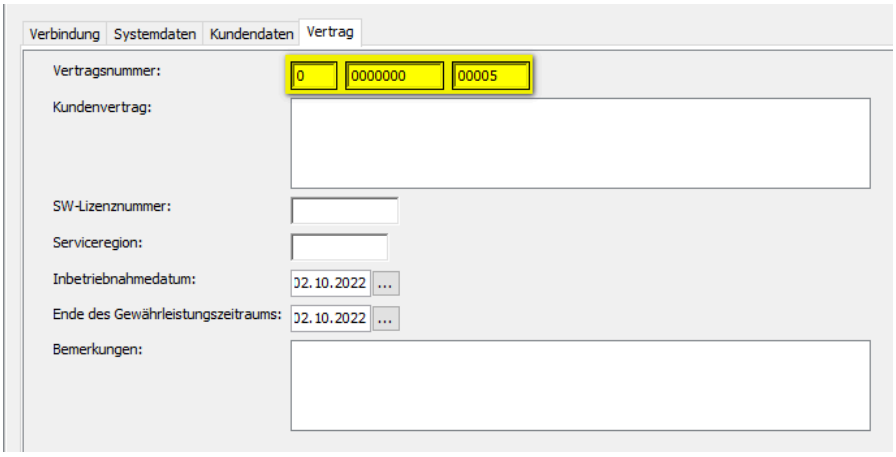


Abbildung 25: Neues Objekt – Registerkarten Verbindung, Systemdaten und Vertrag





7) Füllen Sie in die fehlenden Pflichtfelder aus – in der Regel Kundenname und Name. Entscheiden Sie, welche Verbindungsart Sie verwenden möchten – HLO / HLB (siehe auch Tabelle 3). Die Manager-IP-Adresse im CPTP ist schreibgeschützt und die Angabe der AFR-Nummer ist nur dann obligatorisch, wenn Sie die Anlage Konfigurieren & Speichern möchten.

Wenn Sie Nur speichern möchten, ist die Option nicht obligatorisch (weitere Informationen, siehe unten).

8) Markieren Sie alle übrigen Aktiven Anwendungen, die für diese Anlage relevant sind. Beachten Sie, dass auf dem Bildschirm für jede gewählte Applikation eine weitere Registerkarte erscheint.

Tabelle 1: Hardware-Typen für OpenScape/HiPath 4000

Hardware-Typ	Beschreibung	Version
HLO	Online-Verbindung zur OpenScape/HiPath 4000-Anlage (FAMOS-Verbindung im Dialogmodus, AMO senden, Auf Antwort warten); Standard-Verbindungstyp	UV1.0, UV4, U UV8, R RGV7
HLB	OpenScape/HiPath 4000 mit Atlantic LAN und UNIX; jedoch ohne Unix-Nutzung durch DMS; Rückfall-Lösung, wenn keine andere Verbindung funktioniert	UV1.0, UV4, U UV8
VMSR	VoiceMail-Server (ohne UNIX); nur für Nutzung durch CM	
VMSU	VoiceMail-Server (mit UNIX); nur für Nutzung durch CM	

9) Geben Sie im Register Allgemein die Systemdaten wie folgt ein:

a) Geben Sie die Systemnummer ein, falls diese nicht automatisch abgerufen/ausgefüllt wurde.

Anmerkung: Die Anlagennummer wird in dem AMO ANSU auf der OpenScape 4000-Kommunikationsplattform gespeichert. Obwohl es sich hierbei um ein obligatorisches Feld handelt, validiert der OpenScape 4000 Manager-Server die OpenScape/HiPath 4000-Anlagennummer nicht.

---

b) Vergewissern Sie sich, dass die AMO-Sprache auf den korrekten Wert gesetzt ist (Deutsch oder Englisch).

c) Geben Sie die Domain ein, in die die neue OpenScape/HiPath 4000-Anlage eingefügt wird. Wenn dies die erste OpenScape/HiPath 4000-Anlage ist, die in der Systemverwaltung konfiguriert wird, ist möglicherweise noch keine Domain eingerichtet worden. Anweisungen zur Einrichtung einer neuen Domain enthält Abschnitt 4.5.1.3, "Neue Domain im OpenScape 4000 Manager einrichten".

d) Wählen Sie in der Dropdown-Liste Zeitzone einstellen eine Zeitzone, die dem Standort des Systems entspricht. Dies ist erforderlich, um eventuelle Zeitzonendifferenzen zwischen dem OpenScape 4000 Manager und den zu verwaltenden Systemen auszugleichen.

Anmerkung: Weitere Information zur Datum/Uhrzeit-Einstellung mit Hilfe des OpenScape 4000 Managers finden Sie in der Online-Hilfe "OpenScape 4000 Management, Webmin Base Administration".

---

10) Klicken Sie auf das Unterregister Kundendaten (siehe Bild 53).

Geben Sie hier den Kundennamen (obligatorisch) und andere optionale Informationen ein, die Sie vom Kunden erhalten haben.

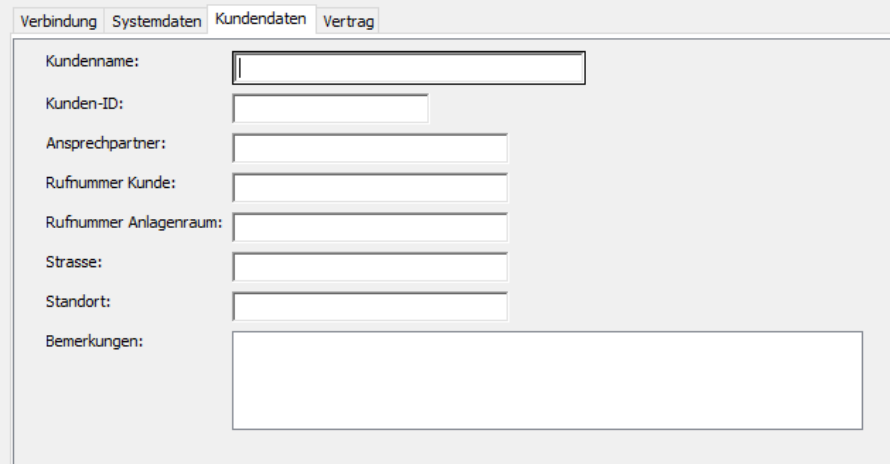


Abbildung 26: Das Unterregister "Kundendaten"

11) Klicken Sie auf das Unterregister Vertrag (siehe Bild 54).

Geben Sie die Vertragsnummer ein, falls diese nicht automatisch abgerufen/ausgefüllt wurde. Dies ist ein obligatorisches Feld. Die Vertragsnummer sollte über den AMO FBTID in der entsprechenden OpenScape/HiPath 4000-Anlage automatisch bereitgestellt werden (siehe Bild 55). Wenn der Wert im Feld "Vertragsnummer>nicht mit den FBTID-

Daten übereinstimmt, läuft Fault Management möglicherweise nicht. Die übrigen Daten für das Unterregister "Vertrag>kann der Kunde liefern.

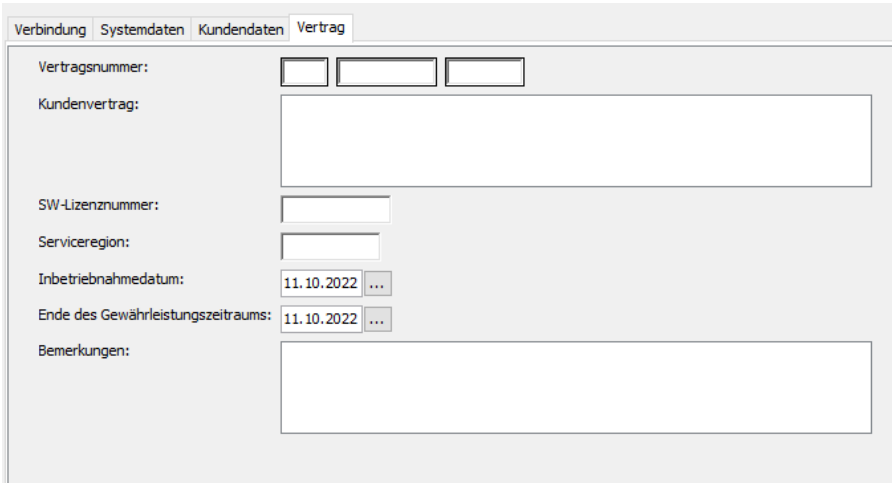


Abbildung 27: Das Unterregister "Vertrag"

```
ABFR-FBTID;
H500:  AMO FBTID GESTARTET
   PARAMETER FUER DEN VERBINDUNGSAUFBAU
    ZWISCHEN SYSTEM UND SERVICEZENTRUM
PARAMETER                    WERT
---------------------        ----------------------
ZN-KENNUNG                 : 12
VERTRAGSNUMMER             : 1234123
POSITIONSNR. DES VERTRAGES : 44321
PASSWORD                   : IDENTIFIKATION
PRODUKTBEZEICHNUNG         :
NAME DES KUNDEN            :
TELEFONNUMMER DER ANLAGE   :

AMO-FBTID-111      LISTE DER VARIABLEN DATEN FUER DEN VERBINDUNGSAUFBAU
ABFRAGEN DURCHGEFUEHRT;
```

Abbildung 28: Der AMO FBTID

12) Klicken Sie auf das Unterregister Verbindung (siehe Bild 56).

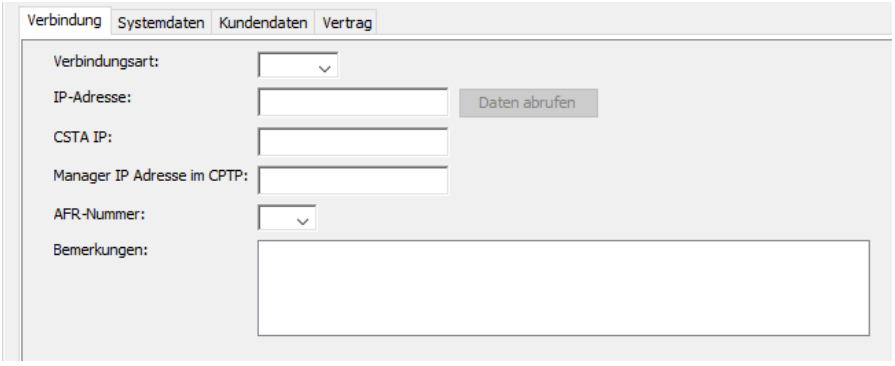


Abbildung 29: Das Unterregister "Kommunikation"

13) Als Verbindungsart unterstützt Manager lediglich LAN.

14) Bitte entscheiden Sie, ob Sie die Verbindung zur Anlage konfigurieren & testen möchten. Wenn ja, klicken Sie auf Konfigurieren & Speichern, andernfalls Sie auf Nur speichern.

15) Wenn Konfigurieren & Speichern angeklickt und als Verbindungsart HLB ausgewählt wurde, werden die folgenden Schritte ausgeführt:

- **a)** die GUI-Daten werden in der DB (chdmain) gespeichert;
- **b)** die Angabe der AFR-Nummer ist obligatorisch und muss ausgewählt werden;
- **c)** /opt/chd/chd_util.sh –m <mnemonisch> wird aufgerufen, um die TNS-Einträge der Datenbank zu aktualisieren;
- **d)** /opt/chd/addcptp wird aufgerufen, um die entsprechenden CPTP-, AFR- und FTCSM-Einträge auf der Anlage zu konfigurieren;
- **e)** /opt/chd/hlbtest.sh wird aufgerufen, um die Stapelaufträge zu testen und den Verbindungsstatus zu überprüfen;
- **f)** das Feld Verbindungsstatus wird anhand des Testergebnis geändert – der Status wird auf den neuen Statuswert Stapelauftrag fehlgeschlagen>gesetzt;
- **g)** der neue Verbindungsstatus wird in der DB-Tabelle "chdmain" im Feld "hicom_status>aktualisiert.

16) Wenn Konfigurieren & Speichern angeklickt und als Verbindungsart HLO ausgewählt wurde, werden die folgenden Schritte ausgeführt:

- **a)** die oben genannten Schritte a) bis d) werden ausgeführt;
- **b)** eine Verbindung zum RMX und zum Assistant wird aufgebaut, um den Verbindungsstatus zu testen;
- **c)** das Feld Verbindungsstatus wird anhand des Testergebnis geändert – der Status wird auf den neuen Statuswert "IP-Verbindung fehlgeschlagen>gesetzt;
- **d)** der neue Verbindungsstatus wird in der Tabelle "chdmain" im Feld "hicom_status>aktualisiert.

17) Wiederholen Sie die zuvor beschriebenen Schritte, um weitere vom OpenScape 4000 Manager-Server verwaltete OpenScape 4000 IP-Kommunikationsplattformen einzurichten.

4.3 Systemverwaltung – OpenScape 4000 Manager Administration

In OpenScape 4000 Manager Administration (siehe Bild 57) können Sie das Standardelement konfigurieren, das bei der Installation des Servers automatisch erzeugt wird. Das Standardelement steht für den OpenScape 4000 Manager-Server selbst. Es ist nicht möglich, dieses Element zu löschen oder weitere Elemente dieses Typs hinzuzufügen.

Bei dem für diesen OpenScape 4000 Manager konfigurierten Namen handelt es sich um den Namen, der in der Titelzeile jeder Web-Applikation erscheint, d. h., um das erste Wort, das sichtbar ist, wenn Sie den OpenScape 4000 Manager in Ihrem Browser über ein Lesezeichen aufrufen.

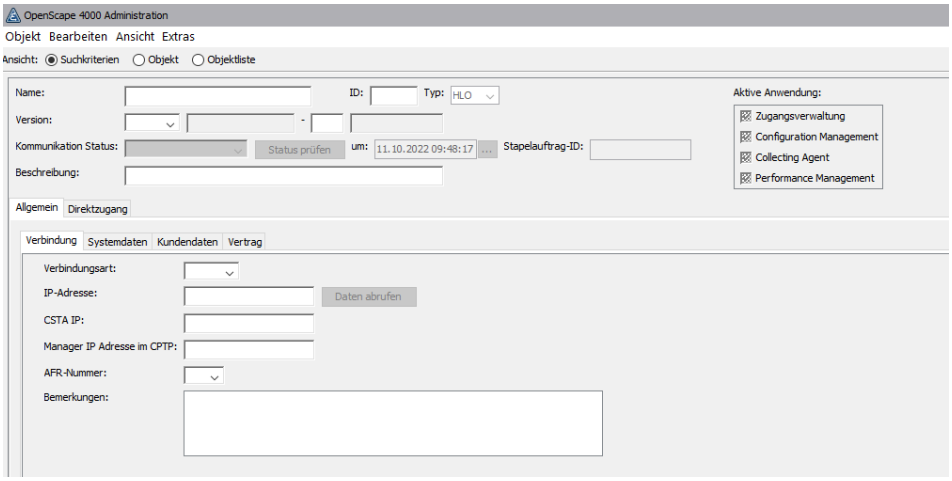


Abbildung 30: OpenScape 4000 Manager-Administration

4.4 Aufgaben in Configuration Management

Nachdem alle Anlagen in der Systemverwaltung eingerichtet worden sind, müssen Sie in Configuration Management die folgenden Maßnahmen durchführen:

- Ein Upload für jede OpenScape/HiPath 4000-Anlage durchführen (siehe Section 4.5.3)

4.4.1 CM – Domain-Verwaltung in OpenScape 4000 Manager

Dieser Abschnitt enthält grundlegende Informationen zu Domains sowie zu deren Einrichtung und Verwaltung in der OpenScape 4000 Manager-Umgebung.

4.4.1.1 Allgemeine Informationen zu Domains

Der Begriff Domain bezeichnet eine einzelne OpenScape/HiPath 4000-Anlage oder eine Gruppe vernetzter OpenScape/HiPath 4000-Anlagen mit eindeutigen oder geschlossenen Wählplänen.

- In einem eindeutigen oder geschlossenen Wählplan ist keine Teilnehmer-Rufnummer doppelt vorhanden.
- Ein offener Wählplan kann doppelte Teilnehmer-Rufnummern enthalten.
- Für Domain Typ 1 werden beim Löschen eines Teilnehmers AMO WABE-Befehle zur Aktualisierung der Routeinformation nicht an alle Anlagen im Domain gesendet. Ein AMO-Befehl zum Löschen des Teilnehmers wird nur an die Anlage gesendet, an der der Teilnehmer angeschlossen ist.
- Für Domain Typ 2 werden beim Löschen eines Teilnehmers AMO WABE-Befehle zur Aktualisierung der Routeinformation an alle Anlagen im Domain gesendet.

Einzelne OpenScape/HiPath 4000-Anlage

Wenn eine OpenScape/HiPath 4000-Anlage nicht über CorNet mit einer anderen OpenScape/HiPath 4000-Anlage vernetzt ist, gehört sie einer Domain an, die nur diese eine OpenScape/HiPath 4000 enthält. Innerhalb einer einzelnen OpenScape/HiPath 4000-Anlage dürfen Teilnehmer-Rufnummern nicht mehrfach vorkommen, d. h. alle Rufnummern sind eindeutig.

Vernetzte OpenScape/HiPath 4000-Anlagen

Wenn OpenScape/HiPath 4000-Anlagen über CorNet miteinander vernetzt sind, können alle vernetzten OpenScape/HiPath 4000-Anlagen derselben Domain angehören, sofern sämtliche teilnehmerspezifischen Rufnummern eindeutig sind. Es ist nicht immer möglich, netzweit eindeutige Rufnummern beizubehalten. Der "erweiterte private Netzplan>(Enhanced Privat Network Plan, EPNP) bietet die Möglichkeit, Standortcodes mit den Teilnehmer-Rufnummern zu kombinieren und so bis zu zwölfstellige vollständige Nummern zu bilden. Innerhalb eines OpenScape/HiPath 4000-Netzwerks mit einem offenen Wählplan kann dieser Plan geschlossen werden, wenn in jeder OpenScape/HiPath 4000-Anlage ein eindeutiger EPNP-Standortcode ordnungsgemäß konfiguriert ist. Gemeinsam bilden die eindeutigen EPNP-Standortcodes und die Teilnehmer-Rufnummern dann eindeutige vollständige Rufnummern. Sind alle vollständigen Rufnummern innerhalb des OpenScape/HiPath 4000-Netzwerks eindeutig, ist der Wählplan geschlossen. In diesem Szenario können alle vernetzten OpenScape/HiPath 4000-Anlagen einer einzelnen Domain angehören.

OpenScape 4000 Manager stellt Funktionen für die Verwaltung von Domains zur Verfügung. In OpenScape 4000 Manager müssen alle verwalteten Anlagen in einem Netzwerk – beispielsweise OpenScape/HiPath 4000-Anlagen – einer Domain zugewiesen werden. Ist der Wählplan des Netzwerks geschlossen, können alle verwalteten Systeme innerhalb dieses Netzwerks ein und derselben Domain angehören. Wenn der Wählplan jedoch offen ist, müssen diese Systeme mehreren Domains zugewiesen werden.

4.4.1.2 WABE-Konfiguration

Wenn Anlagen in ein und derselben Domain eingerichtet sind, werden die AMO WABE-Befehle zur Aktualisierung der Route-Informationen beim Löschen eines Teilnehmers an alle Anlagen in der Domain gesendet.

In einer Konfiguration mit VNR-Unteranlagen von mehreren physischen Anlagen müssen die AMO WABE-Informationen an alle Anlagen übergeben werden, die sich in einer Domain befinden; diese VNR-Unteranlagen sollten in einer Domain eingerichtet werden und sollten dieselbe virtuelle Knoten-ID haben.

Die Zuordnung von großen WABE-Bereichen ist ineffizient, verlangsamt die Ausführung des Assistant CM und führt zu längeren Upload-Zeiten beim Manager. Bitte vermeiden Sie unnötige AMO WABE-Konfigurationen. Tests haben gezeigt, dass bei mehr als 50.000 WABE-Einträgen eine Häufung der erwähnten Probleme auftritt.

4.4.1.3 Neue Domain im OpenScape 4000 Manager einrichten

Gehen Sie wie folgt vor, um im OpenScape 4000 Manager-Server eine neue Domain einzurichten:

1) Klicken Sie im OpenScape 4000 Manager-Launchpad auf Configuration Management.
2) Klicken Sie im Netzwerk-Ordner auf Domain (siehe Bild 58).

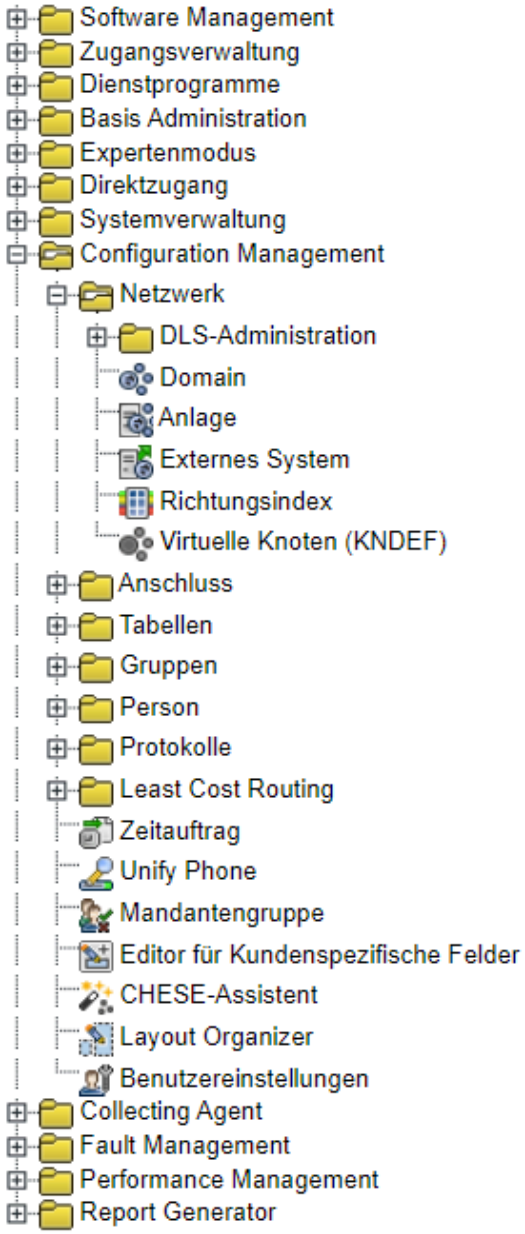


Abbildung 31: Domain in Configuration Management einrichten

3) Öffnen Sie im Fenster Domain das Menü Objekt und wählen Sie dort die Option Neu (siehe Bild 59).

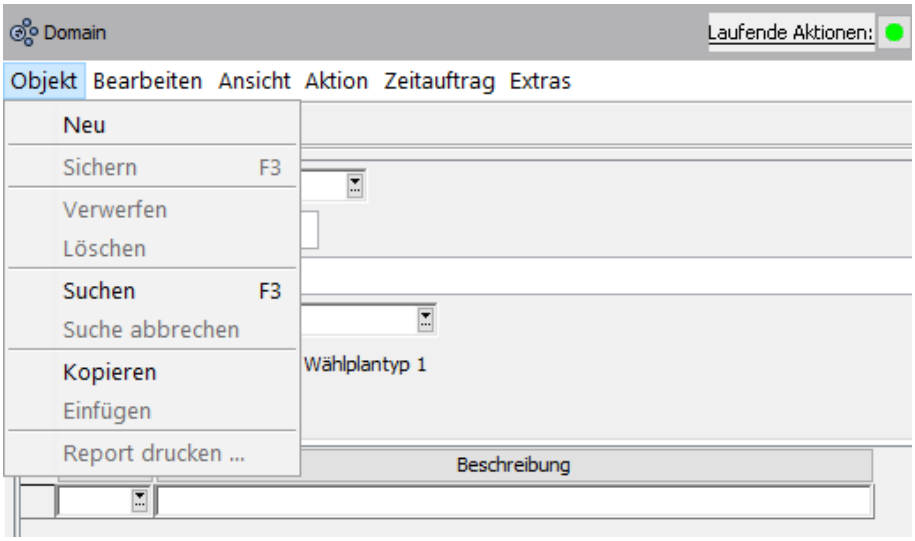


Abbildung 32: Das Menü "Objekt>im Fenster "Domain"

4) Geben Sie in das Feld Domain (siehe Bild 59) einen eindeutigen Namen für die neue Domain ein. Dieser Domainname dient zur Gruppierung von Anlagen, zu denen der Zugang über dieselbe Querwahl-Kennzahl erfolgt (geschlossener Nummerierungsplan).

Anmerkung: Die einer bestimmten Domain zugeordneten Anlagen werden auf der Registerkarte Anlagen angezeigt. Die Registerkarte Sub-Domain zeigt alle Anlagen an, die einem Sub-Netzwerk in dieser Domain zugeordnet sind.

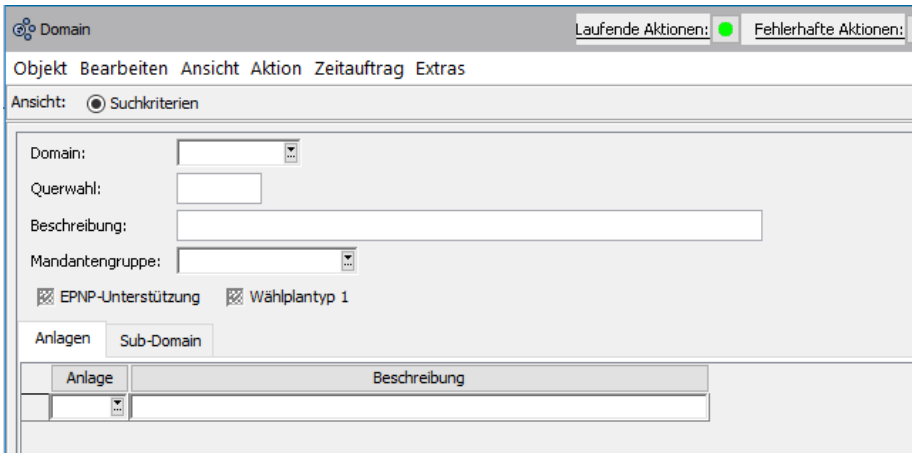


Abbildung 33: Neues Domain-Objekt erzeugen

5) Geben Sie in das optionale Feld Beschreibung eine Kurzbeschreibung der Domain ein.

6) Wiederholen Sie diese Schritte, um gegebenenfalls weitere Domains einzurichten.

Anmerkung:

Die Verwendung eines offenen Nummerierungsplans erfordert mehrere Domains. Wenn Sie mehr als eine Domain hinzufügen, geben Sie im Feld Querwahl die Querwahl-Kennzahl an, die gewählt werden muss, damit Anlagen in anderen Domains Zugang zu dieser Domain erhalten.

Die Option EPNP-Unterstützung (Enhanced Private Numbering Plan - Erweiterter privater Rufnummernplan) muss nur dann aktiviert werden, wenn der betreffenden Domain in den USA basierte Anlagen zugeordnet sind. EPNP wird dort generell anstelle von ISDN verwendet.

Die Option Wählplantyp 1 muss aktiviert werden, wenn der Rufnummernplan nicht für die gesamte Domain gilt, sondern anlagenbasiert ist. Das bedeutet, dass die einem bestimmten Nummernblock entsprechenden Teilnehmer unter Umständen nur einer Anlage zugeordnet sind. Daher müssen Teilnehmerrufnummern in sämtlichen Wählplänen mit ihrer korrekten Zielnummer zugeordnet werden, da Änderungen an einem Wählplan nicht an alle Anlagen innerhalb des Netzwerks weitergegeben werden. Die Änderung erfolgt nur lokal in der betreffenden Anlage.

Mit dem Feld Mandantengruppe kann der Administrationszugriff auf die Domain auf bestimmte Benutzer beschränkt werden. Benutzer, die zu dieser Mandantengruppe zählen, dürfen diese Domain verwalten, andere Benutzer jedoch nicht. Tatsächlich ist es anderen Benutzern nicht einmal möglich, diese Domain anzuzeigen.

4.4.2 CM – Hinzufügen einer neuen Anlage in OpenScape 4000 Manager

Das Fenster Anlage in Configuration Management kann genutzt werden, um folgende Aktionen zu den verschiedenen Anlagentypen einzuleiten:

- Suchen einer vorhandenen Anlage anhand diverser Kriterien
- Hochladen der Anlagendaten für
  - Teilnehmerdaten (UPLO2)
  - VoiceMail-Daten (UPLVM)
  - Least Cost Routing-Daten (UPLOL)
- Hinzufügen einer neuen Anlage
- Ändern einer vorhandenen Anlage
- Löschen einer vorhandenen Anlage

So fügen Sie in Configuration Management eine neue Anlage hinzu:

1) Klicken Sie im OpenScape 4000 Manager-Launchpad auf Configuration Management.

2) Klicken Sie im Netzwerk-Ordner auf Anlage.

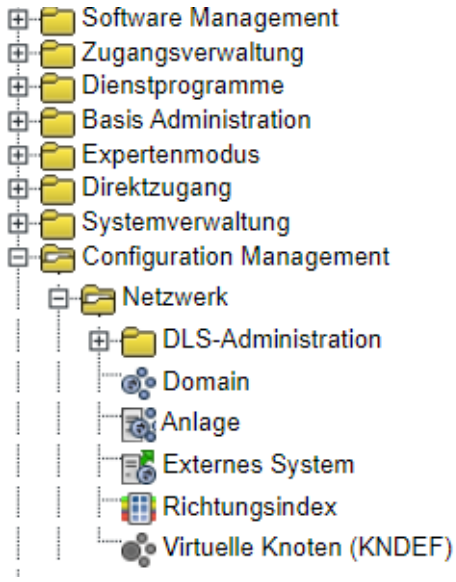


Abbildung 34: Hinzufügen einer neuen Anlage in Configuration Management

3) Geben Sie im Fenster Anlage die entsprechenden Werte in die allgemeinen Datenfelder ein:

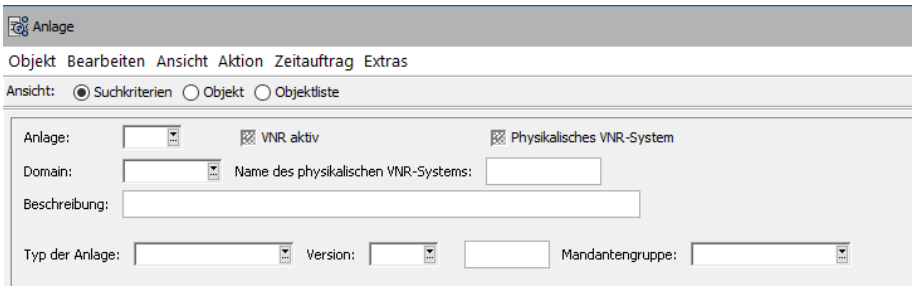


Abbildung 35: Allgemeine Daten für eine neue Anlage in Configuration Management

a) Geben Sie in das Feld Anlage die Anlagen-ID (vierstelliger alphanumerischer Wert) ein, die dieser Anlage in der Systemverwaltung zugewiesen wurde (siehe Abschnitt 4.3, "Systemverwaltung – Hinzufügen von OpenScape/HiPath 4000-Anlagen").

b) Wählen Sie in der Liste Domain die zuvor im Fenster "Domain" zugeordnete Domain aus (siehe Abschnitt 4.5.1.3, "Neue Domain im OpenScape 4000 Manager einrichten"). Hinweis: Das Fenster Domain können Sie öffnen, indem Sie auf die unterstrichene Bezeichnung (siehe Bild 62) klicken, oder indem Sie mit der rechten Maustaste in das Feld Domain klicken und dann in der Dropdown-Liste "Verknüpftes Objekt" auswählen.

c) Das Kontrollkästchen VNR aktiv gibt an, ob die Nummernerweiterungsfunktion des Nebenstellenfelds aktiviert (Kontrollkästchen markiert) oder deaktiviert ist (Kontrollkästchen nicht markiert). Bei aktivierter Funktion können lange Nebenstellennummern verwendet werden, d.h. die Nebenstellennummern in der Anlage werden auf folgende Weise kombiniert: Lange Nebenstellennummer = Virtuelle

Knotenkennzahl + kurze Nebenstellennummer (siehe auch Abschnitt 5.10, "Verwenden des virtuellen Rufnummernplans (VNR)")

Anmerkung:

Ist das Kontrollkästchen **VNR aktiv** markiert, ist das Leistungsmerkmal VNR (virtuelle Nummerierung) bei dieser Anlage aktiv. Sämtliche AMOs stellen die Nummern in langer Form dar; AMO UPLO2 liefert darüber hinaus alle Teilnehmer in langer Form.

Hinsichtlich der AMO-Eingabe werden lange Nummern akzeptiert. Ist das Kontrollkästchen **VNR aktiv** nicht markiert, kann der Benutzer keine mehrdeutigen Nummern hinzufügen.

Alle AMOs verwenden kurze Nummern als Eingabe, und UPLO2 liefert ebenfalls kurze Nummern. Sind mehrdeutige Nummern auf der Anlage konfiguriert, kann dieses Leistungsmerkmal nicht aktiviert oder deaktiviert werden.

AMO ZANDE gibt in diesem Fall eine Fehlermeldung zurück. Der Standardwert für dieses Feld ist "Aus".

OpenScape 4000 Configuration Management folgt der AMO-Darstellung von Rufnummern. Also werden, wenn das Flag "Global>deaktiviert ist, alle Rufnummern in ihrer Kurzform dargestellt, und CM lässt auf keinem virtuellen Knoten dieser Anlage Nummerndarstellung in langer Form zu.

Da dieses Leistungsmerkmal nicht in CM, sondern von AMO ZANDE aus verwaltet wird, kann der Benutzer dies nicht im Fenster "Anlage>ändern. Der Benutzer kann nur feststellen, ob das Leistungsmerkmal VNR aktiviert oder deaktiviert ist.

Die Aktivierung dieses Leistungsmerkmals muss über einen AMO-Befehl erfolgen. Nachdem das Leistungsmerkmal VNR durch AMO ZANDE aktiviert/ deaktiviert wurde und die erforderlichen Unteranlagen-Definitionen erfolgt sind, muss der Benutzer **Upload-All** zu der betreffenden Anlage ausführen. Die Darstellung von Rufnummern muss auf OpenScape 4000 Manager/ Assistant und der OpenScape/HiPath 4000 identisch sein.

---

d) Das Kontrollkästchen Physikalisches VNR-System zeigt an, ob die Anlage in der **Systemverwaltung**sanwendung auf der Registerkarte **Configuration Management** für OpenScape/HiPath 4000-Netzwerkobjekte als VNRAD (VNR über Domains hinweg) definiert ist oder nicht. Wenn es aktiviert ist, kann der Benutzer auf der Registerkarte "Unteranlagen-Daten" auf dieser Seite Unteranlagen definieren.

e) Das Textfeld Name des physikalischen VNR-Systems enthält den Namen der physikalischen Anlage, auf der diese Anlage (Unteranlage) definiert ist. Bei Unteranlagen entspricht dieser Wert nicht dem Namen der Anlage (Feld "Anlage"). Wenn es sich nicht um eine Unteranlage handelt, entspricht dieser Wert demjenigen im Feld "Anlage", der die Anlagen-ID darstellt.

f) In das Feld Beschreibung können Sie beliebige eigene Informationen zu dieser Anlage eingeben.

g) Wählen Sie in der Liste Typ der Anlage den entsprechenden Anlagentyp aus. Die Auswahl des richtigen Typs ist sehr wichtig, da es andernfalls zu Problemen bei der Synchronisation der Daten von der Anlage (UPLOADS) kommen kann.

Dabei stehen folgende Optionen zur Verfügung:

OpenScape/HiPath4000 -> für OpenScape/HiPath 4000-Anlagen

VMSR -> VoiceMail-Anlage ohne SCO-UNIX

VMSU -> VoiceMail-Anlage mit SCO-UNIX

h) Wählen Sie in der Liste Version die korrekte Systemversion aus. Folgende Werte werden unterstützt:

- UV1.0, UV2.0, UV3.0, V4, V5, V6, V7, V8, V10 (OpenScape/HiPath 4000)

i) Mit dem Feld Mandantengruppe kann der Administrationszugriff auf diese Anlage beschränkt werden. Nur Benutzer, die zu dieser Mandantengruppe zählen, dürfen diese Anlage verwalten. Alle anderen Benutzer haben keine Administrationsrechte; tatsächlich können sie diese Anlage nicht einmal anzeigen.

4) Klicken Sie auf die Registerkarte Basisdaten, und geben Sie die erforderlichen Werte in die folgenden Felder ein (siehe Bild 63).

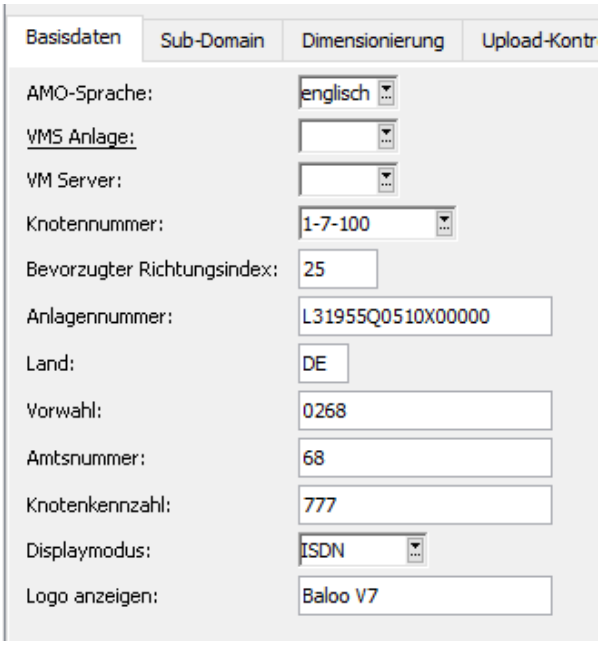


Abbildung 36: Basisdaten für eine neue Anlage in Configuration Management (Teil 1)

a) Wählen Sie im Feld AMO-Sprache "Deutsch>oder "Englisch" die AMO-Sprache für die Ausführung von CM-Aufträgen aus. Im Allgemeinen wird die AMO-Sprache nicht in Configuration Management, sondern in der Systemverwaltung definiert (siehe Abschnitt 4.3, "Systemverwaltung – Hinzufügen von OpenScape/HiPath 4000-Anlagen").

b) Ist noch ein VoiceMail-Server in Ihrem Netzwerk in Betrieb, geben Sie die Anlage, wo der VM-Server installiert ist, in das Feld VMS Anlage ein bzw.

wählen Sie sie dort aus. Wählen Sie anschließend im Feld VM Server einen der Werte (V1 - V3, T1 - T3 oder A1) entsprechend der VoiceMail-Installation aus.

c) Geben Sie in das Feld Knotennummer die Knotennummer der Anlage gemäß Definition in AMO ZAND ein. Geben Sie in das Feld Bevorzugter Richtungsindex die Zielnummer der Anlage ein. Diese Zielnummer kann in einer anderen Anlage im Netzwerk mittels AMO WABE festgestellt werden, und zwar durch Ausführen eines REGEN-Befehls zu einer vorhandenen Nebenstellennummer für die zu erstellende Anlage.

d) Geben Sie in das Feld Anlagennummer die Anlagennummer ein, wie sie in AMO ANSU für diese Anlage zugewiesen ist.

e) Geben Sie in das Feld Land die zweistellige Kennung des Landes ein, in dem die Anlage ihren Standort hat, beispielsweise DE für Deutschland. Geben Sie in das Feld Vorwahl die Vorwahlnummer der Stadt ein, beispielsweise 89 für München. Geben Sie im Feld Ländercode die Amtskennzahl ein, die für den Zugang zu dieser Anlage benötigt wird (beispielsweise 7007 für den Standort unseres Unternehmens in der Hofmannstraße).

f) Die Knotenkennzahl wird beim Upload automatisch eingefügt. Dies ist die Kennzahl der Anlage, wie sie in AMO ZAND zugewiesen wurde.

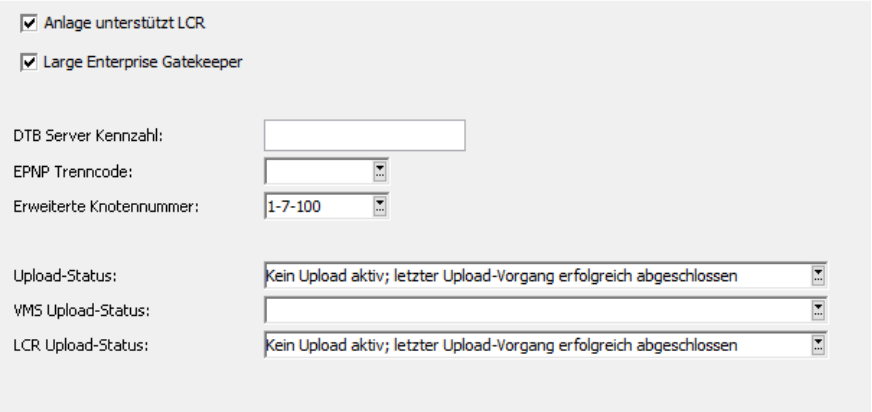


Abbildung 37: Basisdaten für eine neue Anlage in Configuration Management (Teil 2)

Anmerkung: Orientieren Sie sich bei den weiteren Schritten ab Schritt g) an der obigen Bild 64.

---

g) Aktivieren Sie das Kontrollkästchen Anlage unterstützt LCR, wenn auch die LCR-relevanten Daten im UPLOAD erfasst werden sollen. Die Option Large Enterprise Gatekeeper wird vom Upload erkannt und automatisch aktiviert.

h) Das Feld DTB Server Kennzahl ist für mobile Teilnehmer wichtig. Die Namenstasten eines Geräts können für den Zugriff auf das elektronische Telefonbuch (DTB-Taste, Journal) programmiert werden. Der Standardwert ist 900; dieser wird nicht von der Anlage hochgeladen.

i) Das Feld EPNP Trenncode ist wichtig für den US-spezifischen Wählplan des Typs EPNP, der offene Nummerierung (PNP) verwendet, um Konflikte zwischen den Standortcodes und Nebenstellennummern zu vermeiden.

j) In das Feld Erweiterte Knotennummer wird bei Anlagen, die dem dreiteiligen Knotennummerierungsschema entsprechen, automatisch

die Knotennummer eingetragen. Bei älteren Anlagen, die diesem Nummerierungsschema nicht entsprechen, kann die Knotennummer hier an das dreiteilige Nummerierungsschema angepasst werden. Beispielsweise wird die Knotennummer 301 einer älteren V3.4-Anlage durch die Eingabe von 1-85-301 in das Feld Erweiterte Knotennummer angepasst.

k) Die Felder Upload-Status, VMS Upload-Status und LCR Upload-Status sind rein informative Felder, die den aktuellen Status des jeweiligen Upload-Typs anzeigen.

l) Überprüfen Sie alle Parameterwerte auf der Registerkarte Basisdaten, und klicken Sie dann auf Sichern, um diese Einstellungen zu speichern.

m) Laden Sie nun alle relevanten Anlagendaten hoch, indem Sie folgendermaßen vorgehen (Folgen Sie bei einer VNR-Anlage den Anweisungen in Schritt 5, bevor Sie mit dem Upload fortfahren.):

- Wählen Sie im Menü Aktion den Menüeintrag Upload. Damit wird der Abruf der Teilnehmerdaten zu dieser Anlage durch Configuration Management gestartet.
- Starten Sie gegebenenfalls auch den Abruf von LCR-Daten, indem Sie LCR-Upload im Menü **Aktion** wählen.
- Ist mit dieser Anlage ein VoiceMail-Server verbunden, laden Sie die VMS-Daten hoch, indem Sie VMS-Upload im Menü **Aktion** wählen.

Nach Abschluss dieser Uploads werden die anlagenbezogenen Daten auch auf den anderen Registerkarten angezeigt.

5) So fügen Sie in Configuration Management eine neue Unteranlage hinzu

Handelt es sich um eine VNR-Anlage, müssen vor dem Upload die Unteranlagen ordnungsgemäß definiert werden, da sonst der Upload-Vorgang wegen Fehlkonfiguration fehlschlägt.

Klicken Sie auf die Registerkarte **Unteranlagen-Daten**, und geben Sie die entsprechenden Unteranlagen-Informationen zu dieser Anlage ein.

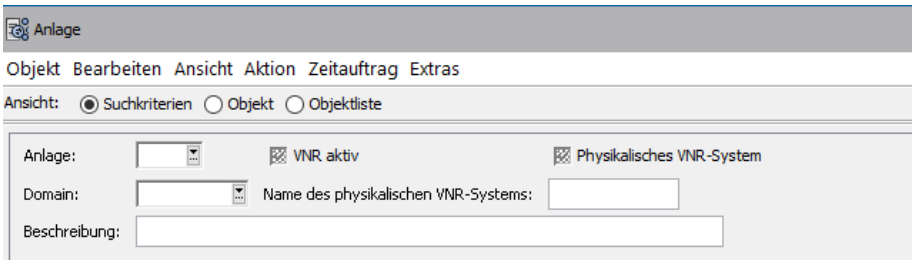


Abbildung 38: Registerkarte "Generic Data and Sub-Switch>(Allgemeine Daten und Unteranlage) für eine neue Anlage in Configuration Management

a) Auf dieser Registerkarte werden Unteranlagen für die VNR-Anlagen definiert. Das Feld **Physikalisches VNR-System** oben muss bei dieser VNR-Anlage aktiviert werden, damit Unteranlagen für sie definiert werden können. Es wird vorausgesetzt, dass sich der Administrator mit der Konfiguration des virtuellen Knotens vertraut gemacht hat, bevor er die Unteranlagen hinzufügt.

b) **Unteranlagen-ID** ist der 4 Zeichen lange Name der Anlage, der im Feld **Anlage** angezeigt wird. In dieser Tabelle sollte dieselbe Anzahl

an Unteranlagen definiert werden, wie es virtuelle Knoten auf der physikalischen Anlage gibt.

c) **Virtuelle Knotennummer** ist die ID des virtuellen Knotens, dem diese Unteranlage auf der Anlage entspricht. Wird es weitere Unteranlagen anderer VNR-PN in der Domain dieser Unteranlage geben, muss der Administrator sicherstellen, dass sie alle dieselbe virtuelle Knoten-ID haben.

d) **Virtuelle Knotenkennzahl** ist die Kennzahl des virtuellen Knotens, dem diese Unteranlage auf der Anlage entspricht. Wird es weitere Unteranlagen anderer VNR-PN in der Domain dieser Unteranlage geben, muss der Administrator sicherstellen, dass sie alle dieselbe virtuelle Knotenkennzahl haben.

e) Die Domain der Unteranlage ist im Feld **Domain** festgelegt. Es ist wichtig, dass alle Unteranlagen desselben physikalischen Knotens unterschiedlichen Domains zugeordnet sind. Es kann entweder eine vorhandene Domain aus der Liste ausgewählt oder ein neuer Domainname eingegeben werden (in letzterem Fall wird diese Domain automatisch erstellt).

f) Die Querwahl-Kennzahl der Domain der Unteranlage wird in das Feld **Querwahl** eingegeben. Beachten Sie, dass die Querwahl-Kennzahl jeder Domain im Netzwerk eindeutig sein muss.

g) **Richtungsindex** bezeichnet die bevorzugte Zielnummer, die andere Anlagen für das Routing zu dieser Anlage nutzen können.

h) In das Feld **Beschreibung** können Sie beliebige Zusatzinformationen zu dieser Anlage eingeben.

i) Sobald Sie auf "Speichern>klicken, werden die neuen Unteranlagen erstellt; über den Dialog "Anlage>können sie gesucht und angezeigt werden. Bei den in dieser Registerkarte eingegebenen Parametern (Name, virtuelle Knoten-ID, virtuelle Knotenkennzahl, Domain, Querwahl, Richtungsindex und Beschreibung) weisen sie eigene Werte auf, während die übrigen, vom virtuellen Knoten unabhängigen Werte von der physikalischen Anlage kopiert werden, da sie bei jeder Anlage auf dem physikalischen Knoten gleich sind.

j) Das Upload erfolgt wie weiter oben beschrieben, allerdings kann es nur zu physikalischen Anlagen und zu VNR-Anlagen gestartet werden. Es ist nicht möglich, ein Upload nur zu einer Unteranlage zu starten. Damit ist sichergestellt, dass alle Unteranlagen einer Anlage zusammen hochgeladen werden.

k) In den restlichen Bildschirmen werden im Feld "Anlage>nur Unteranlagen angezeigt. Physikalische Anlagen werden nur im Dialog "Anlage" angezeigt.

4.4.3 Anlagen hochladen

Nach der Einrichtung aller Anlagen in der Systemverwaltung und in Configuration Management muss der OpenScape 4000 Manager-Server mit den verwalteten OpenScape/HiPath 4000-Anlagen synchronisiert werden. Diese Datenbanksynchronisierung gewährleistet, dass der OpenScape 4000 Manager-Server stets den aktuellen Anlagenstatus enthält.

Um diese Synchronisierung durchzuführen, führt Configuration Management auf jeder OpenScape/HiPath 4000-Anlage ein Upload durch. OpenScape 4000 Manager Configuration Management stellt eine grafische Benutzeroberfläche (GUI) für die Administration dieser Anlagen bereit.

4.4.3.1 OpenScape/HiPath 4000 hochladen

Gehen Sie wie folgt vor, um eine OpenScape/HiPath 4000-Anlage hochzuladen:

1) Klicken Sie im OpenScape 4000 Manager-Launchpad zunächst auf Configuration Management und anschließend auf Anlage (siehe Bild 66).

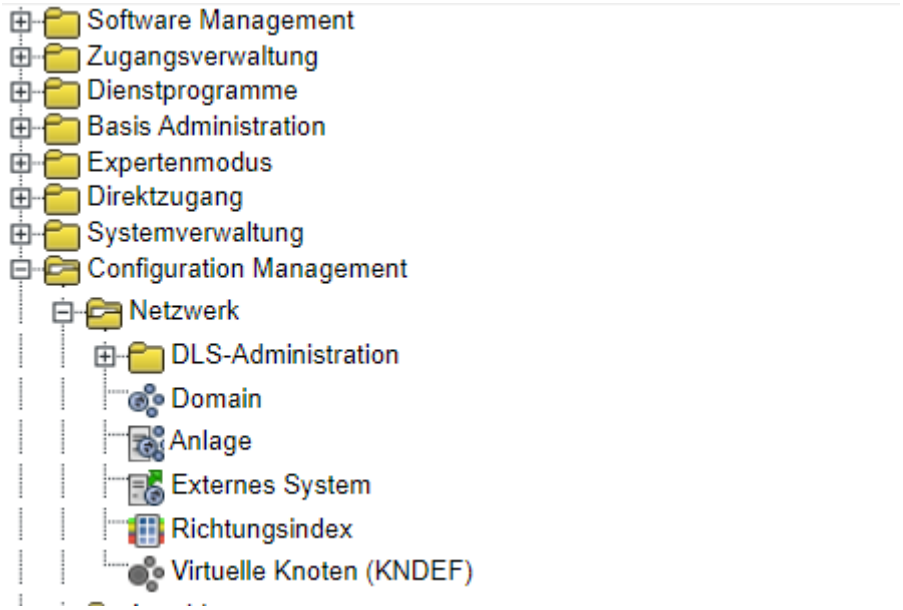


Abbildung 39: Uploads von OpenScape/HiPath 4000 über Configuration Management einleiten

2) Klicken Sie im Dialogfenster Anlage auf die Schaltfläche Suchen, um alle in der Systemverwaltung konfigurierten OpenScape/HiPath 4000-Anlagen zu ermitteln.

3) Wählen Sie mit den Tasten  und  die OpenScape/HiPath 4000-Anlage aus, die Sie hochladen wollen.

4) Öffnen Sie im Dialogfenster Configuration Management – Anlage erneut das Menü Aktion und klicken Sie dann auf Upload (siehe Bild 67).

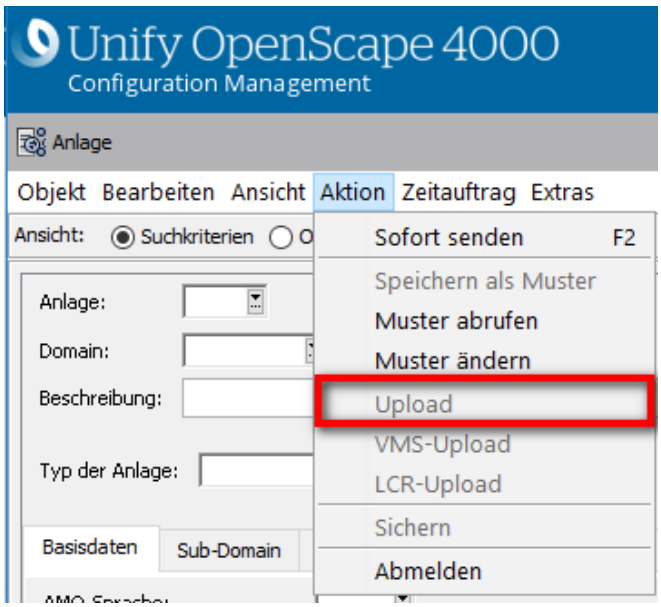


Abbildung 40: Das Menü "Aktion>im Dialogfenster "Anlage"

a) Fall 1: Bisher wurde noch kein Upload durchgeführt Wenn bisher noch keine Upload-Vorgänge durchgeführt wurden (neues System), gestattet Configuration Management nur ein Upload All (siehe Bild 68). Bei einem Upload All handelt es sich um eine vollständige Synchronisierung der OpenScape 4000-Kundendatenbank. Ergebnis eines Upload All-Vorgangs ist die Duplizierung aller OpenScape 4000 Manager-bezogenen Kundendaten im OpenScape 4000 Manager-Server.

b) Fall 2: Es wurden bereits Uploads durchgeführt Wenn zuvor bereits Upload-Vorgänge durchgeführt wurden, stehen in Configuration Management folgende Upload-Typen zur Auswahl (siehe Bild 69):

- Upload All
- Upload Delta

Anmerkung: Wenn eine OpenScape/HiPath 4000-Anlage erstmals ein Upload All zum OpenScape 4000 Manager-Server durchführt, wird in der OpenScape/HiPath 4000-Anlage eine so genannte "Snapshot-Datei>erzeugt, die alle Informationen der Kundendatenbank auflistet, die im OpenScape 4000 Manager-Server dupliziert wurden. Fordert der OpenScape 4000 Manager-Server später ein Upload Delta an, vergleicht die OpenScape/HiPath 4000-Anlage die aktuelle Kundendatenbank mit der vorhandenen "Snapshot-Datei". Dann werden nur die Abweichungen in der aktuellen Konfiguration an den OpenScape 4000 Manager-Server gesendet. Daher nimmt ein Upload Delta in der Regel wesentlich weniger Zeit in Anspruch als ein Upload All.

---

5) Klicken Sie entweder auf Upload All starten oder Upload Delta starten.
6) Starten Sie das ausgewählte Upload durch Anklicken von OK.

7) Wenn Sie auch auf anderen OpenScape/HiPath 4000-Anlagen Uploads durchführen wollen, selektieren Sie den nächsten Datensatz und wiederholen Sie den Upload-Vorgang.

4.4.3.2 Periodische Uploads für OpenScape/HiPath 4000 planen

Nach dem ersten Upload All-Vorgang bei einem System müssen periodische Synchronisierungen geplant werden. Diese Synchronisierungen können täglich oder wöchentlich erfolgen. Alle geplanten Uploads sind Delta-Uploads, die standardmäßig an dem/den zuvor ausgewählten Tag(en) um 10:00 Uhr vormittags durchgeführt werden.

Führen Sie folgende Schritte aus, um die Synchronisierung zu planen:

1) Klicken Sie im OpenScape 4000 Manager-Launchpad zunächst auf Configuration Management und anschließend auf Anlage (siehe Bild 66 auf Seite 150).
2) Klicken Sie im Dialogfenster Anlage auf die Schaltfläche Suchen, um alle in der Systemverwaltung konfigurierten OpenScape/HiPath 4000-Anlagen zu ermitteln.
3) Wählen Sie mit den Tasten  und  die OpenScape/HiPath 4000-Anlage aus, die Sie hochladen wollen.
4) Klicken Sie im Dialogfenster Configuration Management – Anlage auf das Register Upload-Kontrolle (siehe Bild 70).

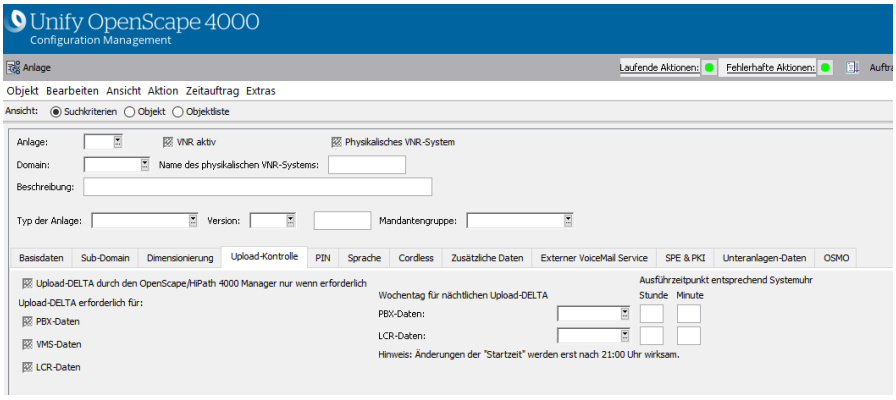


Abbildung 41: Das Register "Upload-Kontrolle>im Dialogfenster "Anlage"

5) Öffnen Sie unter Wochentag für nächtlichen Upload-DELTA das Listenfeld ("PBX-Daten>oder "LCR-Daten"), um die Auswahlliste Suchen in Tabelle anzuzeigen.

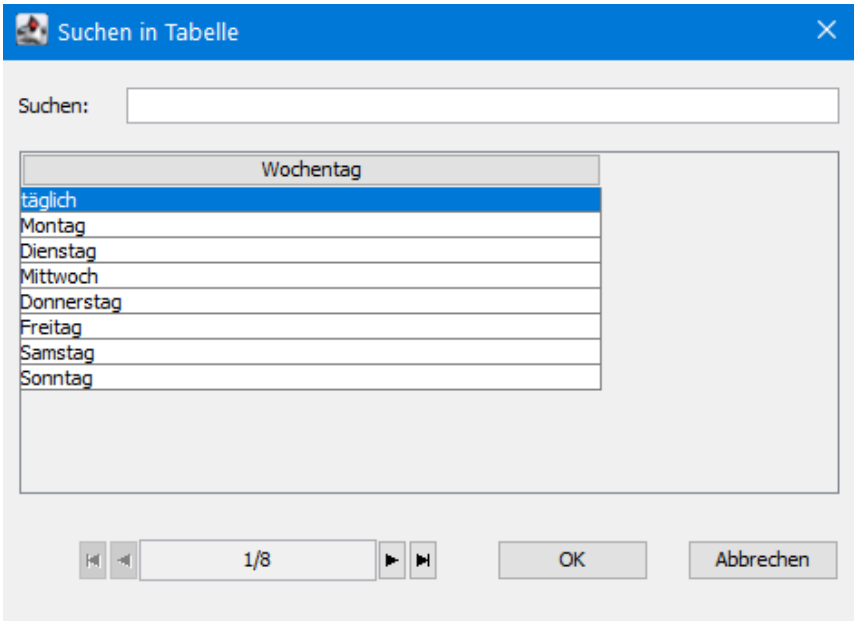


Abbildung 42: Auswahlliste für die Planung von Upload Delta-Vorgängen

6) Wählen Sie per Mausklick den Wochentag, an dem der Upload Delta-Vorgang durchgeführt werden soll, oder die Option "täglich".
7) Klicken Sie auf OK, um zum Dialogfenster "Anlage>zurückzukehren.
8) Klicken Sie dort auf Speichern, um die vorgenommenen Änderungen zu speichern.
9) Klicken Sie in dem Bestätigungsfenster von Configuration Management auf OK, um die Änderung durchzuführen oder auf "Abbruch", um sie zu verwerfen.
10) Wenn Sie auch auf anderen OpenScape/HiPath 4000-Anlagen Uploads durchführen wollen, wählen Sie den Datensatz der betreffenden Anlage aus und wiederholen Sie den Upload-Vorgang.

4.4.3.3 Upload-Status für OpenScape/HiPath 4000 einsehen

In Configuration Management kann der aktuelle Upload-Status für OpenScape/HiPath 4000-Anlagen im Register Basisdaten des Dialogfensters Anlage eingesehen werden.

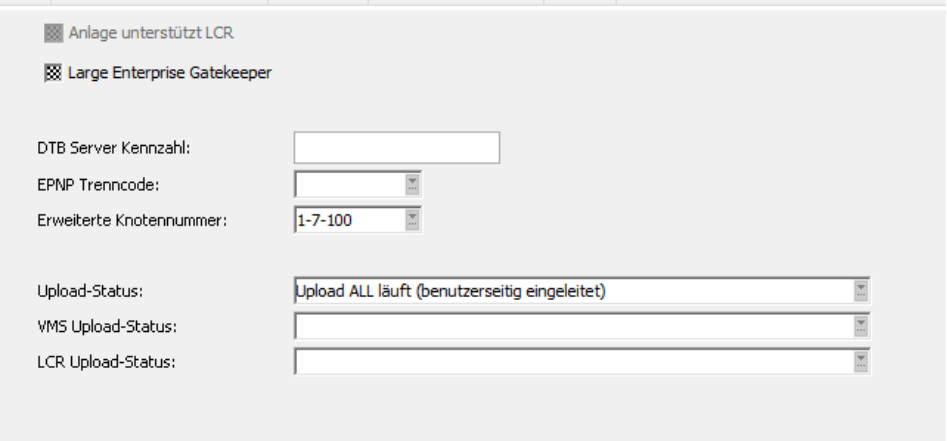


Abbildung 43: Upload-Status in Configuration Management einsehen

Für diese OpenScape/HiPath 4000-Anlage können Sie den Upload-Status auch im Register Configuration Management der Systemverwaltung überprüfen.

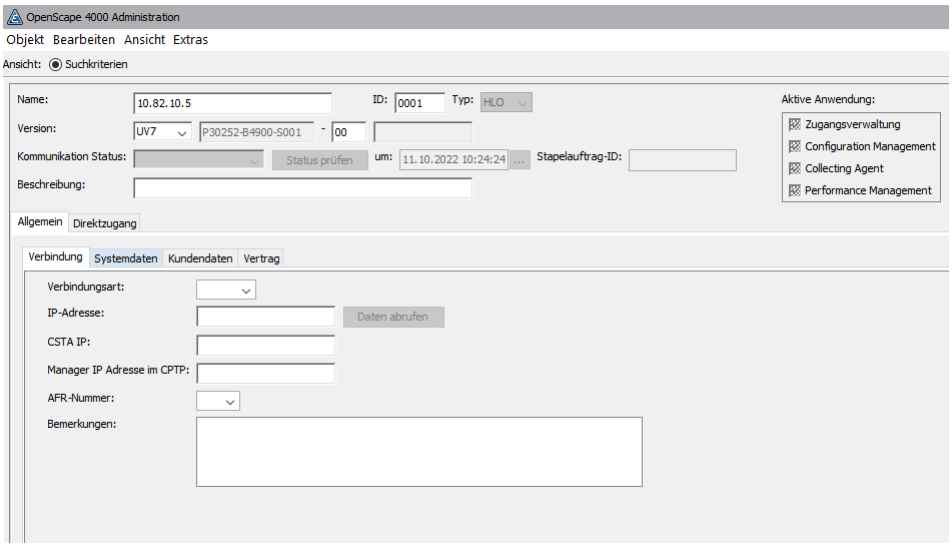


Abbildung 44: Upload-Status in der Systemverwaltung einsehen

4.5 Benutzerverwaltung - Erstellen von Benutzernamen und Zuweisen von Anwendungen

Die Zugriffsverwaltung definiert fünf verschiedene Sicherheitsstufen oder Benutzerrollen innerhalb des Manager Linux Containers.

Anmerkung: Der Root-Zugang zur Plattform ist nur für die Fehlersuche und das Einstellen von kundenspezifischen Daten oder Skripten vorgesehen.

Die vordefinierten Sicherheitsstufen sind in Tabelle 4 unten dargestellt.

Tabelle 2: Sicherheitsstufen in der Zugriffsverwaltung

Sicherheitsst	Vordefiniertes Benutzerkonto	Linux Container Shell-Zugriff	Eigentümer	Bemerkungen
engr	engr	ja	Service	Techniker; nur in Notfällen zu verwenden. Beinhaltet alle anderen Sicherheitsstufen. Zugriff auf Linux-Shell mit Superuser-Rechten (uid 0).
rsta	rsta	ja	Service	Technische Fernwartungsunterstützung; wird von Servicetechnikern der höheren Ebene verwendet. Umfasst die Sicherheitsstufe rsca.
rsca	rsca	ja	Service	Fernservice-Kundenunterstützung; wird von Servicetechnikern der unteren Ebene verwendet.
cusa	cusa	nein	Kunde	Kunden-Sicherheitsadministrator; wird von dem/den „Master“-Administrator(en) des Kunden verwendet. Umfasst die Sicherheitsstufe cust.
cust	----	nein	Kunde	Kundenebene; individuelle Konten können zur Laufzeit erstellt werden, um sie in die kundenspezifische Umgebung einzupassen.

Alle vordefinierten Konten haben ein voreingestelltes Standardpasswort, das bei der ersten Anmeldung geändert werden muss. Individuelle Konten können je nach den Bedürfnissen des einzelnen Kunden eingerichtet werden. Diese Fähigkeit erfordert die Anmeldung mit einer Sicherheitsstufe von cusa, rsca, rsta oder engr.

Jeder OpenScape 4000 Manager Client muss einen eindeutigen Benutzernamen verwenden. Diese zusätzlichen Benutzernamen werden in der OpenScape 4000 Manager Zugangsverwaltung angelegt. Jeder Benutzername wird durch die Zuweisung von Anwendungen, die den Anforderungen des Benutzers entsprechen, angepasst. Wenn OpenScape 4000 Manager Clients eindeutige, angepasste Benutzernamen verwenden, kann der Benutzer nur die dem Benutzernamen zugewiesenen Aufgaben ausführen.

Gehen Sie wie folgt vor, um einen neuen Benutzernamen zu erstellen und Anwendungen zuzuweisen:

1) Klicken Sie im Launchpad von OpenScape 4000 Manager auf die Anwendungsleiste Zugangsverwaltung.

2) Klicken Sie unter Kontoverwaltung auf Benutzerkontenverwaltung.

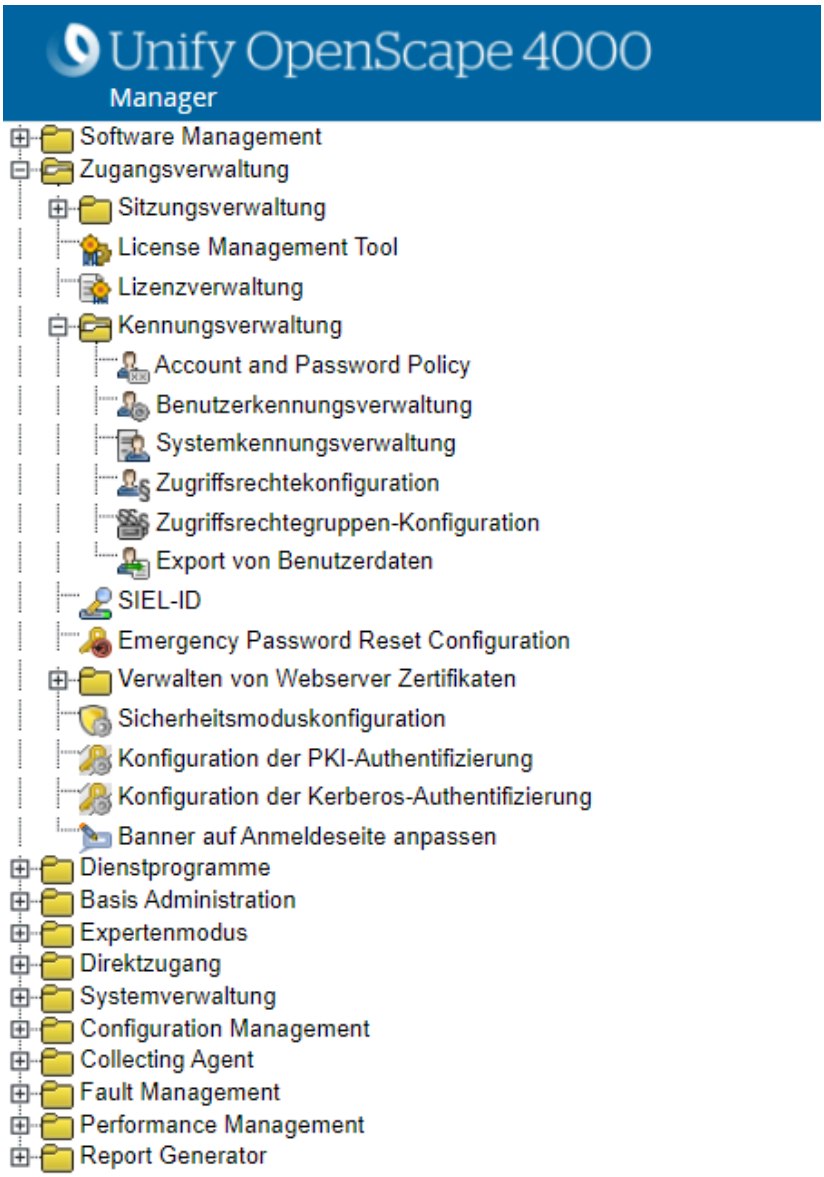


Abbildung 45: Starten der Benutzerkontenverwaltung zum Hinzufügen eines neuen Benutzers

3) Öffnen Sie im Dialogfeld Benutzerkontenverwaltung das Menü Benutzer und klicken Sie auf Hinzufügen.

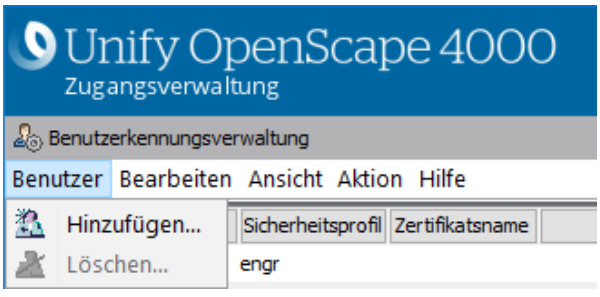


Abbildung 46: Dialogfeld „Benutzerverwaltung

4) Geben Sie im Dialogfeld Neuen Benutzer hinzufügen einen eindeutigen Benutzernamen in das Feld Neuer Benutzername und eine kurze Beschreibung in das Feld Beschreibung ein. Der **Zertifikatsname** sollte nur ausgefüllt werden, wenn die PKI-Infrastruktur für die Anmeldung am System verwendet wird. Wählen Sie eine Sicherheitsstufe für den Benutzer. Der Standardbenutzer ist „cust“. Für eine Liste der Sicherheitsstufen siehe Tabelle 4.
5) Klicken Sie auf „OK“.

Anmerkung: Beachten Sie, dass der neue Benutzername der Liste im Dialogfeld Benutzerkontenverwaltung hinzugefügt wird.

---

6) Geben Sie auf der rechten Seite des Dialogfelds Benutzerkontenverwaltung die folgenden Informationen ein:

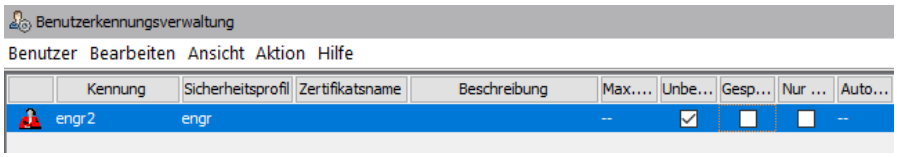


Abbildung 47: Vervollständigen der Informationen für einen neuen Benutzer

a) Geben Sie ein neues Passwort ein und wiederholen Sie das Passwort. Dieses Passwort wird von dem neuen Benutzer beim ersten Anmeldeversuch verwendet.
b) Klicken Sie auf Kennwortänderung erzwingen, um den neuen Benutzer aufzufordern, das Kennwort zu ändern, nachdem er sich zum ersten Mal erfolgreich angemeldet hat.
c) Stellen Sie die Eigenschaften entsprechend den kundenspezifischen Anforderungen ein.

7) Klicken Sie auf Übernehmen, um die Attribute des neuen Benutzers zu speichern.
8) Schließen Sie die Anwendung Benutzerkontenverwaltung.

9) Für Benutzer mit der Sicherheitsrolle „cust“ können Zugriffsrechte definiert werden. Klicken Sie im Launchpad unter Zugangsverwaltung auf Zugriffsrechtekonfiguration.

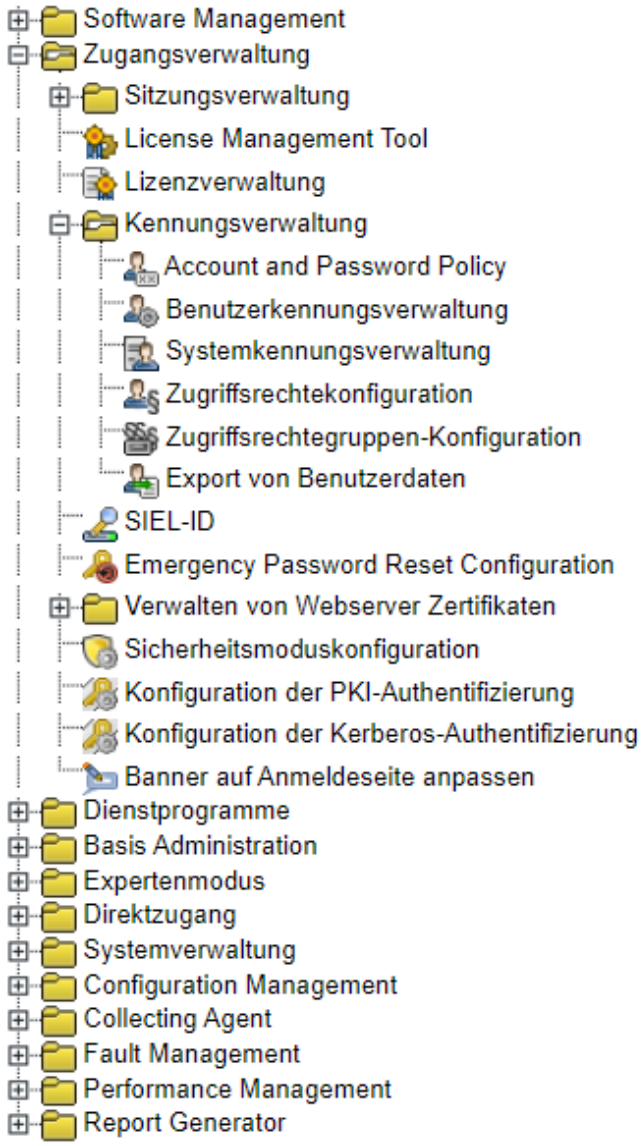


Abbildung 48: Start der Konfiguration der Zugriffsrechte

10) Wählen Sie im Fenster Konfiguration der Zugriffsrechte links den neuen Benutzernamen und dann in der rechten Spalte die Zugriffsrechte aus, die dem Benutzer zugewiesen werden sollen.

Anmerkung: In dem hier gezeigten Beispiel werden dem Benutzer alle verfügbaren Zugriffsrechte zugewiesen. Verwenden Sie die Umschalttaste oder die Strg-Taste, um bestimmte Kombinationen oder Bereiche von Merkmalen

auszuwählen. Ausführlichere Anweisungen finden Sie in der Online-Hilfe.

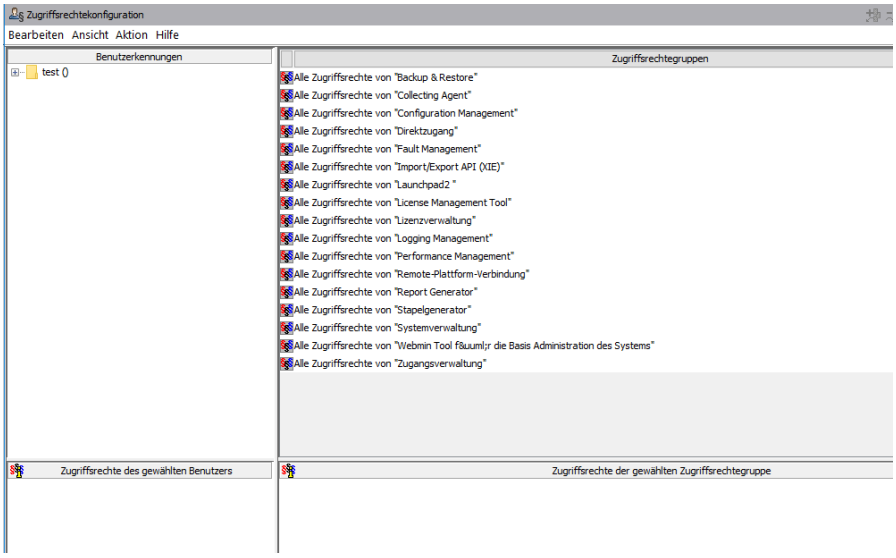


Abbildung 49: Auswahl der Zugriffsrechte, die dem neuen Benutzer zugewiesen werden sollen

11) Um die Zuweisung zu aktivieren, öffnen Sie das Menü Bearbeiten und wählen Sie Zuweisen.

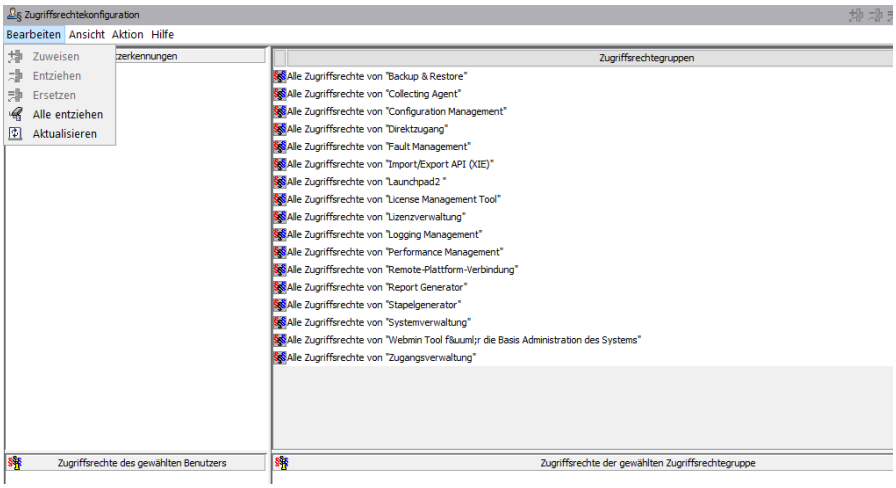


Abbildung 50: Zuweisung von Zugriffsrechten in der Zugriffsverwaltung

Anmerkung: Alternativ können Sie auch auf die Schaltfläche Zuweisen oben rechts auf dem Bildschirm klicken

12) Um einen weiteren Benutzernamen hinzuzufügen, wiederholen Sie diesen Vorgang.

4.6 User Management – Konfigurieren von Zugriffsrechtegruppen

Im Dialogfeld Zugriffsrechtegruppen-Konfiguration können Sie nach Bedarf eigene Zugriffsrechtegruppen für die von Ihnen erstellten Benutzer definieren. Zugriffsrechtegruppen werden zur Verwaltung der Benutzerrechte für die Ausführung und Verwendung der in OpenScape 4000 Manager verfügbaren Anwendungen benötigt.

Unmittelbar nach der Erstinstallation sind bereits einige vordefinierte Zugriffsrechtegruppen verfügbar. Das Dialogfeld Zugriffsrechtegruppen-Konfiguration dient zum Ändern der vorhandenen Gruppen bzw. zum Anlegen weiterer Gruppen. Änderungen an einer Zugriffsrechtegruppe wirken sich auf alle zu dieser Gruppe gehörigen Benutzer aus. Die Zuordnung neu erstellter Zugriffsrechtegruppen zu Benutzern erfolgt im Dialog "Zugriffsrechtegruppen-Konfiguration" (siehe Section 4.6.)

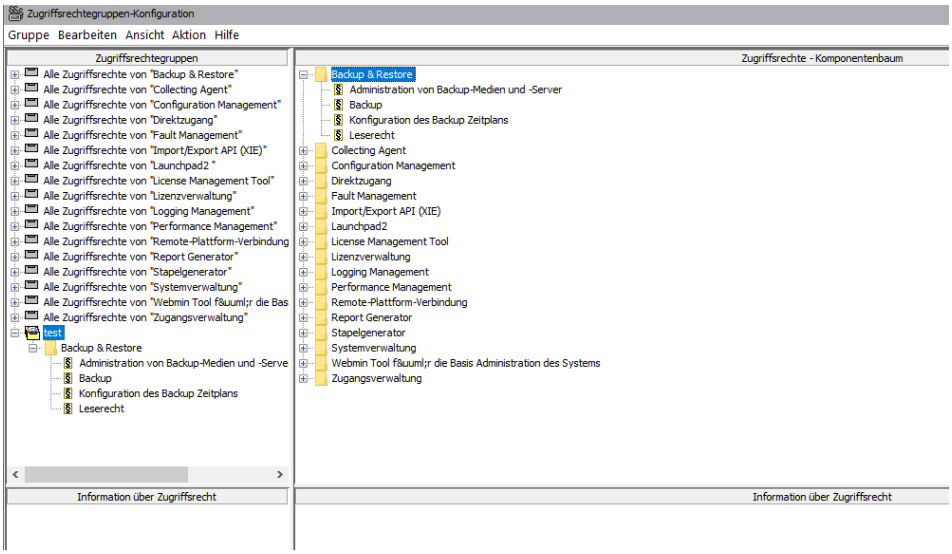


Abbildung 51: Erstellte Zugriffsrechtegruppe "Administrator"

Komponenten der Benutzeroberfläche

Das Dialogfeld besteht aus zwei Teilen. Links sind alle Zugriffsrechtegruppen (vordefiniert, selbstdefiniert und dynamisch) mitsamt ihrer Verzeichnisbaumstruktur aufgeführt. Rechts befinden sich die Zugriffsrechtegruppen und ihre verfügbaren Elemente, die den selbstdefinierten Zugriffsrechtegruppen zugeordnet werden können. Auf jeder Seite gibt es ein Vorschaufenster, in dem die Elemente der Zugriffsrechtegruppe detailliert angezeigt werden. Diese Vorschaufenster können aktiviert bzw. deaktiviert werden. Sie können die vordefinierten Zugriffsrechtegruppen auf der linken Seite zur Ableitung einer neuen Zugriffsrechtegruppe nutzen, indem Sie die Standardgruppe kopieren. Damit gehen alle Rechte der vordefinierten Gruppe auf die neue Gruppe über. Die so erstellte Gruppe können Sie anschließend nach Bedarf modifizieren. Um die Anzeige übersichtlicher zu gestalten, können Sie die verschiedenen Zugriffsrechtegruppen auf der linken Seite ausblenden.

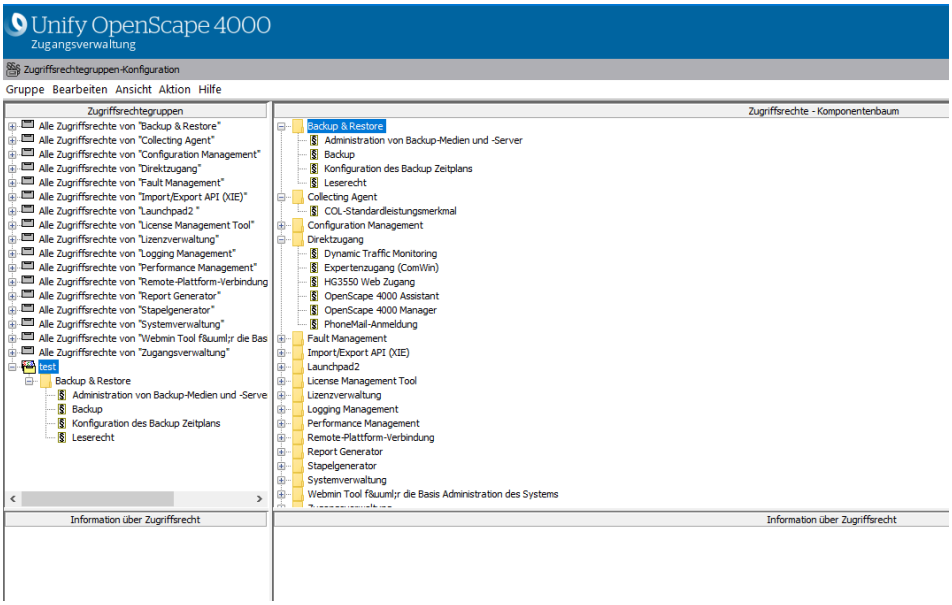


Abbildung 52: Verzeichnisbaumstruktur der Zugriffsrechtegruppe "Administrator"

4.7 User Management – Einrichten und Ändern von Passwörtern

4.7.1 Der Administrator ändert das Passwort für den Benutzer

Mit der Applikation Benutzerkennungsverwaltung der Zugangsverwaltung können Sie Passwörter für neue Benutzer einrichten (siehe Abschnitt 4.6, "User Management – Erstellen von Benutzernamen und Zuweisen von Anwendungen").

Wenn der Systemadministrator von OpenScape 4000 Manager ein Passwort für einen Benutzer eingibt, muss dieses folgende Bedingungen erfüllen:

- Das Passwort muss ein oder mehr alphanumerische Zeichen enthalten.
- Bei alphabetischen Zeichen ist zwischen Groß- und Kleinschreibung zu unterscheiden.
- Sonderzeichen sind möglich.

Wenn ein Benutzer das Passwort ändert, muss das neue Passwort (standardmäßig):

- insgesamt – d. h. einschließlich Sonderzeichen – zwischen 6 und 16 Zeichen umfassen.
- mindestens ein Sonderzeichen enthalten.
- sich in mindestens 3 Zeichen vom bisherigen Passwort unterscheiden.

4.7.2 Account and Password Policy

Die Applikation Account and Password Policy dient zum Aktivieren und Konfigurieren von erweiterten Regeln für Passwort-Richtlinien und die zeitgesteuerte Nutzung von Accounts.

Starten Sie die Applikation.

Die Seite Konfiguration von Account and Password Policy kann über die Startseite aufgerufen werden: Kennungsverwaltung -> Account and Password Policy.

Konfiguration und Aktivierung von Passwort-Regeln

Alle zukünftigen Account-Passwörter (administrativ und nicht-administrativ) müssen konfigurierbaren Regeln entsprechen (xx-Werte sind in der Applikation konfigurierbar):

- Passwörter müssen mindestens xx Zeichen lang sein.
- Passwörter müssen eine bestimmte Kombination aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.
- Die Wiederverwendung eines der xx zuvor verwendeten Passwörter ist nicht erlaubt.
- Passwörter dürfen innerhalb von xx Tagen höchstens einmal geändert werden. Administratoren oder privilegierte Benutzer sind von dieser Regelung ausgenommen. Es kann erforderlich sein, dass privilegierte Benutzer mehr als einmal am Tag vergessene Benutzerpasswörter zurücksetzen oder Passwörter ändern müssen.
- Das neue Passwort muss sich vom vorherigen Passwort in mindestens xx Zeichen unterscheiden.
- Die Verwendung von Wörterbucheinträgen ist nicht erlaubt.

Anmerkung: Die Passwort- und Account-Regeln werden erst aktiv, wenn die entsprechenden Kontrollkästchen markiert sind. Das Befehlszeilenprogramm "passwd" ist deaktiviert!

Konfiguration und Aktivierung von Account-Regeln

Diese Konfiguration umfasst die allgemeinen Einstellungen für alle Konten.

- Enable duty hours (Bürozeiten aktivieren)
- Sperren des Accounts nach einer vorgegebenen Zeit der Inaktivität
  - Ablauf des Passworts. Das Ablaufen des Passworts gilt nur für neue Accounts.

4.7.3 Der Benutzer ändert das Passwort selbst

Die Schnittstelle für die Änderung von Passwörtern wird von der Applikation Sitzungsverwaltung der Zugangsverwaltung zur Verfügung gestellt.

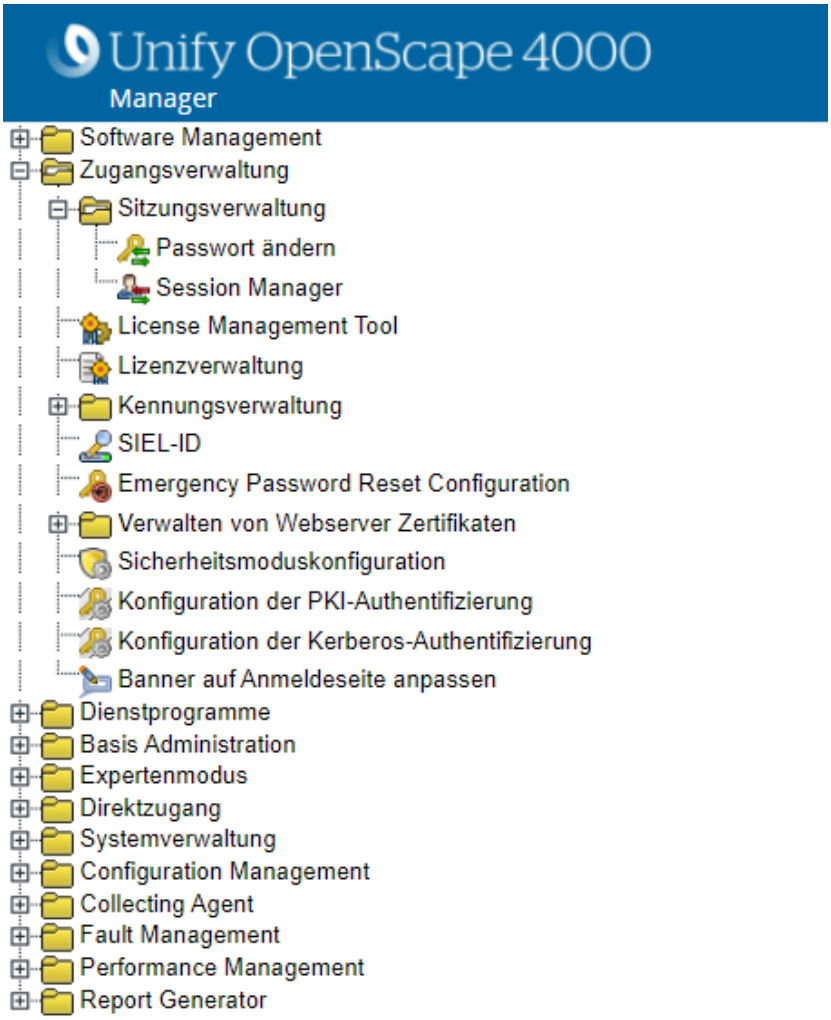


Abbildung 53: Die Applikation "Passwort ändern>in der Sitzungsverwaltung starten

Abbildung 54: Die Applikation "Passwort ändern"

4.8 Verbindungstest an OpenScape/HiPath 4000-Anlagen

Wenn alle Verbindungen installiert und die verwalteten Anlagen in der Systemverwaltung eingerichtet worden sind, sollten Sie die physischen Verbindungen zu allen Anlagen testen.

4.8.1 Assistant-Verbindungen bei Single Sign-On

Um die Verfügbarkeit des Assistant mittels Single Sign On zu testen, führen Sie die folgenden Schritte aus:

1) Klicken Sie im OpenScape 4000 Manager-Launchpad unter Direktzugang auf OpenScape 4000.

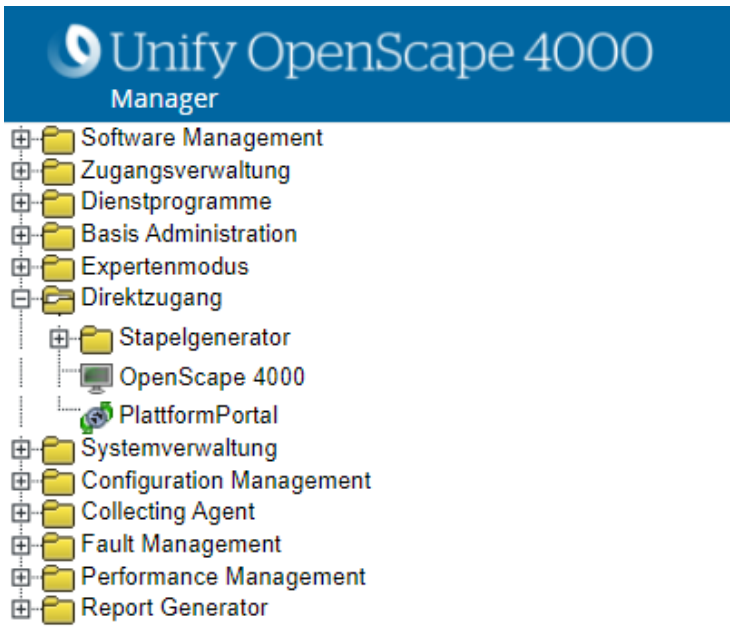


Abbildung 55: Zugriff auf OpenScape 4000 Assistant testen

2) Wählen Sie die zu testende Anlage gegebenenfalls in der Liste der Direktzugang-Benutzeroberfläche aus.

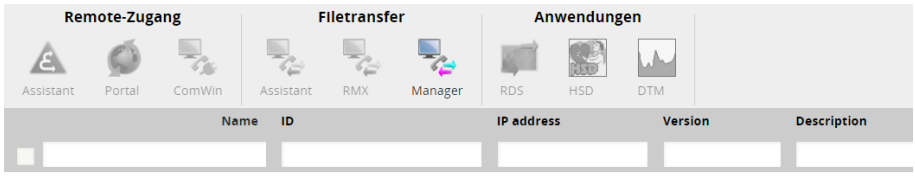


Abbildung 56: Benutzeroberfläche "Direktzugang"

3) Klicken Sie auf das Assistant-Symbol im Feld Remote Access.

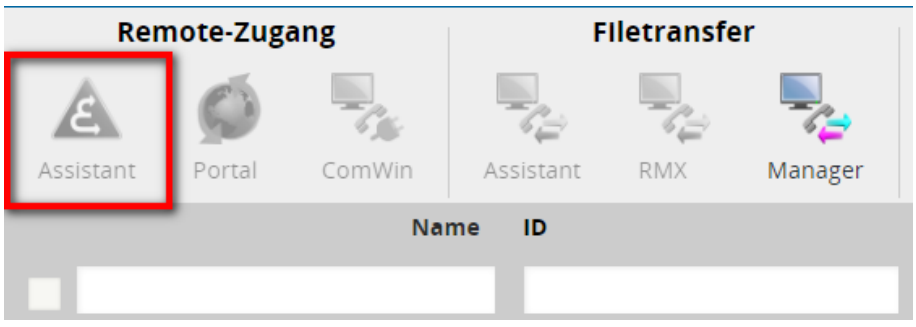


Abbildung 57: Direktzugang: Assistant-Symbol

4) Wenn das OpenScape 4000 Assistant-Launchpad der ausgewählten OpenScape/HiPath 4000-Anlage erscheint, steht die Verbindung zum Assistant und das Single Sign-On funktioniert ordnungsgemäß.

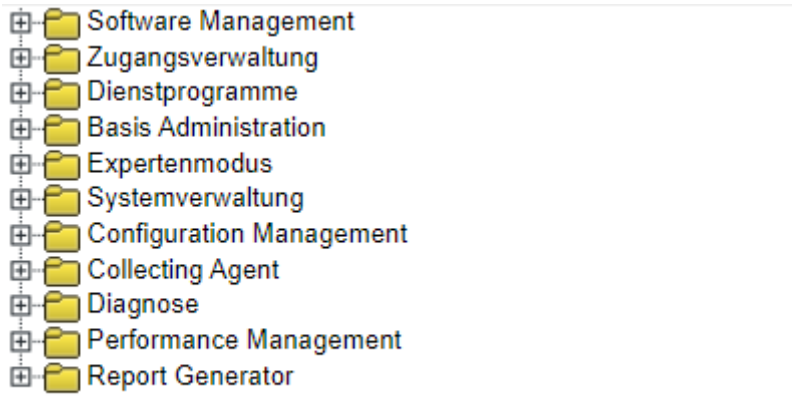


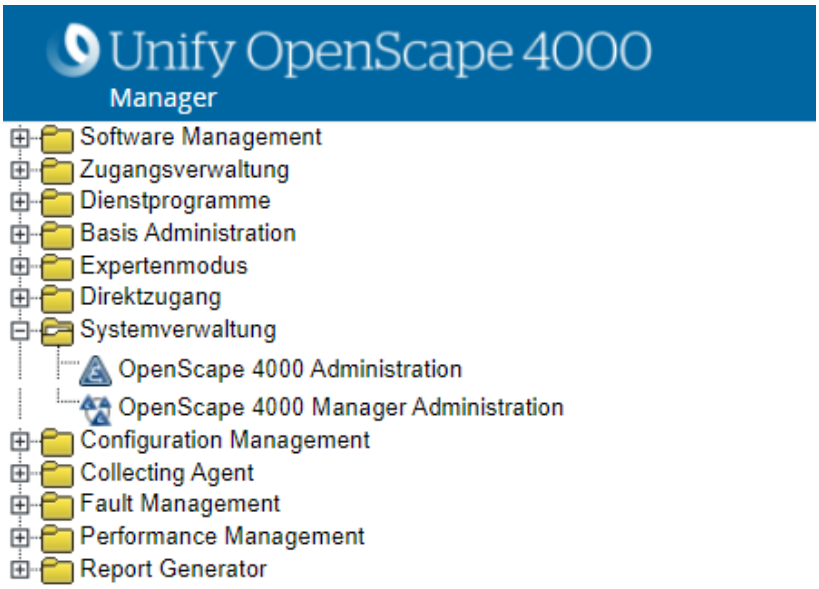
Abbildung 58: Launchpad einer ausgewählten OpenScape/HiPath 4000-Anlage

5) Wiederholen Sie die zuvor beschriebenen Schritte für alle von OpenScape 4000 Manager verwalteten OpenScape/HiPath 4000-Anlagen.

4.8.2 AMO-Konnektivität an OpenScape/HiPath 4000-Anlagen testen

Um zu testen, ob AMO-Stapelaufträge an der angeschlossenen OpenScape/HiPath 4000 ausgeführt werden können, führen Sie die folgenden Schritte aus:

1) Öffnen Sie Systemverwaltung --> OpenScape 4000 Administration.



2) Klicken Sie auf die Schaltfläche Suchen, um alle angeschlossenen Anlagen zu suchen.
3) Wechseln Sie mithilfe des Optionsfelds am oberen Bildschirmrand die Ansicht zu Objekt.
4) Jetzt können Sie mithilfe der Pfeile am unteren Bildschirmrand durch die konfigurierten Systeme navigieren.

5) Für jede der Anlagen wird im Feld Kommunikationsstatus (Communication Status) Unbekannt (Unknown) angezeigt; Sie können den Kommunikationsstatus über die Schaltfläche Status prüfen (Check Status) überprüfen.
6) Die Meldung "Kommunikation ist OK>wird angezeigt, wenn der Zugriff auf die AMO-Schnittstelle möglich.
7) Ansonsten erscheint eine entsprechende Fehlermeldung:
8) Der Kommunikationsstatus "Kommunikation unvollständig (Communication Incomplete)>wird angezeigt.

Anmerkung: Das Feld "Kommunikationsstatus>wird nicht mehr in der Datenbank gespeichert und demzufolge bei jeder Neuanzeige des Objekts gelöscht.

4.9 OpenScape 4000 Manager- und Assistant-Anwendungsfälle

Dieser Abschnitt erklärt die Funktionen und gegenseitigen Beeinflussungen, die dann auftreten, wenn AMOs und der OpenScape 4000 Manager bzw. der OpenScape 4000 Assistant gleichzeitig für die Konfiguration von Anlagen verwendet werden. Der Leser erhält alle nötigen Informationen in Form von Antworten auf häufig gestellte Fragen (FAQ).

Abschnitt 4.10.1, "Netze mit OpenScape 4000 Manager" behandelt die Konfiguration von Netzen mit Hilfe von AMOs, dem OpenScape 4000 Assistant und dem OpenScape 4000 Manager.

Abschnitt 4.10.2, "Netze ohne OpenScape 4000 Manager" behandelt die Konfiguration von Netzen mit Hilfe von AMOs und dem OpenScape 4000 Assistant, ohne den OpenScape 4000 Manager.

4.9.1 Netze mit OpenScape 4000 Manager

Allgemeine Anwendungsregel: Wenn der Kunde über ein Netz mit OpenScape 4000 Manager verfügt, dann sollte er zur Konfiguration der Anlagen immer nur den Manager verwenden. Die Verwendung von direkten AMO-Befehlen könnte in Netzen, in denen sowohl der OpenScape 4000 Assistant **als auch** der OpenScape 4000 Manager läuft, zu Datenbank-Inkonsistenzen führen.

4.9.1.1 Was geschieht, wenn ich zur Änderung der Anlagenkonfiguration nicht den OpenScape 4000 Manager sondern AMO-Befehle verwenden?

Es gibt keinen Mechanismus, um dem Manager davon zu unterrichten, dass die Anlagen-Datenbank mittels AMO-Befehl geändert wurde. Das bedeutet, dass unmittelbar nach Ausführung des AMO-Befehls die Manager-Datenbank und die Anlagen-Datenbank nicht mehr synchron zueinander sind.

4.9.1.2 Wie kann ich feststellen, ob die Manager-Datenbank synchron zur Anlage ist?

Am Manager selbst gibt es keine Vorrichtung, die anzeigen würde, dass die Manager-Datenbank synchron ist. Auch wenn auf der Anlage ein AMO-Befehl ausführt wird, meldet der Manager, dass seine Datenbank zur Anlage synchron ist.

4.9.1.3 Wie kann ich nach Ausführung eines AMO-Befehls den Manager und die Anlagen-Datenbank miteinander synchronisieren?

Starten Sie einen manuellen Delta-Upload am Bildschirm der Anlage (siehe Abschnitt 4.5.3.1, "OpenScape/HiPath 4000 hochladen"). Falls Sie keinen manuellen Delta-Upload durchführen, wird standardmäßig jeden Abend um 22:00 Uhr automatisch ein Delta-Upload zur Synchronisierung der Datenbanken durchgeführt (siehe Abschnitt 4.5.3.2, "Periodische Uploads für OpenScape/HiPath 4000 planen").

4.9.1.4 Was passiert, wenn nach Ausführung eines AMO-Befehls und vor Durchführung eines Delta-Upload am Manager versuche, die Datenbanken zu synchronisieren?

Wenn Sie mit Hilfe des Managers eines der durch den gerade ausgeführten AMO-Befehl betroffenen Objekte ändern, erhalten Sie möglicherweise Fehlermeldungen falschen Inhalts oder sogar nicht zutreffende Fehlermeldungen. Dies ist darauf zurückzuführen, dass der Manager jeden Befehl vor seiner Ausführung auf Gültigkeit prüft. Wenn die Manager-Datenbank mit der Anlagen-Datenbank nicht synchron ist, führt die Gültigkeitsprüfung eventuell zu unverlässlichen Ergebnissen.

Beispiel:

Wenn Sie einen Teilnehmer mit LOE-SBCSU löschen und direkt im Anschluss daran am Manager versuchen, einen Teilnehmer mit derselben Nummer einzurichten, meldet der Manager, dass diese Teilnehmernummer bereits benutzt wird (da der Teilnehmer schon in der Manager-Datenbank existiert).

4.9.1.5 Wird die Leistung des Managers durch die Ausführung von AMO-Befehlen auf der Anlage negativ beeinträchtigt?

Im Prinzip ja, aber aus Anwendersicht nur unmerklich. Der Manager verwendet zwar wie der Assistant AMO-Befehle zur Änderung der Anlagenkonfiguration, aber im Gegensatz zum Assistant schickt der Manager diese Befehle im Hintergrund an die Anlage. In der Praxis bedeutet dies, dass der Manager beim Senden der AMO-Befehle an die Anlage nicht völlig blockiert ist. Möglicherweise muss der Manager-Benutzer etwas länger als gewohnt auf die Antwort der Anlage warten (da diese mit der Abarbeitung von anderen AMO-Befehlen beschäftigt ist), aber er kann mit der Bearbeitung von anderen Aufgaben weitermachen.

4.9.1.6 Was passiert, wenn ich den Assistant verwende, um Konfigurationsänderungen durchzuführen?

Auch der Assistant verwendet AMO-Befehle, um die Anlagenkonfiguration zu ändern. Es gelten also all die o.g. Fälle: die Manager-Datenbank wird nicht mehr mit der Anlage synchron sein (siehe Abschnitt 4.10.1.1 bis 4.10.1.4); ausserdem kann es auch zu Leistungseinbußen beim Manager kommen (Section 4.10.1.5).

4.9.1.7 Ich muss eine grosse AMO-Stapelbefehlsdatei ausführen, um die Kundenkonfiguration zu aktualisieren. Dieser Kunde hat einen OpenScape Manager. Wie muss ich vorgehen?

Bitte führen Sie am Manager während der Abarbeitung der AMO-Stapeldatei keine anderen Tätigkeiten aus. Nach Abarbeitung der AMO-Stapeldatei sollten Sie ein Delta-Upload vom Manager durchführen (nur für die betroffene(n) Anlage(n), nicht für das gesamte Netz). Wenn Sie den Assistant verwenden müssen, sollten Sie warten, bis der Manager das Delta-Upload beendet hat, und anschliessend ein Upload vom Assistant starten. (Das Assistant-Upload kann einige Zeit dauern. Sie sollten lieber auf das allabendliche automatisch Upload warten.).

4.9.1.8 Wenn die Manager-Datenbank nicht mit der Anlage synchron ist und ich dennoch versuche mit dem Manager die Anlagenkonfiguration zu verändern, kann dies zur Korruption der Anlagen-Datenbank kommen (da der Manager eventuell versucht, einen ungültigen Befehl auszuführen)?

Nein. Die Anlage prüft alle Konfigurationsänderungen immer auf Gültigkeit (unabhängig von dem diese Änderungen durchgeführt wurden: AMO, Manager oder Assistant) und weist ungültige Anfragen zurück. Selbst dann, wenn der Manager die Durchführung eines ungültigen Befehls erlaubt (weil die Manager-Datenbank, nicht über gültige Daten zur Prüfung des Befehls verfügt; siehe Section 4.10.1.4), fängt die Anlage diesen Befehl ab und gibt eine entsprechende Fehlermeldung aus.

4.9.1.9 Was geschieht mit der Assistant-Datenbank, wenn jemand mit Hilfe des Manager eine Konfigurationsänderung durchführt?

Der Assistant wird davon unterrichtet, dass AMO-Befehle ausgeführt wurden (der Manager schickt AMO-Befehle an die Anlagen) und aktualisiert seine Datenbank dementsprechend. Einzelheiten zur Funktionsweise des Benachrichtigungsverfahrens finden Sie im Kapitel "Benachrichtigungsverfahren und Anwendungsfälle>im OpenScape 4000 Servicehandbuch.

4.9.1.10 Wirkt der Benachrichtigungsprozess sich negativ auf die Leistung des Manager aus?

Im Prinzip ja, aber aus Sicht des Manager-Benutzers nur unmerklich. Der Manager generiert AMO-Befehle, um die Anlagenkonfiguration zu ändern. Der Assistant verwendet auch AMO-Befehle, um seine Datenbank zu synchronisieren. Da die Anlage zu jedem beliebigen Zeitpunkt immer nur einen AMO-Befehl ausführen kann, werden AMO-Befehle vom Manager zunächst in die Warteschlange eingereiht, wenn der Assistant gerade seine Datenbank synchronisiert. In der Praxis bedeutet dies jedoch, dass der Manager beim Senden der AMO-Befehle an die Anlage nicht völlig blockiert ist. Möglicherweise muss der Manager etwas länger auf die Antwort der Anlage warten, aber der Benutzer kann dennoch mit der Bearbeitung von anderen Aufgaben weitermachen. Siehe auch Section 4.10.1.5.

4.9.1.11 Gibt es einen Mechanismus zur Synchronisierung der Manager-Datenbank für den Fall, dass jemand die Anlagen-Datenbank ändert? (In einem solchen Fall würde der Manager nicht sofort benachrichtigt)

Ja. Jeden abend (um 22:00 Uhr bei der Standardkonfiguration) synchronisiert der Manager seine Datenbank mit der Datenbank der mit ihm verbundenen Anlagen. Er verwendet dazu das sog. Delta-Upload-Verfahren, bei dem von der Anlage nur diejenigen Datenbankänderungen heruntergeladen werden, die seit dem letzten Upload durchgeführt wurden. Bei ruhigen Systemen, d.h. wenn zwischen 22:00 Uhr und dem nächsten Morgen nur wenige Vorgänge bearbeitet werden müssen, sollte die Manager-Datenbank morgens immer synchron zur Anlagen-Datenbank sein.

4.9.2 Netze ohne OpenScape 4000 Manager

Allgemeine Anwendungsregel:

Wenn der Kunde keinen OpenScape 4000 Manager hat, sollten Sie Konfigurationsänderungen immer über den Assistant durchführen, d.h. nicht über direkte AMO-Befehle.

Die Antworten zu den unten aufgeführten Häufig gestellten Fragen (FAQ) sowie Einzelheiten zum Benachrichtigungsprozess (Synchronisierungsprozess zwischen Assistant-Datenbank und Anlagen-Datenbank) finden Sie im Kapitel "Benachrichtigungsverfahren und Anwendungsfälle>im OpenScape 4000 Servicehandbuch.

- Was geschieht, wenn ich zur Änderung der Anlagenkonfiguration nicht den OpenScape 4000 Assistant sondern AMO-Befehle verwende?

- Wie lange dauert die Aktualisierung der Assistant-Datenbank bei Ausführung eines AMO-Befehls?

- Welche Anzeige erscheint auf dem Assistant-Display bis die (Informix-)Datenbank aktualisiert ist?

- Informiert der Assistant die Anwender davon, dass seine Datenbank aktualisiert wurde?

- Wirkt der Benachrichtigungsprozess sich negativ auf die Leistung des Assistant aus?

- Verlangsamt der Benachrichtigungsprozess die Ausführung von direkten AMO-Befehlen?

- Was geschieht, wenn ich viele AMO-Befehle in einem kurzen Zeitraum absetze, z.B. in Form einer AMO-Stapelbefehlsdatei?

- Ich muss eine grosse AMO-Stapelbefehlsdatei ausführen, um die Kundenkonfiguration zu aktualisieren. Wie muss ich vorgehen?

- Gibt es einen Automatismus zur Synchronisierung der Assistant-Datenbank, wenn diese einmal "asynchron>ist?

5 Bedienung und Wartung des OpenScape 4000 Manager-Servers

Dieses Kapitel enthält Anleitungen zur Bedienung und Wartung des OpenScape 4000 Manager-Servers.

5.1 Manager-Uhr

Die Manager-Uhr wird vom Platform Linux Host gesteuert. Es gibt keine Möglichkeit, einen externen NTP-Server zu konfigurieren oder den Manager als Zeitquelle für ein anderes System in Webmin zu konfigurieren. Der NTP-Server für die Plattform wird auf die gleiche Weise wie für den Assistenten während der Systeminstallation konfiguriert (d.h. die XML-Konfigurationsdatei firstinstall).

5.2 Server neu starten

Anmerkung: Für das hier beschriebene Verfahren müssen Sie sich als rsca oder auf einer höheren Benutzerebene anmelden. Bevor Sie mit den nachfolgenden Schritten fortfahren, sollten Sie eine Rundsendenachricht an alle angemeldeten Benutzer übermitteln und darauf hinweisen, dass der Server neu gestartet wird.

Um einen Server-Neustart über den OpenScape 4000 Manager zu aktivieren:

1) Rufen Sie das OpenScape 4000 Manager Launchpad auf und klicken Sie hier auf Basis Administration.
2) Klicken Sie auf Webmin Base Admin.

Abbildung 59: Webmin Base Admin in Basis Administration aufrufen

3) Klicken Sie unter **Systemverwaltung** auf Neu starten / Herunterfahren, um den entsprechenden Bildschirm aufzurufen.

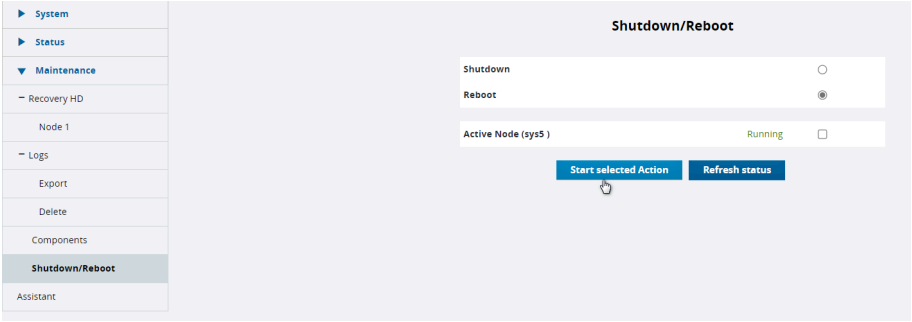


Abbildung 60: Bildschirm "New starten und Herunterfahren"

4) Wählen Sie die erste Option: Manager neu starten.

5.3 Herunterfahren des Betriebssystems

Um den Server ordnungsgemäß herunterzufahren, gehen Sie wie in diesem Abschnitt beschrieben vor.

Anmerkung:

Die in diesem Abschnitt beschriebenen Verfahren sind erforderlich, wenn der Server heruntergefahren wird und insbesondere, wenn Hardware im Server hinzugefügt, entfernt oder ausgetauscht werden soll. Durch die Durchführung dieser Verfahren werden Produktausfälle minimiert.

Schalten Sie das System nicht aus, ohne diese Verfahren zu befolgen. Das Dateisystem kann beschädigt sein, was eine Neuinstallation des Betriebssystems und der Anwendungen erfordert.

Schalten Sie den Server nicht aus oder fahren Sie ihn nicht herunter, während andere Benutzer am OpenScape 4000 Manager angemeldet sind (eine Liste der angemeldeten Benutzer finden Sie unter Session Manager im Abschnitt Session Manager des Launchpad-Baums), während Sie Verschiebungen und Änderungen vornehmen oder die Systemadministration durchführen. Dadurch kann die Datenbank des OpenScape 4000 Managers beschädigt werden.

So fahren Sie das Betriebssystem über den OpenScape 4000 Manager herunter:

1) Klicken Sie im OpenScape 4000 Manager Launchpad auf **Direct Acess**.
2) Klicken Sie auf **Platform Portal** (siehe Abbildung 89 auf Seite 170).
3) Klicken Sie unter **Systemadministration** auf Reboot/Shutdown, um den Bildschirm Reboot and Shutdown anzuzeigen (siehe Abbildung 90 auf Seite 171).
4) Wählen Sie die Option und klicken sie im **Start Selected Action**.
5) Bestätigen Sie auf die angezeigte Warnmeldung hin noch einmal das Ausschalten.

5.4 Software-Aktualisierungen über SWM/SWA

Software-Aktualisierungen in Form von Minor, Fix oder HotFix Releases für den OpenScape 4000 Manager können mithilfe der Software-Management-Applikationen Software Transfer (SWM) und Software Aktivierung (SWA) abgewickelt werden.

SWM ermöglicht die Übermittlung von Software-Aktualisierungen, die anschließend mit Hilfe von SWA aktiviert werden. Der Zugriff auf diese beiden Applikationen erfolgt über das Launchpad.

Falls Probleme mit einem HotFix auftreten, kann dieser mithilfe des Leistungsmerkmals "SWA Hotfix Deaktivierung>deaktiviert werden.

Anmerkung: Weiterführende Informationen und Anleitungen für den Einsatz von SWM und SWA finden Sie in der Online-Hilfe zu diesen Applikationen.

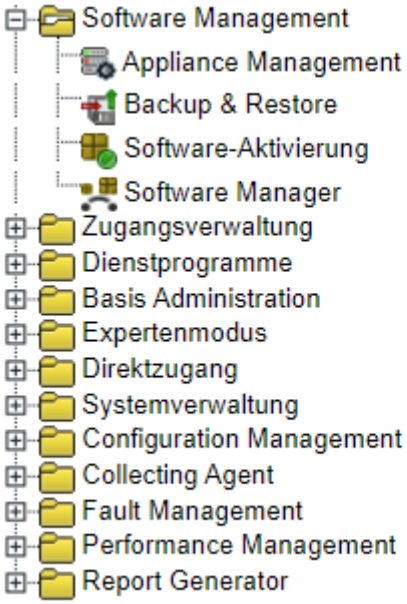


Abbildung 61: Softwaretransfer/Software-Aktivierung in Software Management aufrufen

5.5 Backup und Wiederherstellung von Daten mit OpenScape 4000 Manager

Dieser Abschnitt beschreibt die Backup & Restore-Funktionalität in OpenScape 4000 Manager sowie eine Rückfalllösung nach einem eventuell fehlgeschlagenen Upgrade von OpenScape 4000 Manager.

5.5.1 Durchführen eines Datenbank-Backups

Um eine Sicherungskopie (Backup) der Applikationsdatenbank am OpenScape 4000 Manager-Server zu erstellen:

1) Klicken Sie im OpenScape 4000 Manager Launchpad auf Software Management.
2) Klicken Sie auf Backup & Restore, um die Startseite "Backup & Restore>aufzurufen.

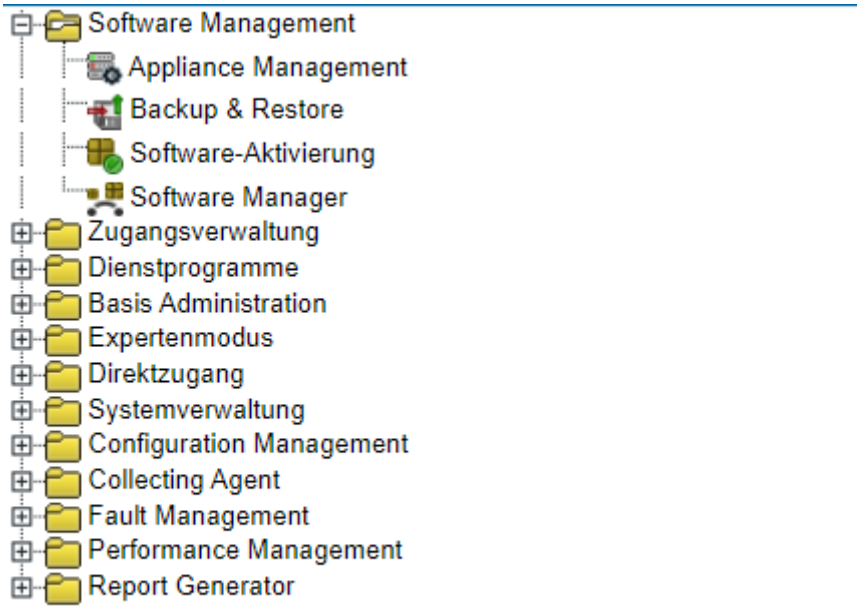


Abbildung 62: Backup & Restore in Software Management aufrufen

Abbildung 63: Startseite "Backup & Restore"

3) Klicken Sie auf Backup, um die Parameter für diese Backup-Prozedur zu vereinbaren. Weitere Informationen und Anleitungen finden Sie in der Online-Hilfe.

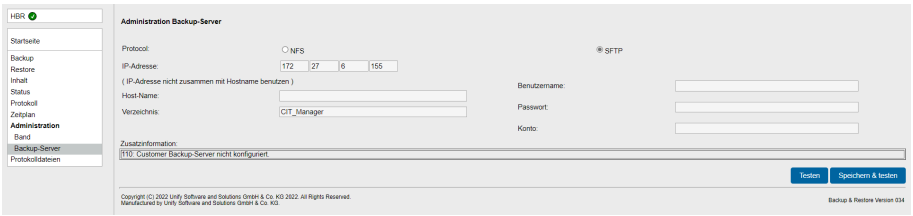


Abbildung 64: Backup-Server definieren

4) Klicken Sie auf Backup, um die Parameter für diese Backup-Prozedur zu vereinbaren (siehe Bild 99). Weitere Informationen und Anleitungen finden Sie in der Online-Hilfe.

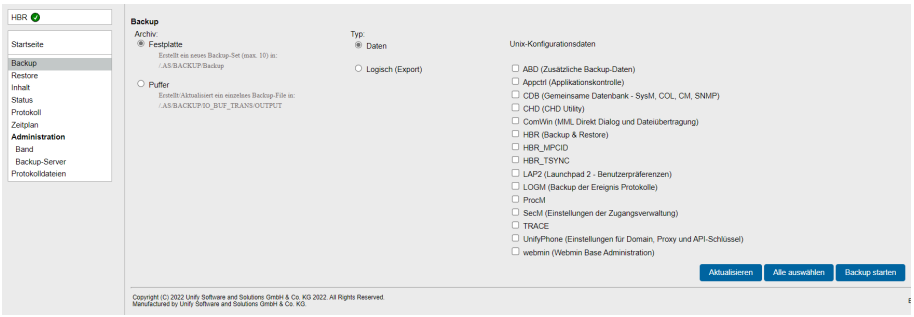


Abbildung 65: Backup-Parameter auswählen

5) Klicken Sie auf Backup starten, um den Backup-Prozess zu starten.

Anmerkung: Der aktuelle Status dieser Prozedur kann jederzeit über die Position Status im Menü "Backup & Restore>abgerufen werden.

5.5.2 Wiederherstellen archivierter Daten

Um die Daten eines Backup-Archivs wiederherzustellen:

1) Klicken Sie im OpenScape 4000 Manager Launchpad auf Software Management.
2) Klicken Sie auf Backup & Restore, um die Startseite "Backup & Restore>aufzurufen.
3) Klicken Sie im "Backup & Restore"-Menü (links) auf Restore.

Abbildung 66: Backup-Sets für die Wiederherstellung auflisten

4) Vereinbaren Sie im Bildschirm Restore die Parameter für die Wiederherstellung. Weitere Informationen und Anleitungen finden Sie in der Online-Hilfe.
5) Klicken Sie auf Liste, um eine Liste aller verfügbaren Backup-Sets abzurufen.
6) Wählen Sie ein geeignetes Backup-Set.
7) Bestätigen Sie Ihre Auswahl, um den Wiederherstellungsprozess zu starten.

Anmerkung: Der aktuelle Status dieser Prozedur kann jederzeit über die Position Status im Menü "Backup & Restore>abgerufen werden.

Das Einspielen einer Sicherungskopie als Wiederherstellungstool für OpenScape 4000 Manager/Assistant ist nur für dieselbe (identische) HW und dieselbe SW-Version freigegeben, von der sie erstellt wurde. Eine anderweitige Verwendung auf einer anderen HW oder unter einer anderen SW-Version kann zu Fehlern bei der Wiederherstellung der Daten führen. Verwenden Sie in anderen Fällen die für die Wiederherstellung von Daten zwischen verschiedener Hardware und verschiedenen Versionen zertifizierte logische Backup & Restore-Lösung.

5.6 Lizenzen des OpenScape 4000 Manager-Servers verwalten

5.6.1 Lizenzverwaltung bei OpenScape 4000 Manager

Mit der Applikation Lizenzverwaltung können Sie Informationen über die installierten Lizenzen und über den Customer License Agent (CLA) anzeigen. Außerdem können Sie den Ort des Customer License Agent (IP-Adresse oder DNS-Name) konfigurieren.

So rufen Sie die Applikation Lizenzverwaltung auf:

1) Melden Sie sich am OpenScape 4000 Manager als rsca oder auf einer höheren Benutzerebene an (Informationen zu den Sicherheitsstufen der Zugangsverwaltung finden Sie in Tabelle 4 auf Seite 157).

2) Klicken Sie im Launchpad auf Zugangsverwaltung und anschließend auf **Lizenzverwaltung** (siehe Bild 101). Anschließend wird die Lizenzverwaltungs-Startseite geöffnet (siehe Bild 102).

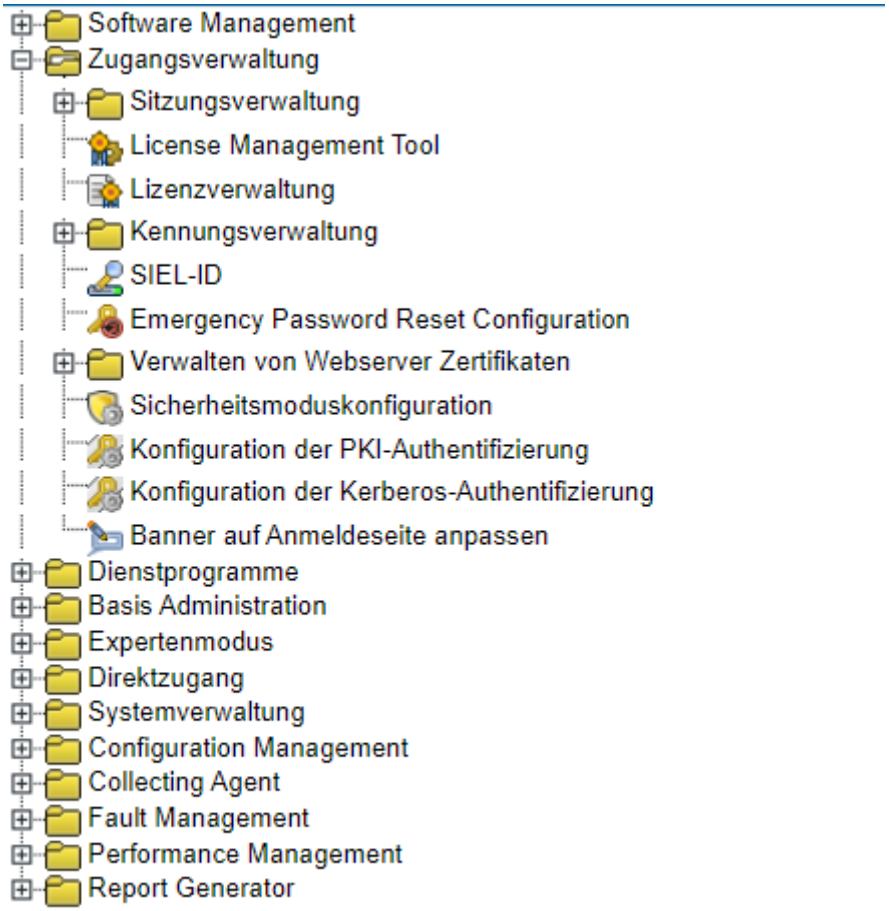


Abbildung 67: Lizenzverwaltung aufrufen

Abbildung 68: Startseite "Lizenzverwaltung"

5.6.2 Abrufen des Lizenzschlüssels für den OpenScape 4000 Manager-Server

Ein Lizenzschlüssel wird benötigt, um den OpenScape 4000 Manager in Betrieb nehmen zu können. Der Lizenzschlüssel beinhaltet verschlüsselte Informationen zur Konfiguration der Ports sowie sonstige Angaben, die für eine

Aktivierung der erworbenen Applikationen erforderlich sind. Der Lizenzschlüssel wird abgerufen, indem über eine Web-gestützte Schnittstelle eine Internet-Verbindung zum Lizenzserver hergestellt wird.

Anmerkung: Die hier beschriebene Prozedur kann sich bedingt durch Anpassungen an Service Agreement Policy (SAP)-Anforderungen oder aufgrund einer Harmonisierung mit den Lizenzierungsprozeduren für andere Produkte ändern. Sollte dies der Fall sein, werden entsprechende Anweisungen in Form einer Online-Hilfe auf dem Lizenzserver bereitgestellt. Einzelheiten zum Lizenzgenerierungsverfahren finden Sie auch in der Central Licence Server (CLS)-Onlinehilfe.

Anmerkung: Seit 4000 OpenScape Manager V8 sind die Lizenzen an die Advanced Locking ID (ALI) und nicht an die MAC-Adresse des Manager-Servers gebunden. Die ALI ist ein für den Lizenzkauf erforderlicher Schlüssel. Der ALI-Schlüssel wird im Manager-Dashboard angezeigt.

5.7 Expertenzugang vom OpenScape 4000 Manager-Server herunterladen

Um den Expertenzugang vom OpenScape 4000 Manager-Server herunterzuladen und zu installieren:

1) Klicken Sie im OpenScape 4000 Manager Launchpad auf Direktzugang und anschließend auf OpenScape 4000.

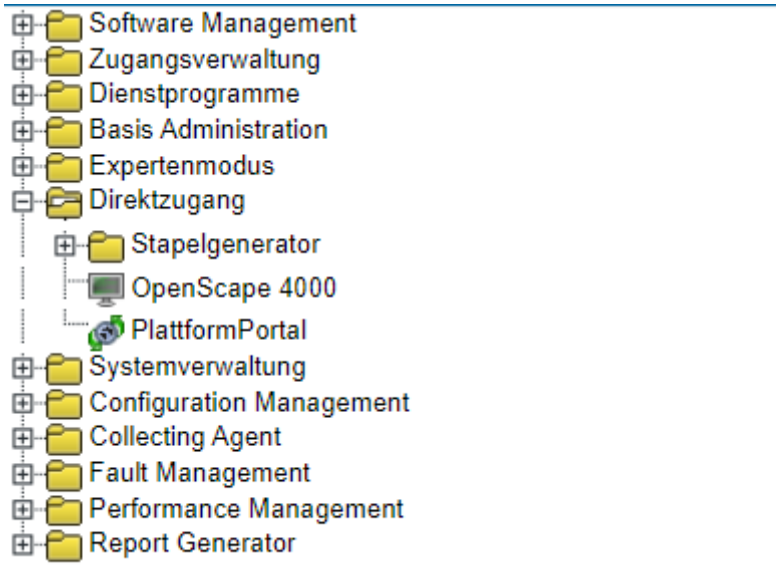


Abbildung 69: Expertenzugang vom OpenScape 4000 Manager-Server installieren (Direktzugang)

2) Im Menü auf der rechten Seite des Expert Access-Fensters können Sie die Installationsdatei über ComWin Expert Access herunterladen.

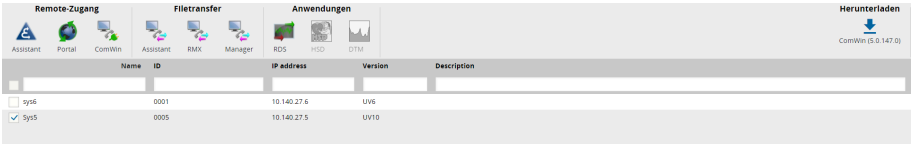


Abbildung 70: Expert Access Client-Installation starten

3) Laden Sie die Installationsdatei herunter und befolgen Sie die Bildschirmanweisungen für die Durchführung der Expert Access Client-Installation.

5.8 Verwenden des virtuellen Rufnummernplans (VNR)

Das Leistungsmerkmal VNR ermöglicht das Definieren identischer und ähnlicher Rufnummern auf einem physikalischen Knoten.

5.8.1 Allgemeines Konzept

In diesem Abschnitt soll anhand einiger Konzepte des Configuration Management verdeutlicht werden, warum und wie bestimmte Dinge an die Anforderungen eines virtuellen Rufnummernplans angepasst wurden.

Bisheriges Domain-, Anlagen- und Routing-Konzept

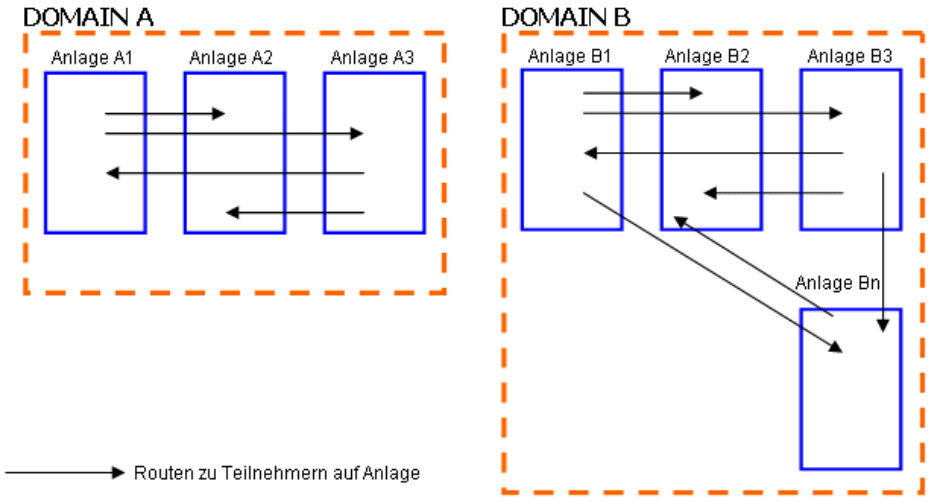


Abbildung 71: Domain-, Anlagen- und Routing-Konzept

Beim aktuellen Domain-Konzept kann eine Anlage nur in einer Domain existieren, und Domains bestehen aus physikalischen Knoten (Anlagen). Routing-Vorgänge werden nur innerhalb einer Domain gehandhabt. Wird beispielsweise ein Teilnehmer aus Anlage A1 in Bild 2 gelöscht (bzw. dazu hinzugefügt), sind hiervon nur die Anlagen in Domain A (A2, A3) betroffen, und ihre Routen werden dementsprechend aktualisiert. Die Routen-Handhabung in Domain B ist hiervon nicht betroffen.

VNR-Konzept

Das Leistungsmerkmal VNR ermöglicht das Definieren identischer und ähnlicher Rufnummern auf einem physikalischen Knoten auf verschiedenen virtuellen Knoten. Bei diesem Leistungsmerkmal werden Nebenstellen in ihrer langen Schreibweise mit bis zu maximal 12 Ziffern verwendet (6-stellige virtuelle Knotenkennzahl + 6-stellige kurze Nebenstellennummer).

Hier reicht es nicht aus, das Routing zu einem bestimmten Teilnehmer nur mithilfe des Richtungsindex (ZLNR) und der Nebenstellennummer zu definieren.

Wie im folgenden Bild zu sehen, sind drei verschiedene Parameter erforderlich, wenn ein Teilnehmer auf PN A3 VN2 einen Teilnehmer auf PN A1 anrufen möchte.

(Hinweis: physikalischer Knoten = physikalisches System)

- Richtungsindex (ZLNR) zur Auffindung des richtigen physikalischen Knotens (**PN**) in der Domain
- Virtuelle Knotenkennzahl (VNAC) zur Auffindung des richtigen virtuellen Knotens (**VN**) auf dem physikalischen Knoten
- Teilnehmernummer

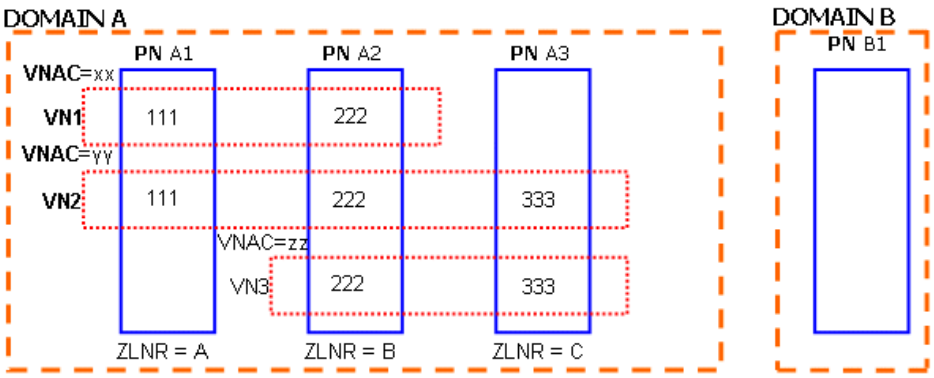


Abbildung 72: VNR-Netzwerk

Routing-Probleme bei gemischten Netzwerken (mit und ohne VNR)

VNR-Anlagen verfügen über die Routing-Informationen mit allen drei Parametern (PN = (ZLNR), VNAC und Teilnehmernummer (= lange Nebenstellennummer); für Anlagen ohne VNR gilt dies nicht.

Bei Anlagen ohne VNR sind die virtuellen Knoteninformationen nicht für das Routing verfügbar, da sie kurze Nebenstellennummern verwenden. Dies führt zu dem nachfolgend beschriebenen Problem, wo es auf der VNR-Anlage PN A2 drei verschiedene Teilnehmer mit der Nummer 222 gibt. Ruft ein Teilnehmer von der Anlage ohne VNR **PN A3** die Nummer 222 an, ist nicht klar, welcher 222 auf der **PN A2** dieser Ruf gilt, da die virtuellen Knoteninformationen fehlen. Folglich ist in diesem Szenario kein ordnungsgemäßes Routing möglich, da die Teilnehmernummer (kurz) und der Richtungsindex nicht ausreichen. Aus diesem Grund erfordern gemischte Netzwerke eine spezielle Routing-Konfiguration.

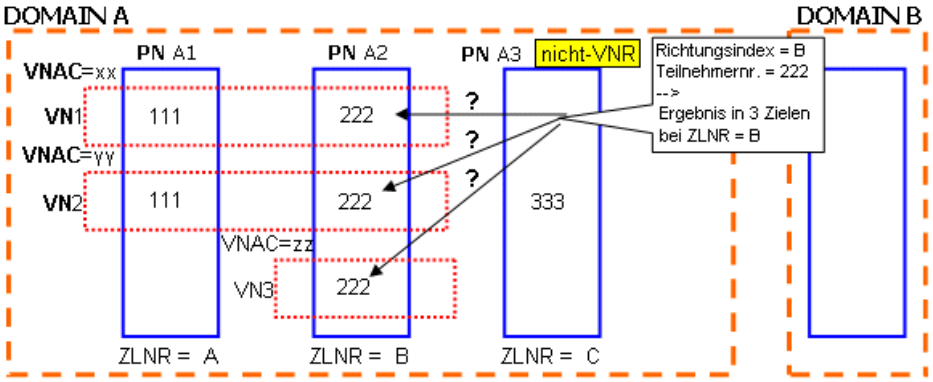
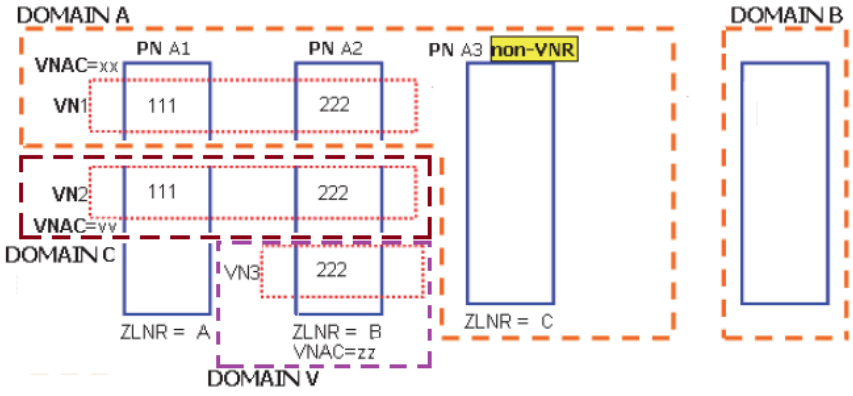


Abbildung 73: Routing-Problem bei gemischten Netzwerken

Betrieb einer VNR-Anlage in mehreren Domains

Die oben beschriebenen Einschränkungen mit gemischten Anlagen (mit und ohne VNR) haben zu dem im nächsten Bild dargestellten Entwurf geführt. In diesem Bild ist zu sehen, dass mehrere Anlagen ohne VNR und **eine einzelne VNR-Anlage** in derselben Domain genutzt werden. Die Kästchen mit ZLNRn stellen die Anlagen ohne VNR dar. Entsprechend diesem Szenario kann eine Anlage mehrere virtuelle Knoten in verschiedenen Domains haben. In einer Domain ist ein virtueller Knoten (eine Unteranlage) definiert. Unteranlagen verschiedener VNR-PN können in derselben Domain existieren, allerdings müssen sie dieselbe virtuelle Knoten-ID und dieselbe virtuelle Knotenkennzahl haben. Diese Voraussetzung (identische virtuelle Knoten-ID und identische virtuelle Knotenkennzahl) entfällt bei Anlagen ohne VNR. Eine weitere Voraussetzung ist, dass alle virtuellen Knoten auf einer physikalischen Anlage unterschiedliche ZLNRn haben.

Diese Konfiguration kann nun (ab V4) dank der neuen Möglichkeit, mithilfe des virtuellen Knotens einen physikalischen Knoten in verschiedene **Unteranlagen** zu zerlegen und diese Unteranlagen in verschiedenen Domains zu konfigurieren, realisiert werden.



Vor Release V4 konnte eine Anlage nicht in mehr als einer Domain existieren, und es war auch nicht möglich, virtuelle Knoten als Elemente einer Domain zu definieren (nur Anlagen, also physikalische Knoten, konnten in einer Domain definiert werden).

5.8.2 Einführung des Unteranlagen-Konzepts

Vor der Realisierung des Leistungsmerkmals VNR gestatteten die Anlagen- und Domain-Konzepte in CM, eine Anlage (als einen physikalischen Knoten) nur in einer Domain zu definieren. Es war nicht möglich, eine Anlage in mehr als einer Domain zu definieren. Vorher war es außerdem nicht möglich, einen anderen Knoten als eine physikalische Anlage innerhalb einer Domain zu definieren.

Um eine Anlage definieren zu können, die in mehr als einer Domain gleichzeitig existieren kann, wurde das "**Unteranlagen**"-Konzept für VNR-Anlagen eingeführt.

Unteranlagen sind innerhalb einer VNR-Anlage erstellte virtuelle Anlagen, die durch virtuelle Knoten voneinander getrennt sind. Da sie sich nach der CM-Logik nicht von physikalischen Anlagen unterscheiden, werden sie von CM genauso behandelt. Allerdings werden Unteranlagen nur von CM wie normale Anlagen behandelt; von der Außenwelt wird die VNR-Anlage weiterhin als gewöhnliche Anlage mit virtuellen Knoten behandelt, und Unteranlagen werden maskiert.

Abbildung 74: Definition einer VNR-Anlage als mehrere Unteranlagen

Aktivieren des Attributs "Physikalisches VNR-System"

Im Configuration Management gibt es ein neues, mit dem Dialog "Systemverwaltung" verknüpftes Kontrollkästchen "Physikalisches VNR-System", das festlegt, ob ein VNR auf diesem physikalischen System verwendet wird oder nicht. Dieses Kontrollkästchen sollte nur markiert werden, wenn die hinzuzufügende Anlage eine VNR-Anlage ist.

Wird das Kontrollkästchen "Physikalisches VNR-System" auf der Registerkarte "Configuration Management>des Dialogs "Systemverwaltung>in OpenScape 4000 Administration markiert, ist es möglich, auf der Registerkarte "Unteranlagen-Daten" des Fensters "Anlage>in Configuration Management mehrere Domains auf dieser Anlage zu definieren; diese Registerkarte dient zur Definition der Beziehung zwischen Unteranlage/Domain/virtuellem Knoten und der Anlage.

Sie können das Attribut "Physikalisches VNR-System>im Bildschirm "Systemverwaltung>nur während der Hinzunahme einer neuen Anlage aktivieren. Bei einer bereits vorhandenen Anlage kann dieses Flag nicht aktualisiert werden. Nach dem Hinzufügen der Anlage kann dieses Flag nur geändert werden, wenn keine Unteranlage hinzugefügt wurde. Sobald aber mindestens eine Unteranlage hinzugefügt wurde, kann das Flag nicht mehr geändert werden.

Unteranlagen können nur auf **VNR-Anlagen** erstellt werden, und es kann nur jeweils eine Unteranlage auf einem virtuellem Knoten einer VNR-Anlage geben. Außerdem kann es auf einer Unteranlage nur jeweils einen virtuellen Knoten geben.

Mit der Einführung von Unteranlagen kann auch weiterhin die aktuelle Domain- und Anlagen-Implementierung beibehalten werden.

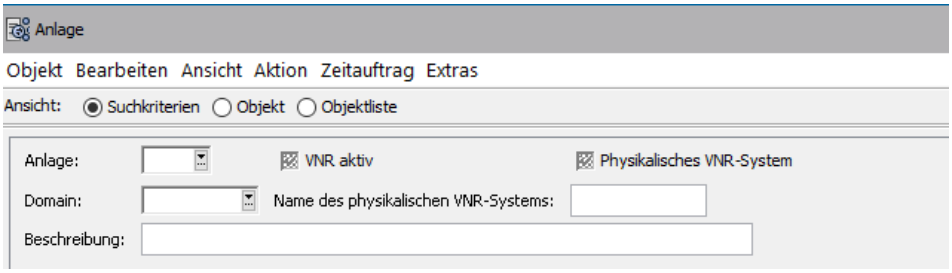


Abbildung 75: Kontrollkästchen Physikalisches VNR-System im Dialog Systemverwaltung / OpenScape 4000 Administration

Sobald die Unteranlagen erstellt sind, werden sie als physikalische Anlagen behandelt. Die nötigen Konvertierungen werden von den Komponenten erledigt, die mit der Anlage und der CDB-Datenbank kommunizieren. CM-intern gibt es *n* Unteranlagen und außerhalb von CM eine physikalische Anlage; alle nötigen Konvertierungen erfolgen automatisch, wenn die Daten empfangen bzw. gesendet werden.

Ein Upload unmittelbar nach dem Hinzufügen dieser Anlage ist erst möglich, wenn die entsprechenden Unteranlageninformationen in **Configuration Management -> Dialog "Anlage>-> Registerkarte "Unteranlagen-Daten"** eingegeben wurden.

Ist das Kontrollkästchen **Physikalisches VNR-System** nicht markiert, erscheint diese VNR-Anlage nicht auf der Registerkarte **Unteranlagen-Daten** des Fensters **Anlage** in **Configuration Management**, und der Benutzer kann auf dieser Anlage keine verschiedenen Knoten konfigurieren.

Das Kontrollkästchen **Physikalisches VNR-System** ist auch im Fenster **Anlage** in **Configuration Management** sichtbar (schreibgeschützt).

5.8.3 CM-Fenster "Anlage>- Verwaltung von Anlagen

Manche Daten sind nur für die Unteranlage von Bedeutung, während andere für die physikalische Anlage selbst gelten. Muss ein bestimmtes Attribut innerhalb des gesamten physikalischen Knotens gleich sein, handelt es sich um ein anlagenweites ("switch-wide") Attribut und kann bei dem physikalischen Knoten nur über den Dialog "Anlage" aktualisiert werden (z.B. DTB-Server-Kennzahl). Daher können über den Dialog "Anlage>einige Daten nur bei dem physikalischen Knoten aktualisiert werden, während andere Daten bei der Unteranlage aktualisiert werden können. Werden Daten bei dem physikalischen Knoten aktualisiert, wird automatisch jede Unteranlage ebenfalls mit dem neuen Wert aktualisiert. Werden jedoch Unteranlagen-bezogene Daten aktualisiert (über die Objektansicht der Unteranlage im Dialog "Anlage"), wirkt sich diese Änderung nur auf die betreffende Unteranlage aus; andere Unteranlagen werden nicht aktualisiert (z.B. Bevorzugter Richtungsindex, Land, Ortskennzahl, Amtskennzahl usw.).

Neue Unteranlagen können über die neue Registerkarte "Unteranlagen-Daten" im Dialog "Anlage>hinzugefügt werden. Es ist möglich, eine Unteranlage nur zu solchen Anlagen hinzuzufügen, deren Flag "Physikalisches VNR-System>bereits gesetzt wurde.

Es ist möglich, auch bei den hochgeladenen Anlagen Unteranlagen hinzuzufügen/zu löschen, nachdem virtuelle Knoten zu der Anlage hinzugefügt bzw. daraus gelöscht wurden.

Allerdings muss nach jedem Hinzufügen bzw. Löschen einer Unteranlage "Upload-All>zu dem physikalischen Knoten gestartet werden. Bevor Sie "Upload-All>starten, müssen die Unteranlagen-Daten zu diesem physikalischen Knoten entsprechend den virtuellen Knoteninformationen auf der Anlage aktualisiert werden (die Anzahl der Unteranlagen sollte mit der Anzahl der virtuellen Knoten auf der Anlage identisch sein, und virtuelle Knotenkennzahl und virtuelle Knoten-ID sollten übereinstimmen.)

Wenn Sie eine Unteranlage löschen möchten, ist dies über die Registerkarte "Unteranlagen-Daten>des Dialogs "Anlage" möglich (markieren Sie den gewünschten Eintrag, klicken Sie rechts auf das Kreuzchen und dann auf "Speichern"). Allerdings sollte nach dem Hinzufügen oder Löschen einer Unteranlage "Upload-All" gestartet werden, und der Benutzer sollte sich vergewissern, dass die Unteranlagen-Daten mit der virtuellen Knotenkonfiguration der Anlage übereinstimmen.

Beim Löschen hochgeladener Unteranlagen wird praktisch der entsprechende virtuelle Knoten von dem physikalischen Knoten entfernt. Daher kann diese Verwaltungsaufgabe auch über den Dialog "Virtuelle Knoten (KNDEF)" erledigt werden. Fällt die Überprüfung vor der Löschung einer Anlage in diesem Bildschirm positiv aus, kann der Benutzer den betreffenden virtuellen Knoten löschen. Eine Del-KNDEF AMO wird zur Löschung des virtuellen Knotens auf dem physikalischen Knoten erstellt, und der virtuelle Knoten wird aus dem Rufnummernplan entfernt. Nach diesem Schritt werden automatisch die Unteranlage und alle zugehörigen Daten in der CDB ebenfalls gelöscht.

Ein Upload (PBX, LCR, All oder Delta) kann nur von dem Objekt aus initiiert werden, das das physikalische VNR-System darstellt, nicht von den Objekten aus, die Unteranlagen darstellen. Daher ist es nicht möglich, ein Upload für eine bestimmte Unteranlage zu starten. Es wird die gesamte VNR-Anlage auf einmal hochgeladen.

"VNR aktiv", "Physikalisches VNR-System>und "Name des physikalischen VNR-Systems>sind schreibgeschützte Felder.

Das Feld "VNR aktiv>wird entsprechend den aus der Anlage hochgeladenen Daten aktualisiert und legt fest, ob es sich um eine Anlage mit oder ohne VNR handelt.

Das Feld "Physikalisches VNR-System>gibt an, ob die Anlage eine physikalische VNR-Anlage ist. Ist es aktiviert, handelt es sich bei der Anlage um eine VNR-Anlage und einen physikalischen Knoten (keine Unteranlage).

Das Feld "Name des physikalischen VNR-Systems>enthält den Namen der physikalischen Anlage. Bei physikalischen Anlagen (mit oder ohne VNR) enthält dieses Feld den Namen der Anlage selbst. Diese beiden Felder unterscheiden sich nur bei Unteranlagen und geben die physikalische Anlage dieser Unteranlage an.

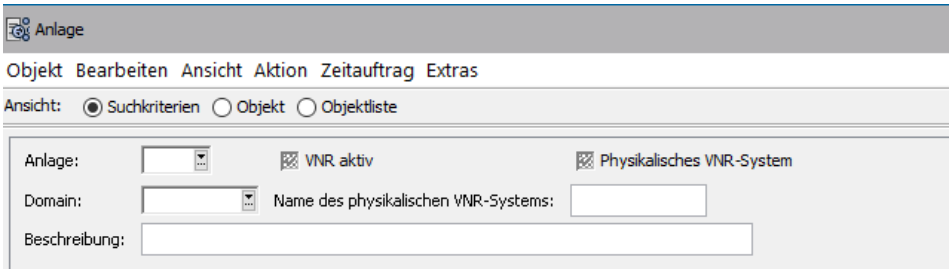


Abbildung 76: Registerkarte "Generic Data and Sub-Switch" (Allgemeine Daten und Unteranlage) für eine neue Anlage in Configuration Management

5.8.4 Spezielle Handhabung virtueller Knoten (KNDEF)

Da eine Unteranlage nur einen virtuellen Knoten enthalten kann (1:1-Zuordnung), ist eine spezielle Handhabung virtueller Knoten (KNDEF) für den Fall erforderlich, dass "Physikalisches VNR-System>auf dem physikalischen Knoten aktiv ist:

Virtuelle Knoten werden auf Unteranlagen-Ebene gehandhabt. Jede Unteranlage (die tatsächlich selbst ein virtueller Knoten ist) enthält jeweils nur einen virtuellen Knoten. Um einen neuen virtuellen Knoten zu einer physikalischen Anlage hinzuzufügen, kann der Benutzer den virtuellen Knoten zu einer beliebigen Unteranlage auf dem physikalischen Knoten hinzufügen. Dies ist nur erforderlich, um den virtuellen Knoten auf der Anlage zu erstellen. Nachdem der virtuelle Knoten erstellt wurde, muss die entsprechende Unteranlage zu der physikalischen Anlage hinzugefügt und "Upload-All>auf der physikalischen Anlage gestartet werden. Nach erfolgtem Upload gibt es wieder auf jeder Unteranlage der Anlage je einen virtuellen Knoten.

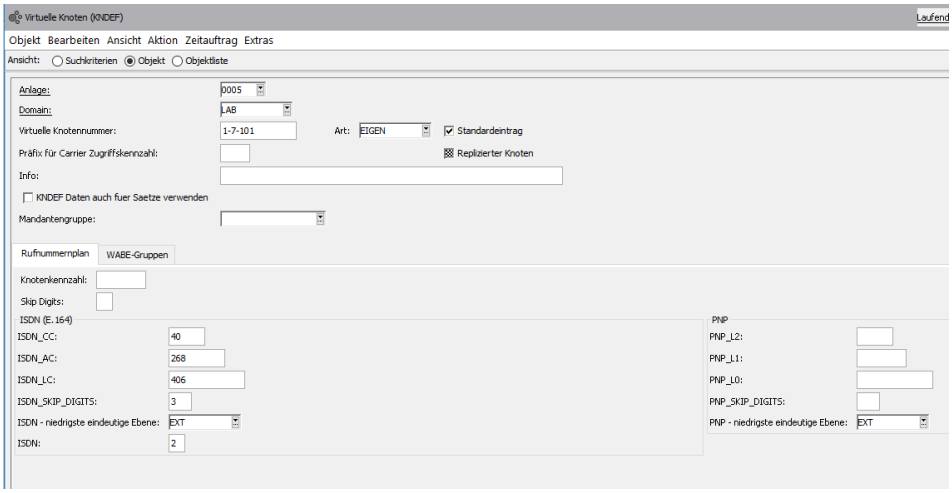


Abbildung 77: Dialog "Virtuelle Knoten (KNDEF)>in Configuration Management

Die Daten für die virtuellen Knoten werden durch den Upload des CM eingegeben. Sie können angezeigt, geändert und gelöscht werden.

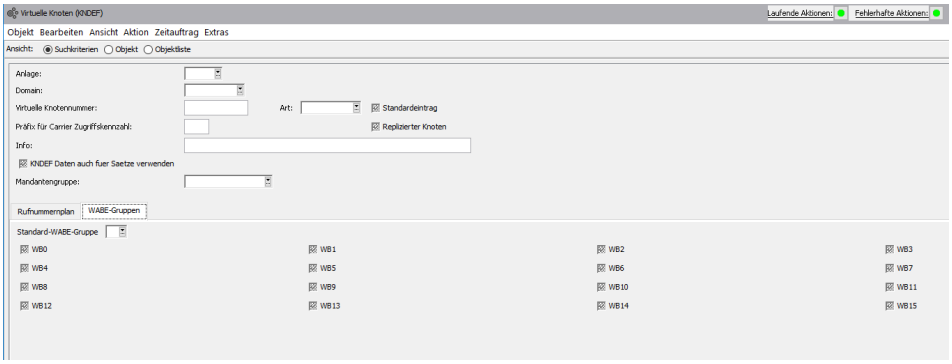


Abbildung 78: Dialog "Virtuelle Knoten (KNDEF)>- Registerkarte "WABE-Gruppen" in Configuration Management

5.8.4.1 Hinzufügen eines virtuellen Knotens

Wird ein neuer virtueller Knoten zu einem physikalischem Knoten mit aktivierter Option "Physikalisches VNR-System>hinzugefügt, muss außerdem die Zuordnung zu der entsprechenden Unteranlage vorgenommen werden, die den neu erstellten virtuellen Knoten darstellen wird:

- Fügen Sie einen neuen virtuellen Knoten im CM-Dialog "Virtuelle Knoten (KNDEF)>hinzu, wobei der Anlagenname einer der Unteranlagen dieses physikalischen Knotens entspricht.
- Klicken Sie auf die Registerkarte **Unteranlagen-Daten** des CM-Dialogs **Anlage**, und erstellen Sie eine neue Unteranlage, die den neuen virtuellen Knoten darstellen wird. Nehmen Sie diese neue Unteranlage in eine der vorhandenen oder in eine neue Domain auf (jedenfalls in eine andere Domain als die Unteranlagen desselben physikalischen Knotens).
- Öffnen Sie den CM-Dialog **Anlage**, und starten Sie "Upload-All" zu dem betreffenden physikalischen System.

5.8.4.2 Ändern eines vorhandenen virtuellen Knotens

Da die Änderungsmöglichkeiten bei vorhandenen virtuellen Knoten sehr begrenzt sind, bleibt das Verhalten (auf AMO-Ebene) unverändert.

5.8.4.3 Löschen eines vorhandenen virtuellen Knotens

Bei der neuen Version löst das Löschen eines bestimmten virtuellen Knotens automatisch das Löschen entsprechender Unteranlagen aus.

Da das Löschen eines virtuellen Knotens sehr restriktiv gehandhabt wird (alle Teilnehmer auf diesem virtuellen Knoten müssen gelöscht werden, bevor der Knoten selbst gelöscht werden kann), folgt CM diesen Restriktionen. Nur wenn alle Voraussetzungen für eine Löschung erfüllt sind, löscht CM die entsprechenden Unteranlagen ebenfalls.

5.8.5 Dialog "Teilnehmeranschluss>in Configuration Management

Die im Dialog "Teilnehmeranschluss>angezeigten Daten sind dieselben wie bei Anlagen ohne VNR. Im Feld "Kennzahl>ist kein Wert angezeigt, selbst wenn der Code für die EIGENKZ zugewiesen wurde. Dieser ist nicht Teil der Teilnehmernummer.

Bei VNR-Anlagen wird der Code für die EIGENKZ im Feld "Kennzahl" angezeigt, da dieser auch Teil der im AMO SBCSU zugewiesenen Teilnehmernummer ist. Dieser wird auch im Feld "Rufnummer>angezeigt.

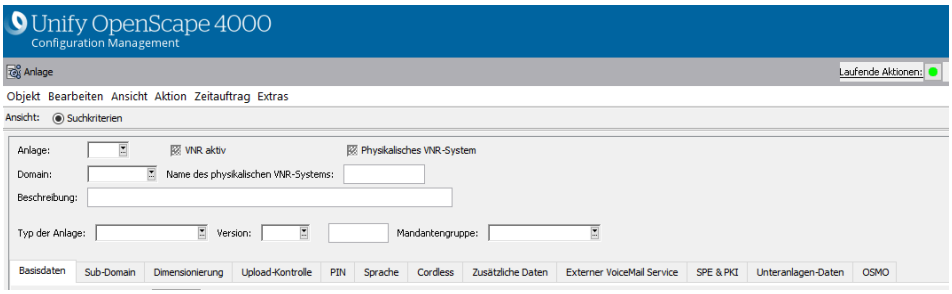


Abbildung 79: Dialog "Teilnehmeranschluss>in Configuration Management

5.8.6 Einschränkungen

Für Unteranlagen gelten einige Einschränkungen.

1) UPLOAD: Das Upload von Unteranlagen kann nicht von Unteranlagen aus gestartet werden; dies muss von physikalischen Anlagen aus erfolgen. (Auch geplante Uploads sind von Unteranlagen aus nicht möglich.) Ein Upload kann zu der physikalischen Anlage gestartet werden; während des Uploads werden alle Unteranlagen auf diesem physikalischen Knoten gleichzeitig hochgeladen. Daher ist es nicht möglich, ein Upload nur zu einer Unteranlage auszuführen.

2) Verwaltung physikalischer Knoten:

- **a)** Bei einem Suchvorgang über den Dialog "Anlage>werden sowohl physikalische Anlagen als auch Unteranlagen aufgeführt. Es ist jedoch nicht möglich, Daten von Unteranlagen in diesem Dialog zu ändern; ausgenommen sind die Felder "VMS Anlage", "VM Server", "Bevorzugter Richtungsindex>und "Land". Ortskennzahl, Amtskennzahl und Knotenkennzahl können bei Unteranlagen festgelegt werden. Bei anderen Feldern kann der Benutzer nur beim physikalischen System Änderungen vornehmen. Wenn Sie eine Unteranlage über den Dialog "Anlage>ändern möchten, können Sie Änderungen an dem physikalischen System vornehmen, für das die Unteranlagen definiert sind. Bei jeder Änderung an einer physikalischen Anlage werden alle auf dieser Anlage definierten Unteranlagen mit den entsprechenden Daten aktualisiert.
- **b)** Die Verwaltung in den anderen Dialogen ist nur bei Unteranlagen und nicht beim physikalischen VNR-Systemen möglich. Möchte der Benutzer einen Teilnehmeranschluss erstellen, verschieben o.ä., wird das physikalische VNR-System nicht als mögliche Zielanlage aufgeführt.

5.9 PIN-Verteilungsprogramm

Dieser Abschnitt beschreibt die Aufgabe und die Funktionsweise des auf dem OpenScape 4000 Manager-Server installierten PIN-Verteilungsprogramms.

5.9.1 Einleitung

Das PIN-Verteilungsprogramm ermöglicht die automatische Verteilung von PINs mit Hilfe des OpenScape 4000 Managers. Die Verteilung der PINs zu den anderen Anlagen kann zeitgesteuert z.B. in der Nacht erfolgen.

Das PIN-Verteilungsprogramm ist Bestandteil des XIE/API Paketes ASxie und wird im Verzeichnis /opt/xie/dmsie/pindist installiert.

5.9.2 Administration

Für die korrekte Arbeitsweise ist es erforderlich, dass das Protokollieren von gelöschten Sätzen der Tabelle upd_pin in der OpenScape 4000-Common Database (CDB) aktiviert ist. Diese Protokollierung kann wie folgt am OpenScape 4000 Manager-Server eingeschalten werden:

1) Aufruf von /opt/xie/dmsie/bin/ujgedelupd.sh -y. Dabei wird das Flag pin_upd in der CDB-Tabelle admin auf 001 gesetzt um die Protokollierung der gelöschten Sätze via CM einzuschalten.
2) Cserver stoppen und neu starten (Aufruf von /opt/cm/bin/cs_control restart).

Das Script "pindist.sh"

Bei der Installation von ASxie wird im Verzeichnis /opt/xie/dmsie/pindist das Startscript pindist.sh installiert. Mit diesem Script können folgende Aktionen durchgeführt werden:

Startscript-Menü:

```
AUTOMATISCHE PINVERTEILUNG

1-Aktivieren
2-Deaktivieren
3-Status
4-Protokolldatei ausgeben
5-Ende

Auswahl: _
```

Aktivieren

Die automatische Verteilung der PINs wird aktiviert. Die Uhrzeit (Stunde und Minute) der automatischen PIN-Verteilung muß in diesem Dialog festgelegt werden:

```
Angaben für die automatische PIN-Verteilung:
-------------------------------
Startzeitpunkt für tägliche PIN-Verteilung (hh:mm): 23:45
```

Deaktivieren

Die automatische PIN-Verteilung wird deaktiviert (Der Eintrag in der UNIX-Crontabelle wird entfernt).

Status

Falls die PIN-Verteilung aktiviert ist, wird der Startzeitpunkt ausgegeben:

```
Status der automatischen PIN-Verteilung:
----------------------------
Stunde: 23
Minute: 45

Weiter mit Return-Taste
```

Protokolldatei ausgeben

Das Protokoll der letzten PIN-Verteilung wird am Bildschirm ausgegeben. In diesem Protokoll werden Ablaufmeldungen und eventuell aufgetretene Fehler im Klartext vermerkt.

```
20.09.03 04:00: BEGIN PIN DISTRIBUTION
Number of switches: 4
Select all PIN modifications since 2003-01-09 04:00:36
Number of Inserts: 1
Number of updates: 0
Number of Deletes: 1
Extension: 45678   Switch: GUD1 new PIN created
Extension: 45678   Switch: ERD1 new PIN created
Extension: 45678   Switch: SIE1 new PIN created
Extension: 45670   3 records deleted
Send AMO's to PABX network
Update file InsertedPins.dat
20.09.03 04:02: END      PIN DISTRIBUTION
```

ENDE

Ende der Bearbeitung und Rückkehr zum Hauptmenü

5.9.3 Anwenderhinweise

Wurden PIN`s modifiziert so wird diese Änderungen nicht an alle Anlagen verteilt! Soll eine bestehende PIN abgeändert werden, muß entweder die PIN an allen Anlagen über das OpenScape Configuration Management geändert werden oder die PIN an einer Anlage gelöscht und neu eingerichtet werden.

PIN`s mit Pin-Typ "G04>(pkz_pin) oder "G05>(wkz_pin) oder "C66>(Cordless E PIN) werden nicht an alle Anlagen verteilt. Ist in der Datei /var/xie/pindist/Extensions.dat das Flag PKZ_PIN=YES gesetzt, werden auch PINs vom Typ "G04>(pkz_pin) verteilt.

Auf allen Anlagen müssen sich die selben Nebenstellen ("extensions") befinden. Ist dies nicht der Fall, so kann pro Anlage eine bestimmte Nebenstelle in der Datei /var/xie/pindist/Extensions.dat festgelegt werden. (Pro Anlage muß eine Zeile mit Anlagenamen und Nebenstelle - getrennt durch Leerzeichen - eingetragen werden). Neu hinzugefügte PIN`s werden dann bei diesen Anlagen generell unter der in der Datei "Extensions.dat" angegebenen Nebenstelle gespeichert. Wird statt der Nebenstelle die Zeichenfolge "IGNORE>angegeben

werden an diese Anlage keine PIN`s verteilt. Befinden sich keine Einträge in der Datei (dies ist der Defaultwert), so wird angenommen, daß sich auf den Anlagen im PABX-Netz die selben Nebenstellen befinden.

Beispiel 1 für Datei "Extensions.dat>im Verzeichnis "/var/xie/pindist"

```
#
# Zuordnungstabelle ANLAGE -> RUFNUMMER
# ----------------------------------------
#
# Syntax: <Switch><spaces><extension>
#
#         <Switch>    ... Anlagename  (max. 4 Zeichen)
#         <spaces>    ... ein oder mehrere Leerzeichen
#         <Extension> ... Nebenstelle  (max. 6 Zeichen)bzw.
#IGNORE wenn keine PINS an diese
#Anlage verteilt werden sollen
#
#(Kommentarzeilen beginnen mit dem Zeichen ,Äò#,Äô)
#
SIE1 4711
SIE2 4711
SIE3 4711
SIE4 IGNORE
# Wird ,ÄúMaster Switch,Äù angegeben so werden nur neue PINs
# dieser Anlage verteilt:
MASTER_SWITCH=SIE1
# zusaetzlich sollen auch PKZ_PINs verteilt werden:
PKZ_PIN=YES
```

In diesem Fall werden nur PIN`s, die auf der Anlage SIE1 unter der Nummer "4711>erfasst wurden, bei den Anlagen "SIE2> und "SIE3>unter der Nebenstelle "4711>abgespeichert und die PIN`s nicht an die Anlage "SIE4>verteilt.

Sollen z.B. alle PINÂ´s einer Anlage verteilt werden so müssen unterschiedliche virtuelle Nummern für jede Anlage in der Datei extensions.dat angegeben werden!

Beispiel 2 für Datei "Extensions.dat>im Verzeichnis "/var/xie/pindist"

```
#
# Zuordnungstabelle ANLAGE -> RUFNUMMER
# ----------------------------------------
#
# Syntax: <Switch><spaces><extension>
#
#         <Switch>    ... Anlagename  (max. 4 Zeichen)
#         <spaces>    ... ein oder mehrere Leerzeichen
#         <Extension> ... Nebenstelle  (max. 6 Zeichen)bzw.
#IGNORE wenn keine PINS an diese
#Anlage verteilt werden sollen
#
#(Kommentarzeilen beginnen mit dem Zeichen ,Äò#,Äô)
#
SIE1 4711
SIE2 4712
SIE3 4713
SIE4 IGNORE
# Wird ,ÄúMaster Switch,Äù angegeben so werden nur neue PINs
# dieser Anlage verteilt:
MASTER_SWITCH=SIE1
# zusaetzlich sollen auch PKZ_PINs verteilt werden:
PKZ_PIN=YES
```

In diesem Fall werden alle PIN`s, die auf der Anlage SIE1 erfasst wurden, bei den Anlagen "SIE2> und "SIE3>unter der Nebenstelle "4712>bzw. "4713>abgespeichert und die PIN`s nicht an die Anlage "SIE4>verteilt.

Bei großen Datenmengen (z.B. >20.000 PIN`s) bzw. bei starker Systembelastung kann die Verbindung zum XIE-Server Prozess durch Timeout unterbrochen werden (Meldung "server timeout, no connection to xieserver" in der Protokolldatei).

In diesem Fall muss der Parameter "SERVER_TIMEOUT>in der Datei /opt/xie/dmsie/CLaccess/xieserver.cfg von 28800 auf z.B. 36000 Sekunden erhöht werden.

Nach dem Ändern muss der xieserver durch Aufruf von /opt/xie/dmsie/bin/xieserver.sh stop gestoppt und mit /opt/xie/dmsie/bin/xieserver.sh start neu gestartet werden!

Folgende Vorgangsweise muß beim "Upgrade>auf eine neue OpenScape 4000-Version beachtet werden:

1) Unmittelbar vor dem "Upgrade>muss das Pinverteilungsprogramm noch einmal gestartet werden.
2) Es dürfen nun keine neuen Pins angelegt oder modifiziert werden
3) Retten der Datei /var/xie/pindist/Extension.dat und /var/xie/pindist/InsertedPins.dat
4) Upgrade der OpenScape-Version
5) Wiederherstellen der Datei /var/xie/pindist/Extension.dat und /var/xie/pindist/InsertedPins.dat
6) Das Datum in der Datei /var/xie/pindist/LastRuntime.ini muß auf das aktuelle Datum (nach dem "Upgrade") gesetzt werden (Format: "JJJJ-MM-DD HH:MM:SS"). Damit wird verhindert daß bereits verteilte PINs noch einmal bearbeitet werden.
7) Das Pinverteilungsprogramm kann nun aktiviert werden.

Folgende Vorgangsweise muss beim Hinzufügen einer neuen Anlage beachtet werden:

1) Retten der Datei "Extensions.dat>nach "Extensions.dat.save"
2) Umbenennen der Datei "LastRuntime.ini>nach "LastRuntime.ini.save"
3) Bei allen Anlagen muß die Rufnummer auf "IGNORE>in der Datei "Extensions.dat>gesetzt werden
4) Die neue Anlage muß mit der entsprechenden Nebenstelle in die Datei "Extension.dat>und "Extensions.dat.save>hinzugefügt werden
5) Das Pinverteilungsprogramm muß aktiviert werden; Nun werden alle PINs auf die neue Anlage verteilt.
6) Nach dem Verteilen der PINs an die neue Anlage muß die Datei "Extensions.dat.save" nach "Extensions.dat>und die Datei "LastRuntime.ini.save" nach "LastRuntime.ini>kopiert werden.

Folgende Vorgangsweise muss beim Löschen einer Anlage beachtet werden:

1) Deaktivieren der Pinverteilung
2) Löschen der Anlage (und eventuell neues Einrichten der selben Anlage?)
3) Das Datum in der Datei /var/xie/pindist/LastRuntime.ini muß auf das aktuelle Datum (nach dem Löschen) gesetzt werden (Format: "JJJJ-MM-

DD HH:MM:SS"). Damit wird verhindert, dass bereits verteilte PINs an den anderen Anlagen gelöscht werden!

4) Das Pinverteilungsprogramm kann nun aktiviert werden.

5.9.4 Interner Ablauf

Zur Realisierung der Aufgabenstellung wurden folgende Komponenten entwickelt:

Das Shell Skript "pindist.sh>ist zuständig für:

- Die Administration der PIN-Verteilung (Aktivieren/Deaktivieren und Abfrage der Startzeit)
- Das Eintragen/Austragen des PIN-Verteilungsprogrammes "pindist" in die Cron-Tabelle
- Das Anzeigen der Protokolldatei

Das C++ Programm "pindist>ist zuständig für die eigentliche Verteilung der PINs an alle Anlagen:

- Das Programm benutzt zur Kommunikation mit dem OpenScape/HiPath 4000 die XIE-Klassenbibliothek XIE-API.
- Mit "SELECT switch_name FROM SWITCH>werden alle Anlagenamen gelesen und in einer Liste gespeichert.
- Die in der Datei "Extensions.dat>angegebenen Anlagen und Nebenstellen werden gelesen und in einer Liste gespeichert.
- Mit dem "SELECT_UPDATES>Aufruf werden alle modifizierten Datensätze aus der ODF PIN ab einem bestimmten Zeitpunkt gelesen (Beim 1. Programmaufruf werden alle Sätze gelesen, danach entspricht dieser Zeitpunkt dem des letzten Aufrufes von "pindist").
- Handelt es sich um einen "UPDATE"- Satz (d.h. eine PIN wurde modifiziert) erfolgt keine Aktivität -- da UPDATE-Anweisungen auf DMS-API Objekte vom Typ PIN nicht zugelassen sind (DMS-API Fehlermeldung: 3754 - PIN und PIN Typ können nicht geändert werden).
- Handelt es sich um einen "INSERT"-Satz (d.h. eine PIN wurde hinzugefügt) wird eine "INSERT"-Anweisung für jede Anlage an den OpenScape 4000 gesendet (durch Aufruf einer XIE-API C++ Methode). Die "pin_num>wird dabei an allen Anlagen auf den gleichen, neuen Wert gesetzt. Befindet sich die Anlage in der Datei "Extensions.dat" so wird beim INSERT die Nebenstelle aus der Datei "Extensions.dat" verwendet anderenfalls die Nebenstelle aus dem entsprechenden "SELECT_UPDATES" Satz. Zusätzlich werden die Felder unique_key, domain, switch_name, extension, pin_num, pin_type, pin_class, pinindiv und user_create der eingefügten Sätze in der Datei "InsertedPins.dat>gespeichert.
- Handelt es sich um einen "DELETE"- Satz (d.h. eine PIN wurde gelöscht) werden mit Hilfe der Daten aus der Datei "InsertedPins.dat" alle Sätze mit der selben domain und pin_num und pin_typ und pin_class gelöscht (ebenfalls durch Aufruf einer entsprechenden XIE-API Methode). Die gelöschten Sätze werden auch aus der Datei "InsertedPins.dat" gelöscht.
- Nach der Abarbeitung aller von "SELECT_UPDATES>gelieferten Sätze wird das aktuelle Datum und die Zeit im File "LastRuntime.ini" vermerkt. Diese Angaben werden beim nächsten Aufruf von "pindist" als Zeitpunkt für den "SELECT_UPDATES"-Aufruf verwendet.

5.9.5 Verzeichnisstruktur

Bei der Installation von ASxie werden im Verzeichnis /opt/xie/dmsie/pindist folgende Dateien installiert:

Tabelle 3: Installationsdateien

Verzeichnis/Datei	Beschreibung
Extensions.dat.sample	Beispiel Zuordnungstabelle ANLAGE zu NEBENSTELLE
pindis.sh	Shell Skript, zuständig für die Administration
pindis	Hauptprogramm

Zur Laufzeit werden folgende Dateien im Verzeichnis /var/xie/pindist angelegt:

Tabelle 4: Zur Laufzeit angelegte Dateien

Verzeichnis/Datei	Beschreibung
LastRuntime.ini	Datei mit Zeitstempel des letzten Aufrufs (ASCII Datei, Format: JJJJ-MM-DD HH:MM:SS)
InsertedPins.dat	Tabelle mit aktuellen PIN`s (Diese Informationen werden beim Löschen von PIN`s benötigt)
pindist.prot	Protokoll des letzten Aufrufs
Extensions.dat	Zuordnungstabelle Anlage zu Nebenstellen

In der xieserver Konfigurationsdatei /opt/xie/dmsie/CLaccess/xieserver.cfg sind folgende Parameter mit Standardwerten vorbelegt:

Tabelle 5: xieserver-Konfigurationsparameter

Parameter	Wert	Beschreibung
MAX_CLIENTS	10	Maximale Anzahl gleichzeitiger XIE-Clients
PORT	2011	TCP/IP Portnummer - darf nicht verändert werden!

Parameter	Wert	Beschreibung
SERVER_TIMEOUT	1800	Timeout in Sekunden; Anzahl der Sekunden die der XIE-Server auf Anforderungen des Clients wartet bevor die Verbindung abgebaut wird. Bei großen Datenmengen (> 20.000 PINs) muss diese Zeit auf z.B. 18000 Sekunden erhöht werden. Nach dem Ändern muss der xieserver durch Aufruf von /opt/xie/dmsie/bin/xieserver.sh stop gestoppt und mit /opt/xie/dmsie/bin/xieserver.sh start neu gestartet werden!

6 Überwachung der Systemparameter mit OpenScape FM Client Agent

Die Überwachung von Systemparametern mit dem OpenScape FM (Fault Management) Client Agent ist auf OpenScape 4000 Manager und Assistant möglich.

Anmerkung: Dieser Vorgang muss erneut durchgeführt werden, wenn ein Update mit Major, Minor oder FixRelease durchgeführt wird oder wenn eine Neuinstallation von Assistant/Manager manuell oder automatisch durchgeführt wird (wenn der Mechanismus „Festplatte voll“ ausgelöst wird).

Um Systemparameter wie CPU, Dateisystem, Speichernutzung oder die Netzwerklast des OpenScape 4000 Assistant/Manager zu überwachen, muss der lokale Systemverwaltungsagent von OpenScape FM installiert sein.

Führen Sie die folgenden Schritte aus, um den OpenScape FM Client Agent zu installieren und zu konfigurieren:

1) Öffnen Sie die OpenScape FM-Installations-ZIP-Datei und suchen Sie die beiden folgenden Dateien: `setup_agent_osfm.sh` und `setup_agent_osfm.jar`.

   Diese Dateien müssen an einen temporären Speicherort auf dem Manager/Assistenten kopiert werden (z. B. `/tmp/`).

   So installieren Sie den Agenten:

   a) Öffnen Sie eine SSH-Verbindung zum Manager oder Assistenten und navigieren Sie zu dem Speicherort, an den die Dateien kopiert wurden.

   b) Führen Sie das Installationsskript mit dem folgenden Befehl aus:

   ```
   sh ./setup_agent_osfm.sh
   ```

   c) Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

   Sobald die Installation abgeschlossen ist, ist der Agent betriebsbereit.

2) Für die Kommunikation zwischen dem installierten Agenten und OpenScape FM müssen am Manager/Assistant die Ports 3051 und 3039 geöffnet sein. Dies kann im Webmin-Bereich von Manager/Assistent unter durchgeführt werden **Firewall** Section.

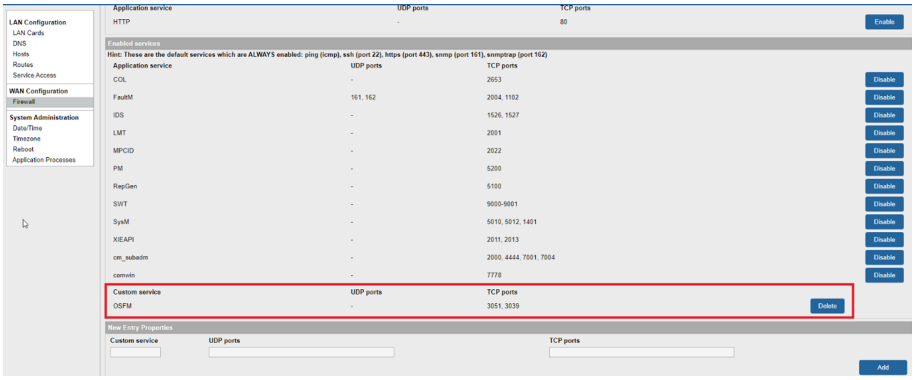


Abbildung 80: Aktivieren der Ports 3051 und 3039 in Webmin

3) Nach erfolgreicher Installation des Agenten sollte ein neues Host-Objekt im OpenScape FM-Client-Baum verfügbar sein.

Wenn der Host nicht im Client-Baum aufgeführt ist, muss er manuell hinzugefügt werden.

So fügen Sie einen Host manuell hinzu:

a) Klicken Sie im OpenScape FM-Client mit der rechten Maustaste auf **Network Topology**, und select **New** > **Host**.

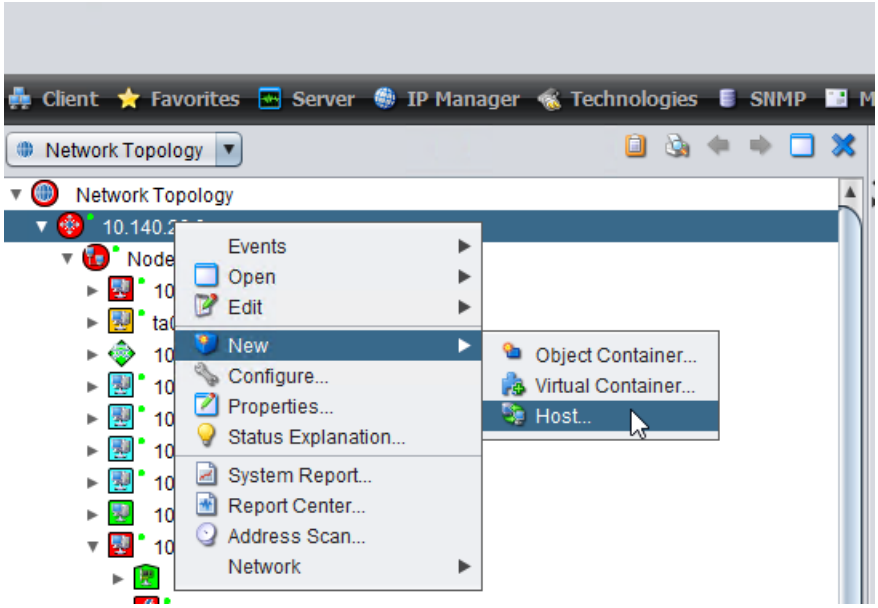


Abbildung 81: Hinzufügen des Hosts im OpenScape FM-Client-Baum

b) Geben Sie die IP-Adresse des Managers/Assistenten ein **IP address** Feld.

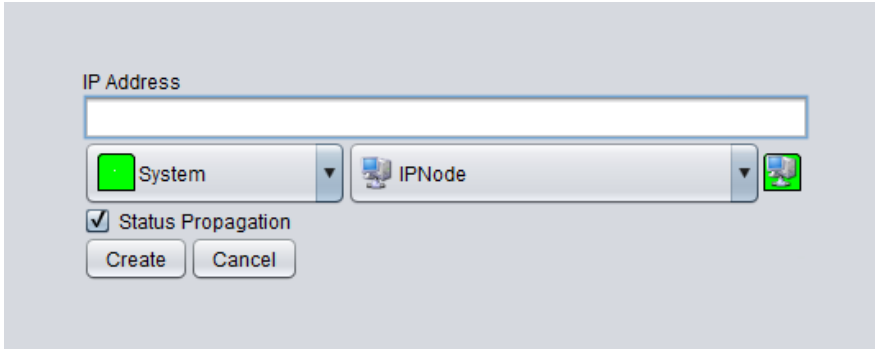


Abbildung 82: Eingabe der IP-Adresse des Managers/Assistenten

4) Sobald der Host im OpenScape FM-Client-Baum erscheint, muss der automatische Erkennungsprozess gestartet werden, um alle von OpenScape FM überwachten Eigenschaften aufzulisten.

So starten Sie den automatischen Erkennungsprozess:

a) Klicken Sie im OpenScape FM-Client mit der rechten Maustaste auf den Host und wählen Sie ihn aus**Host** > **Start Discovery**.

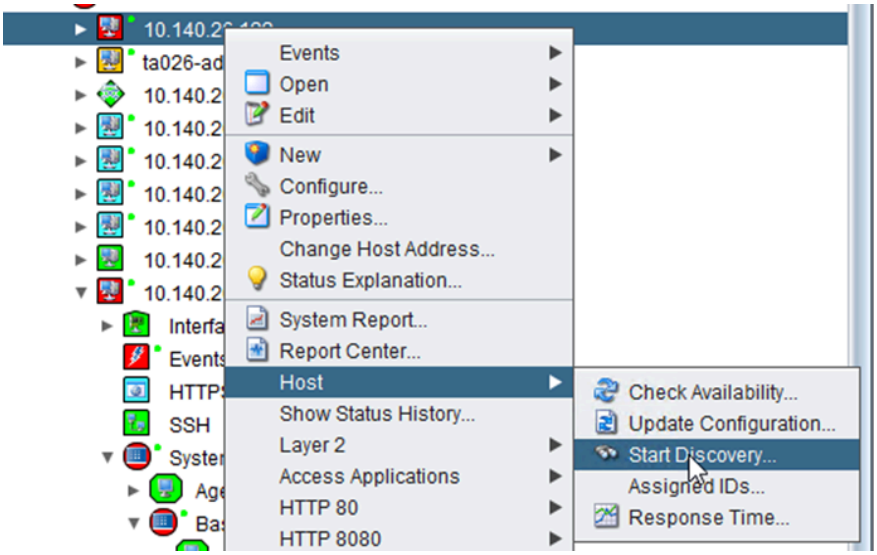


Abbildung 83: Starten des Discovery-Prozesses

b) Wenn der Erkennungsprozess abgeschlossen ist, wird unter der OpenScape FM-Client-Struktur ein neuer **System Management** erstellt.

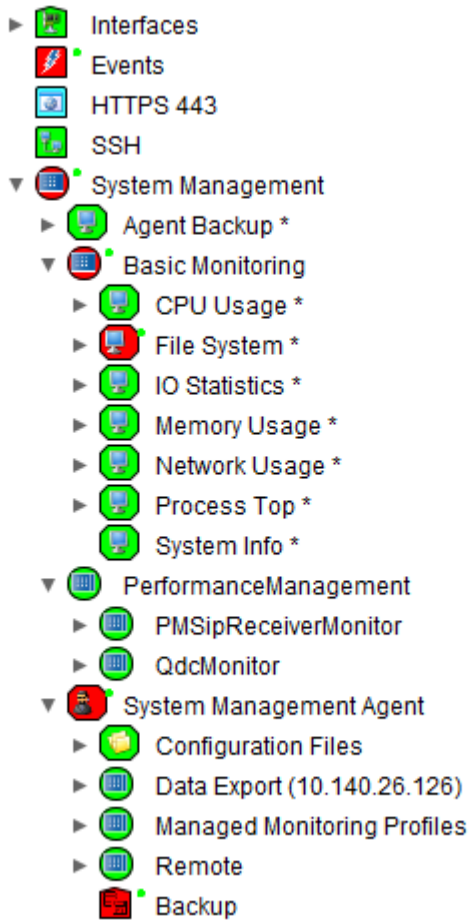


Abbildung 84: System Management Eintrag im OpenScape FM Client-Baum

6.1 Konfigurieren Sie das Zertifikat für TLS in OpenScape FM Agent

Um das Zertifikat für TLS in OpenScape FM Agent zu konfigurieren, wird der Befehl keytool verwendet (dies ist Teil der Java-Installation).

Beispielsweise wird ein Zertifikat mit dem privaten Schlüssel im Keystore und Alias `mycert1` in `/tmp/thecert.p12`gefunden.

Durch das Ausführen des folgenden Befehls konfiguriert das Zertifikat für die Verwendung des Agenten:

```
keytool -importkeystore -srckeystore /tmp/thecert.p12 -
srcalias mycert1 -destalias InternalWebServer -destkeystore
INSTALLDIR/ssma/conf/trustedcerts.jks
```

Das Agentenzertifikat wird im Keystore `INSTALLDIR/ssma/conf/trustedcerts.jks` mit dem Alias `InternalWebServer`gespeichert.

Das Passwort für den Keystore und den privaten Schlüssel wird in `INSTALLDIR/system.properties`gespeichert:

```
javax.net.ssl.keyStorePassword=xxxxxxx
```

```
javax.net.ssl.trustStorePassword=xxxxxxx
```

Anmerkung:

Sowohl der Keystore als auch der private Schlüssel müssen dasselbe Passwort haben. Ein privater Schlüssel ohne Passwort funktioniert nicht. Das in `system.properties`angegebene Passwort wird für Keystore und privaten Schlüssel verwendet.

Einige Sonderzeichen wie **!** werden mit dem Backslash entkommen. Diese sind nicht Teil des Passworts.
Bei jeder Passwortänderung muss der Agent neu gestartet werden, um das neue Passwort zu berücksichtigen.

6.2 Fehlerbehebung

1) Wenn Java nicht gefunden wird, können Sie die Umgebungsvariable `JAVA_HOME` so setzen, dass sie auf die gewünschte Java-Installation verweist, wie in der Abbildung unten dargestellt.

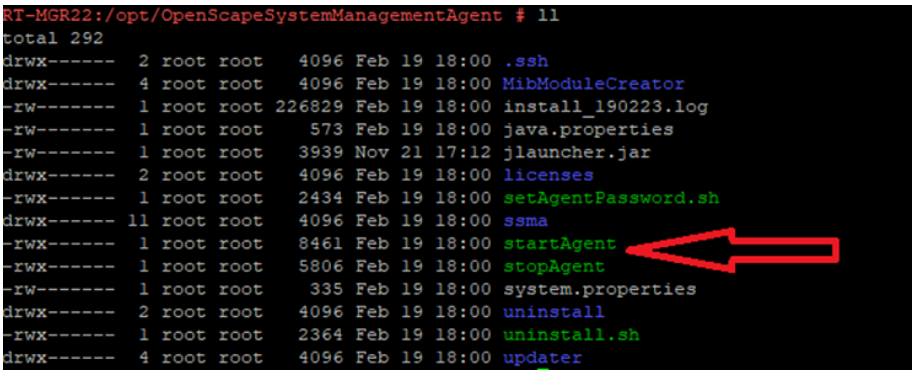
```
[[root@bender:/tmp]$ export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64/
[[root@bender:/tmp]$ /bin/bash ./setup_agent_osfm.sh
openjdk version "1.8.0_181"
OpenJDK Runtime Environment (build 1.8.0_181-8u181-b13-2~deb9u1-b13)
Matching Java version found:
/usr/lib/jvm/java-8-openjdk-amd64//bin/java
Logging to /tmp/install_210319.log

-------------------------------------------------------------------------
OpenScape System Management Agent
This installer will guide you through the installation process
of OpenScape System Management Agent.
For an update installation, please install into the same folder where the
current version is installed.
-------------------------------------------------------------------------
```

2) OpenScape FM erfordert ICMP, um Daten vom Agenten abzurufen. Daher müssen Sie sicherstellen, dass das für die OpenScape FM-Instanz verwendete Betriebssystem dies nicht blockiert. Einige Firewall-Regeln müssen möglicherweise in bestimmten Betriebssystemen definiert werden.

3) Wenn System Management vom OpenScape FM nicht erkannt wird, müssen Sie prüfen, ob der Agent auf dem Manager oder Assistant läuft.

Standardmäßig wird der Agent nach der Systeminstallation oder einem Neustart gestartet. Wenn kein Dienst für den Agenten läuft, kann er manuell gestartet werden, indem Sie die an dem Ort, an dem der Agent in Manager/Assistant installiert wurde, verfügbaren Skripte verwenden (z. B. der Standardspeicherort des Agenten: `/opt/OpenScapeSystemManagementAgent`).



7 Überwachung der Systemparameter mit OpenScape FM Client Agent

Die Überwachung von Systemparametern mit dem OpenScape FM (Fault Management) Client Agent ist auf OpenScape 4000 Manager und Assistant möglich.

> **Anmerkung:** Dieser Vorgang muss erneut durchgeführt werden, wenn ein Update mit Major, Minor oder FixRelease durchgeführt wird oder wenn eine Neuinstallation von Assistant/Manager manuell oder automatisch durchgeführt wird (wenn der Mechanismus „Festplatte voll“ ausgelöst wird).

Um Systemparameter wie CPU, Dateisystem, Speichernutzung oder die Netzwerklast des OpenScape 4000 Assistant/Manager zu überwachen, muss der lokale Systemverwaltungsagent von OpenScape FM installiert sein.

Führen Sie die folgenden Schritte aus, um den OpenScape FM Client Agent zu installieren und zu konfigurieren:

1) Öffnen Sie die OpenScape FM-Installations-ZIP-Datei und suchen Sie die beiden folgenden Dateien: `setup_agent_osfm.sh` und `setup_agent_osfm.jar`.

Diese Dateien müssen an einen temporären Speicherort auf dem Manager/Assistenten kopiert werden (z. B. `/tmp/`).

So installieren Sie den Agenten:

a) Öffnen Sie eine SSH-Verbindung zum Manager oder Assistenten und navigieren Sie zu dem Speicherort, an den die Dateien kopiert wurden.

b) Führen Sie das Installationsskript mit dem folgenden Befehl aus:

```
sh ./setup_agent_osfm.sh
```

c) Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

Sobald die Installation abgeschlossen ist, ist der Agent betriebsbereit.

2) Für die Kommunikation zwischen dem installierten Agenten und OpenScape FM müssen am Manager/Assistant die Ports 3051 und 3039 geöffnet sein. Dies kann im Webmin-Bereich von Manager/Assistent unter durchgeführt werden **Firewall** Section.

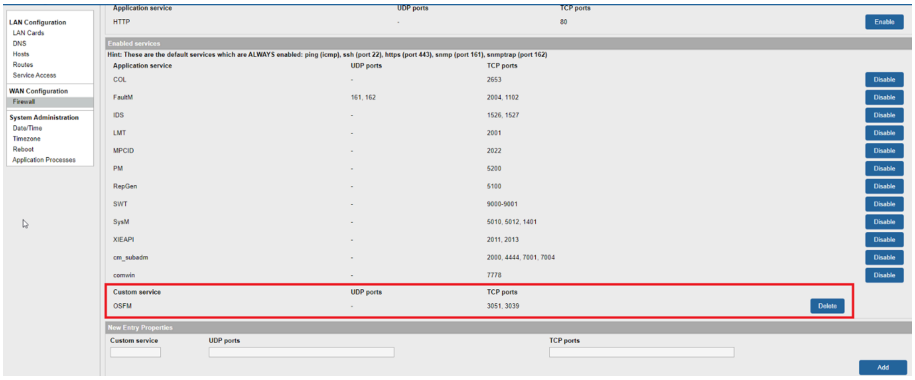


Abbildung 85: Aktivieren der Ports 3051 und 3039 in Webmin

3) Nach erfolgreicher Installation des Agenten sollte ein neues Host-Objekt im OpenScape FM-Client-Baum verfügbar sein.

Wenn der Host nicht im Client-Baum aufgeführt ist, muss er manuell hinzugefügt werden.

So fügen Sie einen Host manuell hinzu:

a) Klicken Sie im OpenScape FM-Client mit der rechten Maustaste auf **Network Topology**, und select **New** > **Host**.

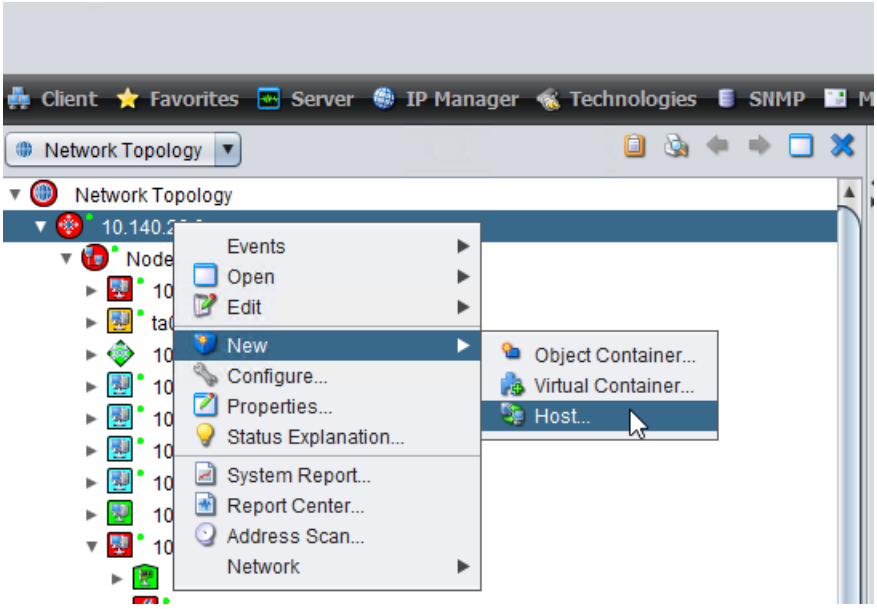


Abbildung 86: Hinzufügen des Hosts im OpenScape FM-Client-Baum

b) Geben Sie die IP-Adresse des Managers/Assistenten ein **IP address** Feld.

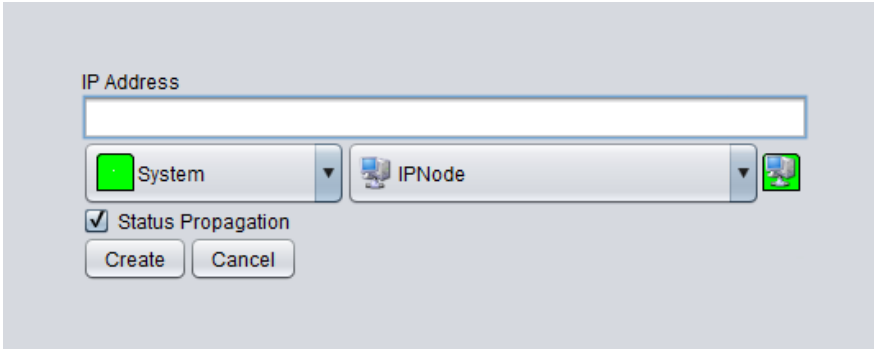


Abbildung 87: Eingabe der IP-Adresse des Managers/Assistenten

4) Sobald der Host im OpenScape FM-Client-Baum erscheint, muss der automatische Erkennungsprozess gestartet werden, um alle von OpenScape FM überwachten Eigenschaften aufzulisten.

So starten Sie den automatischen Erkennungsprozess:

a) Klicken Sie im OpenScape FM-Client mit der rechten Maustaste auf den Host und wählen Sie ihn aus**Host** > **Start Discovery**.

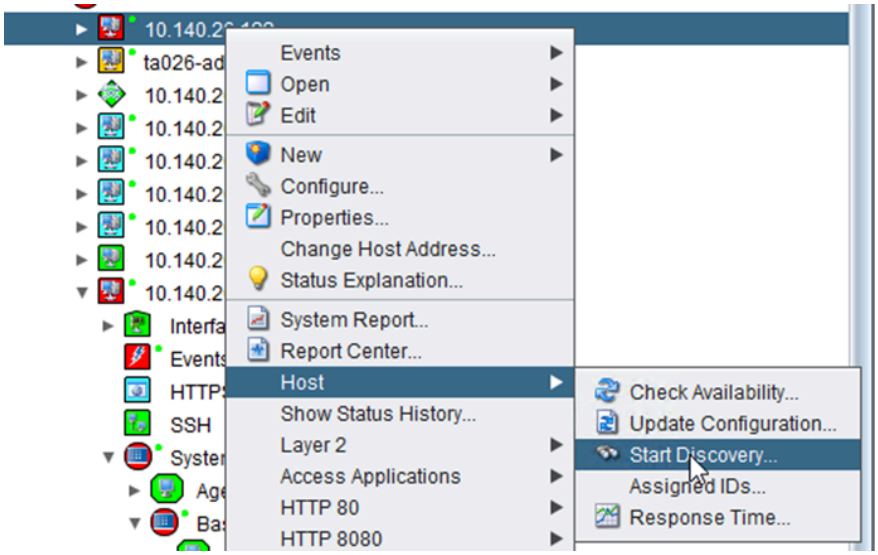


Abbildung 88: Starten des Discovery-Prozesses

b) Wenn der Erkennungsprozess abgeschlossen ist, wird unter der OpenScape FM-Client-Struktur ein neuer **System Management** erstellt.

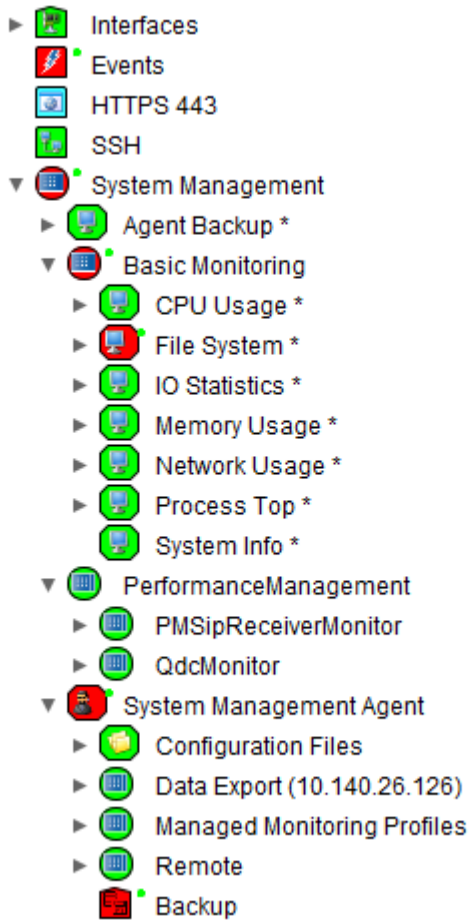


Abbildung 89: System Management Eintrag im OpenScape FM Client-Baum

7.1 Konfigurieren Sie das Zertifikat für TLS in OpenScape FM Agent

Um das Zertifikat für TLS in OpenScape FM Agent zu konfigurieren, wird der Befehl keytool verwendet (dies ist Teil der Java-Installation).

Beispielsweise wird ein Zertifikat mit dem privaten Schlüssel im Keystore und Alias `mycert1` in `/tmp/thecert.p12`gefunden.

Durch das Ausführen des folgenden Befehls konfiguriert das Zertifikat für die Verwendung des Agenten:

```
keytool -importkeystore -srckeystore /tmp/thecert.p12 -
srcalias mycert1 -destalias InternalWebServer -destkeystore
INSTALLDIR/ssma/conf/trustedcerts.jks
```

Das Agentenzertifikat wird im Keystore `INSTALLDIR/ssma/conf/trustedcerts.jks` mit dem Alias `InternalWebServer`gespeichert.

Das Passwort für den Keystore und den privaten Schlüssel wird in `INSTALLDIR/system.properties`gespeichert:

```
javax.net.ssl.keyStorePassword=xxxxxxx
```

```
javax.net.ssl.trustStorePassword=xxxxxxx
```

Anmerkung:

Sowohl der Keystore als auch der private Schlüssel müssen dasselbe Passwort haben. Ein privater Schlüssel ohne Passwort funktioniert nicht. Das in `system.properties`angegebene Passwort wird für Keystore und privaten Schlüssel verwendet.

Einige Sonderzeichen wie **!** werden mit dem Backslash entkommen. Diese sind nicht Teil des Passworts.
Bei jeder Passwortänderung muss der Agent neu gestartet werden, um das neue Passwort zu berücksichtigen.

7.2 Fehlerbehebung

1) Wenn Java nicht gefunden wird, können Sie die Umgebungsvariable `JAVA_HOME` so setzen, dass sie auf die gewünschte Java-Installation verweist, wie in der Abbildung unten dargestellt.

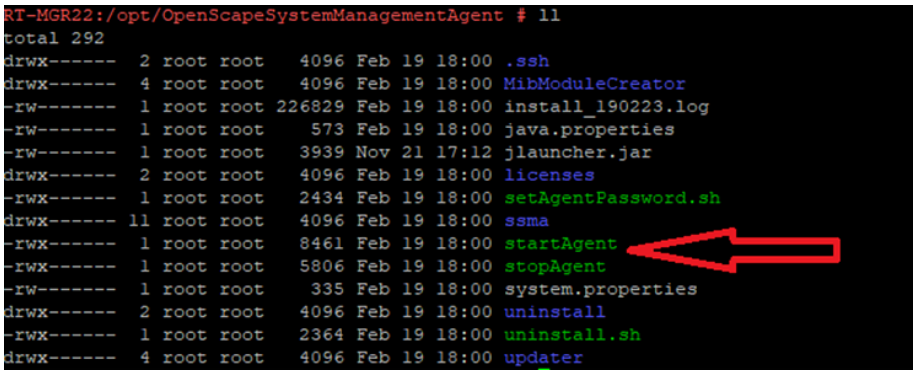
```
[[root@bender:/tmp]$ export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64/
[[root@bender:/tmp]$ /bin/bash ./setup_agent_osfm.sh
openjdk version "1.8.0_181"
OpenJDK Runtime Environment (build 1.8.0_181-8u181-b13-2~deb9u1-b13)
Matching Java version found:
/usr/lib/jvm/java-8-openjdk-amd64//bin/java
Logging to /tmp/install_210319.log

-------------------------------------------------------------------------
OpenScape System Management Agent
This installer will guide you through the installation process
of OpenScape System Management Agent.
For an update installation, please install into the same folder where the
current version is installed.
-------------------------------------------------------------------------
```

2) OpenScape FM erfordert ICMP, um Daten vom Agenten abzurufen. Daher müssen Sie sicherstellen, dass das für die OpenScape FM-Instanz verwendete Betriebssystem dies nicht blockiert. Einige Firewall-Regeln müssen möglicherweise in bestimmten Betriebssystemen definiert werden.

3) Wenn System Management vom OpenScape FM nicht erkannt wird, müssen Sie prüfen, ob der Agent auf dem Manager oder Assistant läuft.

Standardmäßig wird der Agent nach der Systeminstallation oder einem Neustart gestartet. Wenn kein Dienst für den Agenten läuft, kann er manuell gestartet werden, indem Sie die an dem Ort, an dem der Agent in Manager/Assistant installiert wurde, verfügbaren Skripte verwenden (z. B. der Standardspeicherort des Agenten: `/opt/OpenScapeSystemManagementAgent`).



8 OpenScape 4000 SNMP-Management

Dieses Kapitel beschreibt die Konfiguration und Inbetriebnahme der SNMP-Agenten auf OpenScape 4000 sowie die Skripte „read_filter.ksh“ und „set_filter.ksh“, die zur zeitgesteuerten Filterung von Alarmmeldungen des OpenScape 4000 Proxy Agent verwendet werden.

8.1 Geltungsbereich

Dieses Kapitel beschreibt die Verwaltung von SNMP auf OpenScape 4000, einschließlich der Überprüfung von Installation, Konfiguration und Inbetriebnahme.

8.2 Allgemeine Hinweise

Der OpenScape 4000 SNMP Proxy Agent ermöglicht das Management von OpenScape/HiPath 4000-Anlagen auf Basis des Simple Network Management Protocol (SNMP). SNMP ist das standardisierte Netzwerkmanagement Protokoll der Internet-Welt. Ein Grundprinzip des Internet-Managements ist, daß Agenten die Netzwerkmanagement-Daten sammeln und einer zentralen Netzwerkmanagment-Station zur Verfügung stellen.

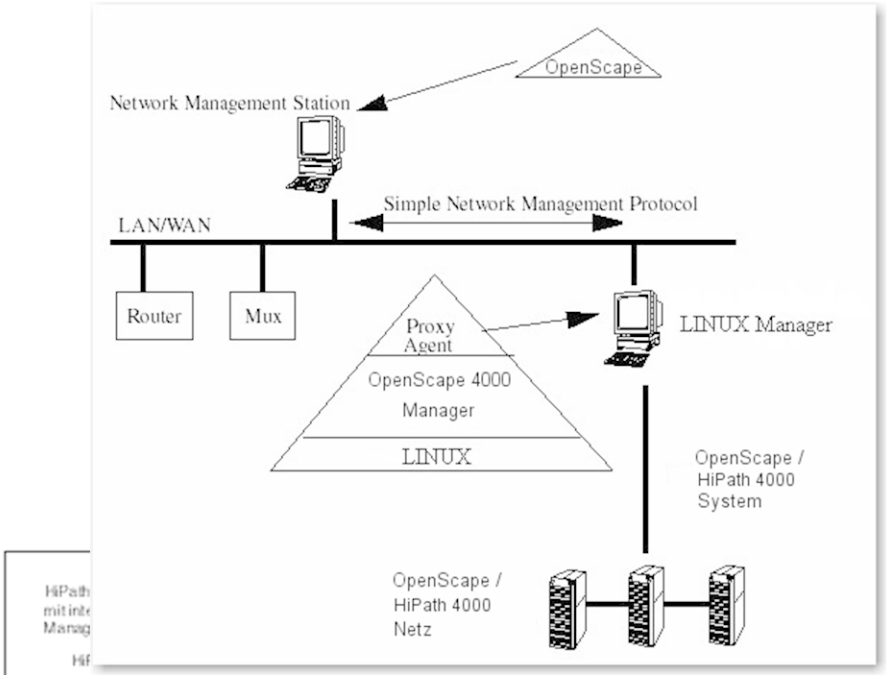


Abbildung 90: Komponentenstruktur des OpenScape SNMP Managements

Ein OpenScape/HiPath 4000-Netz besteht aus einer Anzahl von OpenScape/HiPath 4000-Systemen. Diese werden durch den OpenScape 4000 Manager verwaltet Der OpenScape 4000 SNMP Proxy Agent ist Bestandteil des OpenScape 4000 Manager-Installationspakets. Die OpenScape 4000-Anlage (AMO-Schnittstelle) und der OpenScape 4000 Manager bilden die Informationsbasis des OpenScape 4000 SNMP Proxy-Agenten. Die für das Management notwendigen Informationen werden durch den

OpenScape 4000 SNMP Proxy-Agenten in einer Management Information Base (MIB) modelliert bzw. zugreifbar gemacht. Die MIB wird von einer Netzwerkmanagement-Station überwacht bzw. ausgewertet. Zusätzlich werden SNMP Traps (z.B. Alarmmeldungen) vom OpenScape 4000 SNMP Proxy Agenten an die Netzwerkmanagement-Station (Station mit der OpenScape Netzwerkmanagement-Software) weitergeleitet.

8.3 OpenScape 4000 SNMP Proxy Agent

Die Installation des OpenScape 4000 SNMP Proxy Agent (Pakte: ASsnmp, ASfm) erfolgt automatisch im Rahmen der Installation der OpenScape 4000 Manager-Plattform.

8.3.1 Installationsinhalt

Der OpenScape 4000 SNMP Agent besteht aus verschiedenen Subagenten. Die Subagenten sind logischer Bestandteil (MIB) des EMANATE Master Agent, d.h. sie werden von diesem mit SNMP-Anforderungen (SNMP-Get, SNMP-Set etc.) versorgt und liefern die Ergebnisse via Master Agent an den SNMP-Requester zurück.

Im Einzelnen besteht der OpenScape 4000 SNMP Agent aus folgenden Subagenten bzw. Prozessen:

1) systemagt : Der System-Subagent verwaltet die Liste der bekannten OpenScape 4000-Anlagen mit ihren Systeminformationen und benachrichtigt andere Komponenten des OpenScape 4000 SNMP wenn Änderungen in dieser Liste entdeckt werden. Die Managerstation (OpenScape) wird mittels Traps über bestehende Änderungen informiert.

2) alarmagt : Durch diesen Agenten werden OpenScape 4000-Alarme bzw. Alarm-Filterkonfigurationen verfügbar gemacht. Der Alarm-Agent verschickt Traps, wenn sich Alarmzustände ändern.

3) erroragt: Über diesen Subagenten werden Informationen über angefallene Fehler des OpenScape/HiPath 4000-Netzwerkes zur Verfügung gestellt.

4) softagt: Der Software-Subagent macht Informationen über Softwareversionen und eingespielte Patches zugänglich.

5) hardagt: Mit Hilfe des Hardware-Subagenten können Informationen zur Hardwarekonfiguration einer OpenScape/HiPath 4000-Anlage über SNMP ausgelesen werden.

6) topoagt : Der Topologie-Subagent stellt die Informationen über den Netzaufbau zur Verfügung.

7) sqlagt : Mit Hilfe des SQL-Subagenten können umfangreiche Informationen aus der Datenbank des OpenScape 4000 Manager direkt über SNMP abgefragt werden.

8) disagt: Der Discovery-Subagent hat die Aufgabe, direkt über die AMO-Schnittstelle die Grundinformationen (HW, SW, Topologie, Alarmkonfiguration) zu einer OpenScape/HiPath 4000 abzufragen und diese in eine von den anderen Subagenten verarbeitbare Form umzuwandeln.

9) commonagt: Der Common Agent versorgt das Common Management Portal mit Informationen (System-Versionen, CPU-Auslastung, Speicherauslastung, Backup-Status, CM-Upload-Status).

10) hipathmgragt: Der Supervisor-Agent dient zur Verwaltung des OpenScape 4000 Manager (Prozess-Management, Festlegen von Intervallen für die Batch-Ausführung, Einrichten des Dateisystem-Speicherplatzmonitors).

11) mib2agt: Dieser Subagent liefert Informationen gemäß RFC-1213 (http://www.ietf.org/rfc/rfc1213.txt).

Anmerkung: Eine genaue Beschreibung der von den einzelnen Subagenten zur Verfügung gestellten Informationen können Sie bei Interesse aus der MIB entnehmen.

8.3.2 Test der Installation

Die Subagenten systemagt, alarmagt, erroragt, softagt, hardagt, topoagt, sqlagt, disagt, commonagt, hipathmgragtund mib2agt werden bei einer erfolgreichen Installation des OpenScape 4000 SNMP Proxy Agent automatisch gestartet.

Nach Durchführung der Installation sollte geprüft werden, ob die Subagenten laufen.Diese Prüfung wird wie folgt durchgeführt:

```
ps -ef | grep agt
```

Wenn alle Agentenprozeße laufen, sollte ungefähr folgende Ausgabe erscheinen.

```
root 6524 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
systemagt
root 7065 1 0 May16 ? 00:00:05 /opt/hipath_agents/bin/
alarmagt
root 7084 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
erroragt
root 7108 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
softagt
root 7125 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
hardagt
root 7146 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
topoagt
root 7163 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
sqlagt
root 7180 1 0 May16 ? 00:00:00 /opt/hipath_agents/bin/
disagt
root 18575 1 0 Jun06 ? 00:00:00 mib2agt
root 18577 18570 0 Jun06 ? 00:00:31 hipathmgragt
root 18581 18563 0 Jun06 ? 00:00:00 commonagt
root 27971 1 0 May25 ? 00:00:00 /opt/hipath_agents/bin/
portagt
```

Falls nicht alle Subagentenprozeße laufen, wurde der SNMP-Agent möglicherweise nicht korrekt installiert.

Nehmen Sie bitte folgenden Prüfungen vor:

Prüfen Sie, ob der EMANTE Master Agent läuft.

```
ps -ef | grep snmpdm
```

Wenn der Master Agent läuft, sollte folgende Ausgabe erscheinen.

```
root 18548 18540 0 Jun06 ? 00:00:00 snmpdm -d
```

8.4 Einrichten von Communities und Traps

Der SNMP-Agent muss konfiguriert sein, um SNMP-Traps (events) an OpenScape FM zu senden, sowie um OpenScape FM Lese- und Schreibzugriffe zu erlauben.

Diese Konfiguration kann über die Benutzeroberfläche Fault Management-> SNMP-Konfigurator erfolgen. Im lokalen Profil.

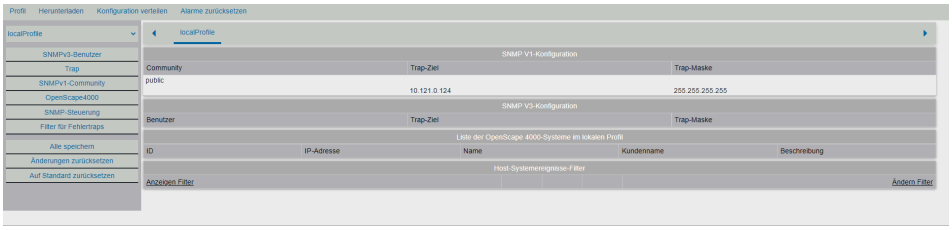


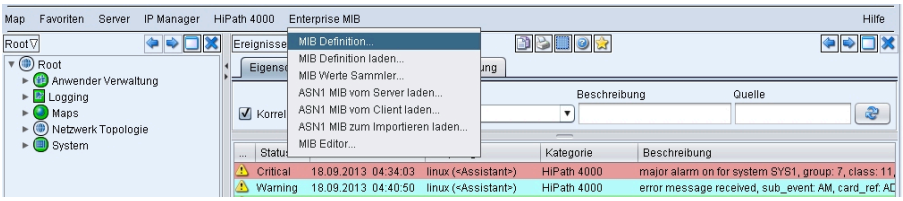
Abbildung 91: SNMP-Konfigurationsdaten (Beispiel)

Anmerkung: Dieselbe Community (z.B. ‘mib’ wie im Beispiel oben) muss im OpenScape FM gesetzt werden (Menüposition “...SNMP parameters...”) nachdem ein OpenScape 4000 Manager-System zum Netzwerk-Topologie zugefügt wurde. Falls die Communities nicht übereinstimmen, wird der Discovery-Vorgang den OpenScape 4000 Manager nicht als Typ OpenScape 4000 Manager entdecken (nur das PC-Symbol erscheint).

Um alle vom OpenScape 4000 Manager/Assistant in OpenScapeFM generierten Trap-Meldungen anzuzeigen, muss die PN-MIB (herunterladbar unter “Download MIB files --> Definitions (.mib)-Datei für die Hipath 4000 MIB herunterladen, Bild 6-2) über Enterprise MIB-> MIB Definitions in OpenScape FM aktiviert werden. Dabei ist zu beachten, dass diese MIB auch HiPath 4000 Alarm-Traps enthält, die bereits vom HiPath 4000-Plugin behandelt werden. Die Aktivierung der gesamten SIEMEMS-PN-MIB könnte also zu Doppeleinträgen in der Ereignisanzeige führen. Deaktivieren Sie nicht benötigte Traps über die Ereigniskonfiguration.

8.4.1 Schritt für Schritt:

1) Öffnen Sie das **OpenScape FM** Client-Fenster.
2) Öffnen Sie **Enterprise MIB-> MIB Definition**.

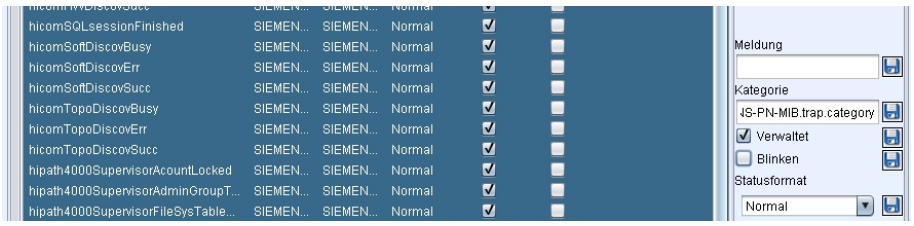


3) Wählen Sie die Datei **SIEMENS-PN-MIB Enterprise MIB** aus und klicken Sie auf die Schaltfläche **Aktivieren**.

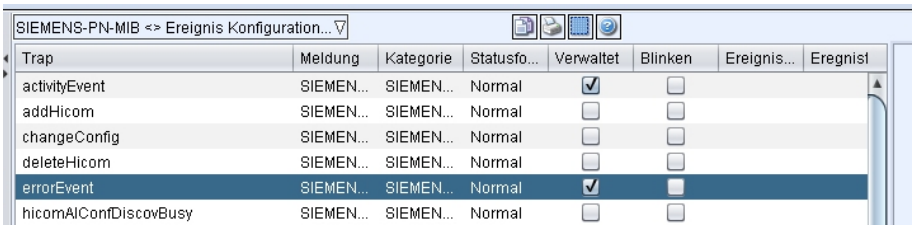
4) Klicken Sie auf die Schaltfläche **Ereignis Konfiguration**, um das Fenster **Ereigniskonfiguration** anzuzeigen.

5) Klicken Sie auf **Alle Einträge auswählen**.

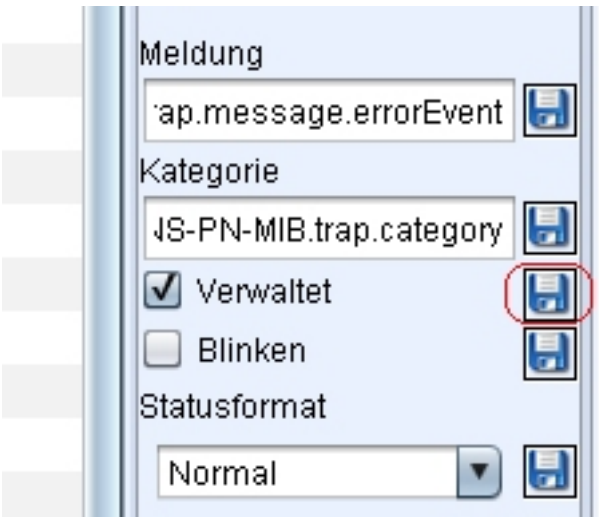
6) Deaktivieren Sie das Kontrollkästchen **Verwaltet** und klicken Sie auf die Schaltfläche **Speichern**.



7) Markieren Sie in der Spalte **Verwaltet** die Einträge **activityEvent**, **errorEvent** und **syslogMessage**.



8) Klicken Sie auf die Schaltfläche **Speichern**.



8.5 Verwendete AMO-Kommandos

Die von den einzelnen Subagenten über die MIB zur Verfügung gestellten Daten werden teilweise aus der OpenScape 4000 Manager-Datenbank unmittelbar entnommen. Ein größerer Teil dieser Daten wird jedoch direkt aus den Ausgaben verschiedener AMO-Befehle gewonnen und während des Discovery-Vorgangs in einem eigenen Bereich der OpenScape 4000 Manager-Datenbank abgespeichert. Tabelle 8 führt die benutzten AMOÂ´s und die daraus extrahierten Daten auf.

Tabelle 6: Aus AMOs extrahierte Daten

AMO	Extrahierte Information	Subagent
APS	Programmsystem, Sachnummer	softagt
BCSM	Modul, Slotadr., Soll-BG, HW-Abk., Ist-BG, Firmware, Stand, BG-Zustand	hardagt
BCSU	LTU, LTG, Soll-BG, Ist-BG, Typ, Stand, Firmware, BG-Zustand	hardagt
BUEND	Bündelnr., Bündelname, Max. Anzahl, Gerätetyp	topoagt
CDSM	Schrankadresse, Einbauebene, EBT, Ist-BG, HW-Abk., Stand, Firmware	hardagt
CDSU	Schrankadresse, Einbauebene, EBT, Ist-BG, HW-Abk., Stand, Firmware	hardagt
CONSY	Shelfno., Frame, PID1, PID2, PID3, LTU	hardagt
DDSM	Controller, Typ, Größe, SS-NO, GRAN	hardagt
PATCH / PATAD	Patchgruppe, Patchnummer, Aktivierungszustand, HD/RAM	softagt
TACSU	Lage, GER, BUNR, SATZNR, INBETR, KNNR, ALARMNR	topoagt
TDCSU	Lage, GER, BUNR, BKANAL, BKGR, INBETR, ALARMNR	topoagt
TSCSU	LAGE, GER, BUNR, SATZNR, INBETR, KNNR, ALARMNR	topoagt
VADSM	ALARMGRUPPE, ALARMNR, SCHWELL1, SCHWELL2, ZEIT1, ZEIT2, NAME	erroragt
VADSU	ALARMGRUPPE, ALARMNR, SCHWELL1, SCHWELL2, ZEIT1, ZEIT2, NAME	erroragt
KNTOP	ltg, ltu, slot, satznr, bkanalgrp, p_nodeindex, p_ltg, p_ltu, p_slot, p_satznr, p_bkanalgp, p_nodeno, bunr	topoagt
KNDEF	vknnr, def_vknnr	topoagt
APRT	ipaddr	hardagt
ZAND (FUNCT)	KNNR, LANGUAGE	systemagt

AMO	Extrahierte Information	Subagent
SBCSU	tel_nr,pen	hardagt
PERSI	location	hardagt
GRA	Upload Alarm Mirror, Reset Alarm	Alarmagent

8.6 Zeitgesteuerte Alarmmeldungen

Das vorliegende Kapitel beschreibt die Administration bzw. den Gebrauch der Scripte read_filter.ksh und set_filter.ksh um Alarmmeldungen der OpenScape 4000 Proxy Agenten zeitgesteuert filtern zu können. Insbesondere wird die Installation, Konfiguration und Inbetriebnahme der Software beschrieben.

8.6.1 Allgemeine Hinweise

Die Realisierung zeitgesteuerte OpenScape 4000 Alarmmeldungen ist eine Erweiterung des OpenScape 4000 Proxy Agent. Eine der Funktionen des OpenScape 4000 Proxy Agent ist es OpenScape 4000 Alarmmeldungen an das OpenScape FM weiterzuleiten. Mit der Erweiterung zur Realisierung zeitgesteuerter OpenScape 4000 Alarmmeldungen am SNMP Proxy Agent kann die Weiterleitung und Anzeige bestimmter OpenScape 4000 Alarmmeldungen zu konfigurierten Zeiten deaktiviert bzw aktiviert werden. Die Umsetzung wurde auf Basis des bereits existierenden Filtermechanismus des SNMP Proxy Agent für Alarmmeldungen realisiert.

Das Filter-Handling kann über SNMP get/set-Anforderungen oder Skripte gesteuert werden:

- /opt/hipath_agents/bin/read_filter.ksh
- /opt/hipath_agents/bin/set_fileter.ksh

Diese Skripte verkapseln get/set-Anfragen mit "privaten>Community-Einträgen und verwalten cron-Einträge, um SNMP-Traps anhand der an diese Skripte als Argumente übergebenen Konfigurationsdateien zu filtern.

Beispielkonfigurationsdateien:

- /opt/hipath_agents/bin/conf/activate.cnf
- /opt/hipath_agents/bin/conf/filter_demo.cnf
- /opt/hipath_agents/bin/conf/feiertag_demo.cnf

Um diese Skripte verwenden zu können, muss der SNMP v1 "private" Community-String konfiguriert sein (siehe Abschnitt 6.4, "Einrichten von Communities und Traps").

8.6.2 Programmablauf

Der Mechanismus zur Steuerung der Alarmfilter beruht im wesentlichen auf zwei Scripte. Das Script read_filter.ksh dient zum Auslesen der Ausführungsdatei activate.cnf. Diese definiert die Aktivierungs- bzw. Deaktiverungs-Zeitpunkte der zu filternden Alarmmeldungen. Der Name der Ausführungdatei ist fix. Die in ihr beschriebenen

Aktivierungszeitpunkte für die Filter werden mit den entsprechenden Parametern (Filter-,Feiertagsdatei,Aktivierungsflag) zu einem Befehl geformt und als Cronjob abgelegt. Es können dabei verschiedene Dateien für die Filter und Feiertage genutzt werden. Die Namen der dabei genutzten Dateien für die Filter und Feiertage sind frei. Die Dateien selber müssen jedoch genau wie die Ausführungsdatei activate.cnf in dem Verzeichnis /opt/hipath_agents/conf abgelegt werden. Wird der durch das Script read_filter.ksh in die Crontabelle geschriebenen Cronjob aktiviert, wird das Script set_filter.ksh aufgerufen. Dieses Script aktiviert bzw. deaktiviert aufgrund der Parametern des Cronjobs einerseits die Filter für die Alarmmeldungen über ein SNMP-Set und pflegt anderseits die Datei "filter_state", die den Status der gesetzten Filter für eigene Zwecke sichert.

Wichtig zu beachten ist, daß jede Filterdatei in der Ausführungsdatei als eine Art Filtergruppe angesehen wird. Die Filter einer solchen Filtergruppe/-datei können,wenn sie einmal gesetzt wurden, nur mit derselben Filtergruppe/-datei deaktiviert werden. Zusätzlich gilt ausserdem, daß nur Filter zurückgesetzt werden, die nicht durch eine weitere Filtergruppe/-datei gesetzt wurden. D.h. wurden z.B 6 Alarmfilter über 2 Filterdateien "filtergrp1[1,2,3,4]", "filtergrp2 [3,4,5,6]" gesetzt. Dann werden bei einer Deaktiveriung über die Filterdatei "filtergrp1>nur die Alarmfilter 1,2 zurückgesetzt, da die Alarmfilter 3 und 4 auch Bestandteil der Filterdatei "filtergrp2>sind.

Anmerkung: Durch Setzen eines Filter über diesen Mechanismus wird der vorherige Status des Filters unwiderbringlich überschrieben.

8.6.3 Hinweise zur Anwendung

Voraussetzung für die Nutzung der Software ist, daß die Agenten sowie der Emanate Master Agent zu den Aktivierungszeitpunkten laufen. Desweiteren muß die Schreib-Community in dem File set_filter.ksh entsprechend der Konfiguration des Emanate Master Agenten gesetzt sein.

Die Software kann dann durch die folgenden zwei Schritte aktiviert werden:

1) Konfiguration der Auführungsdatei "activate.cnf",sowie der diversen Filter und Feiertagsdateien. Näheres siehe Abschnitt 6.6.4, "Ausführungsdatei", Abschnitt 6.6.5, "Alarmfilterdatei" bis Abschnitt 6.6.6, "Feiertagsdatei".

2) Starten des Scripts read_filter.ksh.

Nach jeder Änderung der Konfigurationsdateien ist ein Ausführen des Scripts read_filter.ksh vonnöten um die Cron-Tabelle auf den neuesten Stand zu bringen.

8.6.3.1 Beispiel Konfiguration

Angenommen wir wollen, daß für die Anlage mit der Pabx_id 10002 jeden Montag, ausser dieser ist ein Feiertag, um 10 Uhr ein Alarmfilter für den Alarm mit der Gruppe 3 Klasse 33 und Priorität Major gesetzt wird. Desweiteren, daß dieser an einem Feiertags Dienstag um 12 Uhr wieder zurückgesetzt wird.

Dann müssen wir folgenden Konfiguration vornehmen.

Filterdatei "filter.cnf":

100002 3 33 2 // Alarm der gefiltert werden soll

Die Feiertagsdatei ist in diesem Fall nicht relevant, muß aber vorhanden sein z.B.:

Feiertagsdatei "feiertag.cnf":

// Dies ist die Feiertagsdatei 01.11.2005 // Allerheiligen 24.12.2005 // Heiligabend

Um die Filter zu den beabsichtigten Zeitpunkte zu aktivieren bzw. reaktivieren müssen folgenden Einträge in der Ausführungsdatei "activate.cnf>geschrieben werden:

mo 10:00 filter.cnf feiertag.cnf false true di 12:00 filter.cnf feiertag.cnf true false

Nach Konfiguration des Konfigurationfile muß nun das Script read_filter.ksh ausgeführt werden z.B. mit dem Kommando "/opt/hipath_agents/bin/ read_filter.ksh"

Diese Befehl erzeugt in der Cron-Tabelle nun die zuzätzlichen Einträge:

00 10 * * 1 /opt/hipath_agents/bin/set_filter.ksh filter.cnf feiertag.cnf false true 00 12 * * 2 /opt/hipath_agents/bin/set_filter.ksh filter.cnf feiertag.cnf true false

Zu den entsprechenden Zeitpunkte wird dann das Script set_filter.ksh aufgerufen, das die entsprechenden Filter setzt bzw. zurücksetzt.

8.6.3.2 Administration der Scripte

Hier werden Variablen innerhalb der Scripte read_filter.ksh und set_filter.ksh vorgestellt, die das Verhalten der Scripte beeinflussen.

Community:

Die Community in dem File set_filter.ksh muß entsprechend den Einstellungen des Emanate Master eingestellt werden. Diese Community muß Schreibrechte auf die OpenScape 4000 MIB haben. Als Defaultwert ist hier "private" eingetragen. Dies sollte entsprechend nach der Installation geändert werden.

DBG_FLAG:

Wird diese Flag in den Scripte auf 0 (on) gesetzt werden, diverse Debugausgaben in der Datei /tmp/set_filter.log bzw /tmp/read_filter.log abgelegt. Mit Setzen des Wert auf 1 (off) wird diese Funktion wieder deaktiviert.

8.6.4 Ausführungsdatei

Jede Zeile der Ausführungsdatei /opt/hipath_agents/conf/activate.cnf definiert einen Deaktivierungs- oder Aktivierungszeitpunkt. Hier ist darauf zu achten, daß die einzelnen Aktivierungspunkte zeitlich auseinander liegen. Ansonsten kann es zu Fehlern bei der Auswertung kommen.

Die Datei ist dabei folgendermassen aufgebaut:

// Kommentar

oder

Wochentag { mo | di | mi | do | fr | sa | so | all } Uhrzeit {HH:MM} Alarmfilterdatei Feiertagdatei Feiertagsflag{true|false} Aktivierungsflag{true|false}

Die Einträge in einer Feiertagsdatei müssen durch den Kunden manuell gepflegt werden. Ein Beispiel:

mo 10:00 filter.cnf feiertag.cnf false true

Dies würde bedeuten die Alarme aus der Datei filter.cnf würden jeden Montag um 10 Uhr aktiviert werden, es sei denn es wäre ein Feiertag aus der Feiertagsdatei feiertag.cnf.

all 10:00 filter.cnf feiertag.cnf true false

Dies würde bedeuten die Alarme aus der Datei filter.cnf würden jeden Tag um 10 Uhr deaktiviert werden, wenn es ein Feiertag aus der Feiertags datei feiertag.cnf wäre.

8.6.5 Alarmfilterdatei

Jede Zeile einer Alarmfilterdatei definiert einen Alarm, für den der Filter je nach Aufruf des Scripts an- oder ausgeschaltet wird.

Das Format der Zeile ist folgendermaßen aufgebaut:

// Kommentar

oder

PabxId AlarmGruppe AlarmNummer Priorität // Kommentar

Die Werte für das Feld Priorität sind folgendermaßen zugeordnet:

1 -> minor

2 -> major

3 -> device

Die Einträge in der Alarmfilterdatei müssen durch den Kunden manuell gepflegt werden.

Beispiel:

// Dies ist die Filterdatei

10 1 1 1 // KOELN CC Restart Minor

10 1 1 2 // KOELN CC Restart Major

8.6.6 Feiertagsdatei

Jede Zeile einer Feiertagsdatei definiert einen Feiertag. Das Format der Zeile ist folgendermaßen aufgebaut:

// Kommentar

oder

TT.MM.JJJJ // Kommentar

Wobei TT für Tag, MM für Monat und JJJJ für Jahr steht

Die Einträge in einer Feiertagsdatei müssen durch den Kunden manuell gepflegt werden.

Beispiel:

// Dies ist die Feiertagsdatei

01.11.2005 // Allerheiligen

24.12.2005 // Heiligabend

25.12.2005 // 1. Weihnachtsfeiertag

26.12.2005 // 2. Weihnachtsfeiertag

31.12.2005 // Silvester

01.01.2006 // Neujahr

8.6.7 Alarm-Filter-Handling über SNMP

Sie können interne Skripte zum Filtern von OpenScape 4000 Proxy-Alarm-Trap-Meldungen verwenden; Sie können aber auch SNMP-Set-Anforderungen einsetzen, um permanente Filter zu definieren.

Der Filter wird mithilfe von SNMP-Set-Anforderungen in folgendem OID-Format definiert, mit der Einstellung “4” (Integer):

.1.3.6.1.4.1.231.7.2.1.2.3.1.6.pabxid.AlGroup.AlSubID.AlPriority

Hierbei ist AlPriority definiert als: 1 .. minor, 2 .. major, 3 .. device.

Nach Erstellung des Eintrags ist der Filter automatisch aktiv.

Die gleiche SNMP-Set-Anforderung mit der Einstellung “6” (Integer) löscht den Filter aus der Filtertabelle.

Um den Filter zu aktivieren bzw. zu deaktivieren, verwenden Sie eine SNMP-Set-Anforderung in folgendem OID-Format:

.1.3.6.1.4.1.231.7.2.1.2.3.1.5.pabxid.AlGroup.AlSubID.AlPriority

Die Einstellung “2” (Ganzzahl) deaktiviert den Alarm; die Einstellung “1” (Integer) aktiviert ihn.

Beispiel:

Sie möchten den Trap für den folgenden Alarm (Manager-Alarm SWA_ACTIVATION_FAILED) filtern:

hicomAlPabxId	hicomAlGroup	hicomAlSubId	hicomAlPriority
1	7	101	major

Abbildung 92: Alarme filtern

Definieren Sie hierzu die folgende Anforderung:

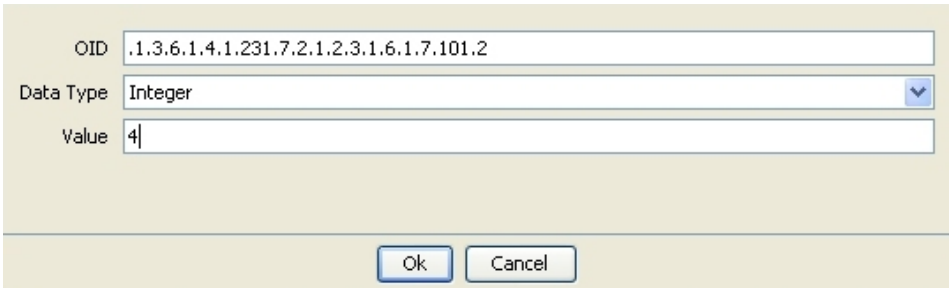


Abbildung 93: SNMP-Anforderung definieren (Beispiel)

Um diesen Filter zu deaktivieren, setzen Sie den Wert für den Datentyp (Integer) auf “2”:

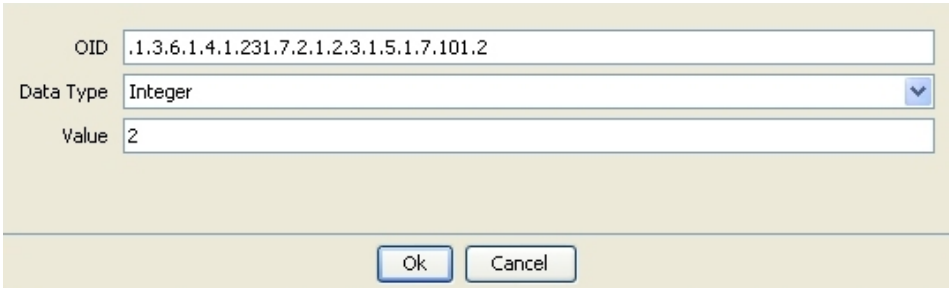


Abbildung 94: SNMP-Anforderung definieren (Beispiel)

Die Liste der definierten Filter und deren Status sind in der Tabelle SNMP hicomFiltAlConfTable im Format OID .1.3.6.1.4.1.231.7.2.1.2.3 aufgeführt.

8.7 Lokale Alarme im OpenScape 4000 Manager einrichten

Bearbeiten Sie die Datei /opt/ncc/bin/options durch Ändern der Zeile
`#STORE_LOG=ON;export STORE_LOG`

in
`STORE_LOG=ON;export STORE_LOG`

Danach werden die folgenden neuen Alarme im OpenScape 4000 Manager generiert:

```
RETRY EXCEEDED: Col could not fetch CDR file
NOT ENOUGH SPACE: No Space for Performance Management
SWITCH ACCESS FAILING: Polling of OpenScape/HiPath failed
 (activation project specific)
DB FULL: Informix DB reached high water
INFORMIX: General DB problems
DISK FULL: No Disk space
AFR DB SPACE : Database Threshold reached: Inserting error
 messages into Database table "lerror>was stopped
AFR STOPPED : No alarm and error messages will be received
 because AFR was stopped on RMX side
AFR FAULT : An error occured during analysis of received
 AFR message
AUTOLCK: User account automatically locked
BACKUP FAILED : An error occured during data backup
RESTORE FAILED : An error occured during restore of data
```

```
DISK FULL : Disc space has reached threshold level
THRESH. EXCEEDED : Database of PM has reached threshold
 level
```

Anmerkung: Auf dem Manager können noch weitere Alarme generiert werden. Zur Aktivierung dieser Alarme, siehe Kapitel 6, "Erweiterte SNMP-Alarme zur Überwachung des Managers".

8.8 Überwachen von Manager über SNMP – HiPath Supervisor Agent

Der HiPath Supervisor Agent bietet SNMP-Unterstützung für den OpenScape 4000 Manager, sodass die Ressourcen des Managers überwacht werden können.

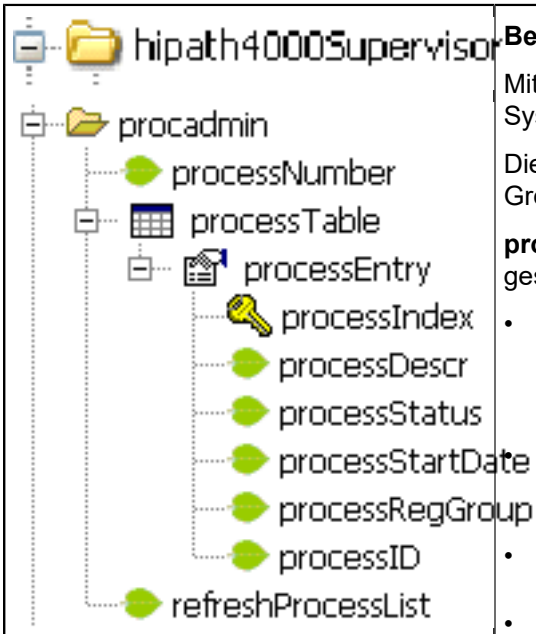
Der SNMP Agent ermöglicht die Remote-Überwachung der folgenden Prozesse und Zustände:

- Systemprozesse auf dem Manager
- Dateisysteme
- Proxy-Agenten
- Erreichen des PM-Datenbank-Schwellwerts
- LogM
- LMT-Statusübersicht
- Zu aktivierende bzw. deaktivierende COL-Backup-Einstellungen
- dipasBatch-Parametereinstellungen
- Fehler und Alarme

Der HiPath Supervisor Agent arbeitet mit der OpenScape 4000 MIB (Management Information Base; siehe Section 6.8.1).

Die MIB kann vom SNMP-Konfigurator heruntergeladen werden (siehe Section 6.4).

8.8.1 MIB-Tabelle für den HiPath 4000 Supervisor Agent



Beschreibung

Mit dem HiPath Supervisor Agent können Sie Informationslisten zu Systemprozessen und deren Status anzeigen.

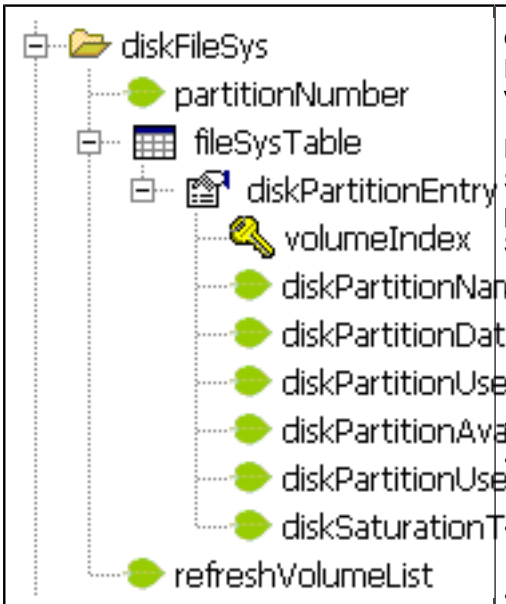
Die Ergebnisse werden an die SNMP **processTable** übertragen; die Größe ist in **processNumber** definiert.

processEntry enthält Informationen über bestimmte von **procadmin** gesteuerte Prozesse. Dabei treten die folgenden Elemente auf:

- **processIndex** ist ein eindeutiger Wert für jeden Prozess. Er liegt im Bereich zwischen ‘1’ und dem Wert processNumber . Der Wert für jeden Prozess muss mindestens von einer Reinitialisierung der Prozessinstanz bis zur nächsten gleich bleiben.
- **processDescr** ist eine Textzeichenfolge mit Informationen über den Prozess. Diese Zeichenfolge sollte den Namen des von procadmin angezeigten Prozesses enthalten.
- **processStatus** ist der Status des von procadmin angezeigten Prozesses.
- **processStartDate** zeigt das Datum und die Uhrzeit, zu der der Prozess gestartet wurde.
- **processRegGroup** ist die Registrierungsgruppe, zu der der Prozess gehört.
- **processID** ist die ID des Prozesses, die vom Betriebssystem bereitgestellt wird. Wenn ein Prozess nicht läuft, erscheint ‘record about pid’ in der Tabelle mit dem Wert ‘0’.

Alle Zeilen in **processTable** werden im Speicher gehalten. Bei jeder ‘get’- oder ‘get-next’-Abfrage werden die aktuellen Daten zurückgegeben, die Anzahl der Prozesse bleibt jedoch unverändert. Der Abfragetyp ‘get’ kann nur bei Elementen verwendet werden, die bereits über ‘get-next’ geladen wurden.

Falls eine **processRegGroup** deinstalliert wird, wird in der Tabelle eine leere Zeile mit PID=0 verarbeitet. Um die gesamte Tabelle neu zu laden, muss der Wert **refreshProcessList** auf ‘1’ gesetzt werden.



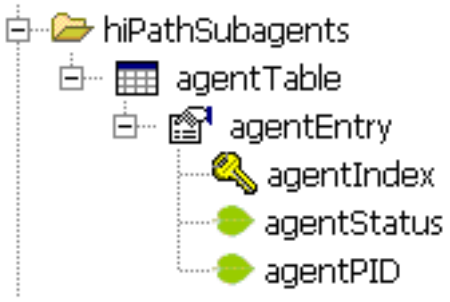
diskFileSys dient zum Überwachen des Dateisystems der Festplattenpartition sowie der Speicherauslastung des Partitions-Volumes.

Die Tabelle **fileSysTable** wird aus den Informationen über den Systembefehl df -kP erstellt, während die Zeilenanzahl durch **partitionNumber** festgelegt wird. Die Tabelle enthält die folgenden Spalten:

- **volumeIndex** ist ein eindeutiger Wert für jedes Volume. Er liegt im Bereich zwischen ‘1’ und dem Wert partitionNumber. Der Wert für jedes Volume muss mindestens von einer Reinitialisierung der Volume-Instanz bis zur nächsten gleich bleiben.
- **diskPartitionName** ist der Name der Festplattenpartition.
- **diskPartitionDataBlocs** bezeichnet die Datengröße des Volumes auf der Festplattenpartition (in KB).
- **diskPartitionUsed** ist der belegte Speicherplatz auf der Festplattenpartition (in KB).
- **diskPartitionAvailable** ist der verfügbare Speicherplatz auf der Festplattenpartition (in KB).
- **diskPartitionUsePercent** ist der Wert für den freien Speicherplatz auf der Festplattenpartition, angegeben in Prozent.
- **diskSaturationThreshold** ist der Schwellwert für die Auslastung des Festplatten-Volumes in Prozent. Scanvorgänge finden in 30 Sekunden-Intervallen statt, wenn **diskPartitionUsePercent** gleich oder größer **diskSaturationThreshold** ist.

Später werden Trap-Meldungen zu diesen Vorgängen gesendet. Der Wert für diskSaturationThreshold kann mittels SNMP-Anforderung auf 0 bis 100% gesetzt werden. Wenn ein Kunde den Schwellwert auf 0 gesetzt hat, wird die Überwachung der Auslastung für diese Festplattenpartition deaktiviert.

Die Reinitialisierung der Dateisystem-Tabelle fileSysTable kann gestartet werden, indem in refreshVolumeList der Wert ‘1’ festgelegt wird.



hiPathSubagents ermöglicht die Überwachung und Bearbeitung der Status für die folgenden SNMP-Daemons:

– systemagt (1)

– alarmagt (2)

– erroragt (3)

– softagt (4)

– hardagt (5)

– topoagt (6)

– sqlagt (7)

– disagt (8)

– portagt (9)

– mib2agt (10)

- **agentIndex** ist ein eindeutiger Wert für jeden Subagenten.
- **agentStatus** ist der Status eines bestimmten Subagenten und kann zum Stoppen bzw. Starten des Subagenten verwendet werden. Mittels SNMP-Set-Anforderung kann einer der folgenden drei Status eingestellt werden: ’running’ (läuft) (1), ’stopped’ (angehalten) (2), ’restart’ (Neu starten) (3).
- **agentPID** ist die Prozess-ID eines bestimmten Subagenten.

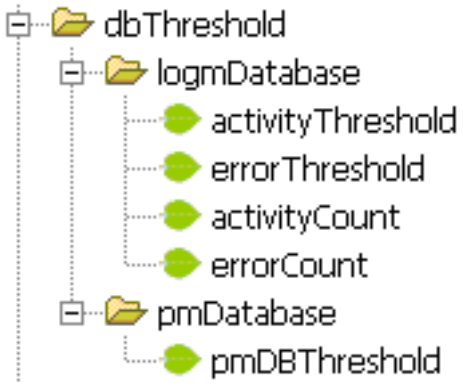
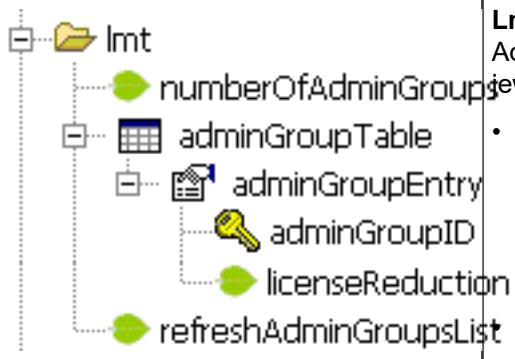
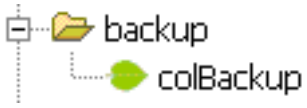
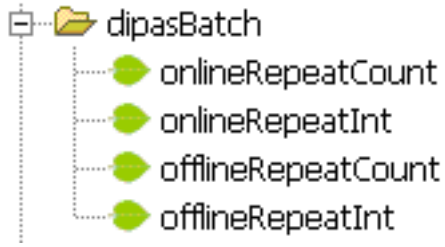
Die Tabelle agentTable kann aktualisiert werden.

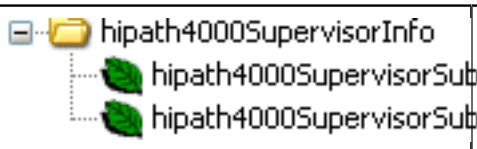
Die Operationen ‘Start/Neustart’ können zu einem Neustart führen oder durch den Neustart eines anderen Proxy-Agenten verursacht werden. Dabei sind folgende Abhängigkeiten zu beachten:

1) *sqlagent* und *portagent* arbeiten ohne irgenwelche Abhängigkeiten. Sie können einzeln neu gestartet werden, ohne dass andere Subagenten beinträchtigt werden.

2) *softagt , topoagt , hardagt , alarmagt , erroragt* und *disagt* sind vom Systemagenten abhängig. Sie werden nach einem Neustart von systemagt automatisch neu gestartet. In diesem Fall wartet die Set-Anforderung (set_request) nicht auf einen Neustart aller Proxy-Agenten, sondern initiiert sofort einen Neustart, und gibt bei erfolgreicher Durchführung eine dementsprechende Meldung aus. Der Grund hierfür liegt darin, dass der Systemagent zirka eine Minute für einen sauberen Start benötigt, erst danach werden die anderen Subagenten gestartet.

3) Beim Discovery-Agent (*disagt*) gibt es Abhängigkeiten zu *softagt* , *topoagt* , *hardagt* und *erroragt* . Dies bedeutet, dass der Discovery-Agent (disagt) beim Neustart eines dieser Agenten automatisch neu gestartet wird.

	**logmDatabase** • **activityThreshold** ist der für die Aktivitätstabelle der LogM-Datenbank festgelegte Schwellwert. • **errorThreshold** ist der für die Fehlertabelle der LogM-Datenbank festgelegte Schwellwert. • **activityCount** ist die Anzahl der Einträge für die Aktivitätstabelle der LogM-Datenbank. • **errorCount** ist die Anzahl der Einträge für die Fehlertabelle der LogM-Datenbank. **pmDatabase** • **pmDBThreshold** ist der für die Fehlertabelle der LogM-Datenbank festgelegte Schwellwert. Wenn ein Datenbank-Schwellwert erreicht ist, wird ein entsprechender Trap gesendet.
	**Lmt** zeigt die von LMT verwaltete Tabelle mit den Administrationsgruppen. Diese Tabelle enthält Informationen zur jeweiligen Administrationsgruppe. • **adminGroupID** ist die eindeutige ID einer bestimmten Administrationsgruppe.Zulässig sind Werte zwischen 1 und dem Wert für **numberOfAdminGroups** . Der Wert für jede Administrationsgruppe muss mindestens von einer Reinitialisierung der Gruppeninstanz bis zur nächsten gleich bleiben. • **licenseReduction** ist die vom LMT angewendete Lizenzreduzierung in Prozent. Die Reinitialisierung kann initiiert werden, indem der Wert für **refreshAdminGroupsList** auf ‘1’ gesetzt wird.
	• **colBackup** gibt den Status der AScol-Backup-Komponente an. Der Status kann geändert werden, indem die Anforderung auf einen der folgenden Werte gesetzt wird: – ‘activated’ (aktiviert) (1) oder – ‘deactivated’ (deaktiviert) (2)
	**dipasBatch** • **onlineRepeatCount** Wiederholungszähler für die Online-Stapelverarbeitung (FAMOS-Verbindung). • **onlineRepeatInt** Wiederholungsintervall in Minuten für die Online-Stapelverarbeitung (FAMOS-Verbindung). • **offlineRepeatCount** Wiederholungszähler für die Offline-Stapelverarbeitung (Filetransfer). • **offlineRepeatInt** Wiederholungsintervall in Minuten für die Offline-Stapelverarbeitung (Filetransfer).

	Wenn der HiPath Supervisor-Subagent aktiv ist, führt er Überprüfungen auf Ausnahmen, Fehler und Warnmeldungen durch. Dabei stehen folgende Optionen zur Verfügung: • **hipath4000SupervisorSubagentLastMsgNo** ist die Nummer der letzten vom Supervisor-Subagent übergebenen Meldung oder Warnmeldung bzw. des letzten von ihm übergebenen Fehlers. • **hipath4000SupervisorSubagentLastMsgText** ist der Text der letzten vom Supervisor-Subagent übergebenen Meldung oder Warnmeldung bzw. des letzten von ihm übergebenen Fehlers.

8.8.2 Erweiterte SNMP-Alarme zur Überwachung des Managers

Im Zusammenhang mit der Einführung des erweiterten OpenScape Manager Agent werden auch zusätzliche Alarme zur Überwachung von Prozessen auf dem Manager eingeführt. Diese Alarme werden vom *alarmagt* verarbeitet.

Demzufolge werden auch diese Alarme in Alarm-/Fehlertabellen aufgeführt. Die zu diesen Alarmen gehörigen Alarm-/Fehlertraps können an zuvor definierte Trap-Ziele versendet werden. Die Alarme können dann anschließend durch OpenScape Fault Management oder einen anderen SNMP-Client bearbeitet werden.

8.8.2.1 Manager konfigurieren, um Alarme zu versenden

Um sicherzustellen, dass der Manager diese Alarm-Traps versenden kann, müssen zunächst folgende Konfigurationsschritte durchgeführt werden:

1) Konfigurieren Sie Communities und Trap-Ziele wie in Abschnitt 6.4, "Einrichten von Communities und Traps" beschrieben.

2) Aktivieren Sie die Manager-Alarmüberwachung, indem Sie die Auskommentierung einer Zeile in `/opt/ncc/bin/options` rückgängig machen:

Ändern Sie
```
#MANAGER_TRAP=ON; export MANAGER_TRAP
```
in
```
MANAGER_TRAP=ON; export MANAGER_TRAP
```

8.8.2.2 Erweiterte auf dem Manager generierte Alarme

License Management Tool (LMT)-Alarme

LMT_CDW_UPDATE	Das LMT kann das Codewort für die Anla aktualisieren
LMT_LICENSE_REDUCTION	Das LMT startet die Lizenzreduzierung in Administrationsgruppen
LMT_GLOBAL_ALARM_THRESHOLD	Der Alarmschwellwert wird für eine der Administrationsgruppen eingestellt

LMT_GLOBAL_ALARM	'Global_Alarm' wird im LMT einges
LMT_GLOBAL_WARNING_THRESHOLD	Der Warnschwellwert wird für eine Administrationsgruppen eingestellt
LMT_GLOBAL_WARNING	'Global_Warning' wird im LMT eing

Anmerkung: Die Liste aller Administrationsgruppen und ihre Status können mithilfe von SNMP Get-Anforderungen an die LMT-Tabelle in der erweiterten OpenScape 4000 MIB erfasst werden.

Procadmin-Alarme

Der Prozessadministrations-Daemon **procadmin** (Daemons in der MIB **processTable**) generiert Alarme, wenn einer der überwachten Daemons sich im Zustand inaktiv befindet.

Das Format des Alarms ist PROCM_DAEMONNAME (z. B. PROCM_CMPROC_CCS).

Anmerkung: Die Liste aller überwachten Daemons und ihre Status können mithilfe von SNMP Get-Anforderungen an die Tabelle **processTable** in der erweiterten OpenScape 4000 MIB erfasst werden.

Datenbanktabellen-Alarme

LOGM_ACTIVITY_TABLE_THRESHOLD	ist der in der Aktivitätstabelle erreichte Schwellwert
LOGM_ERROR_TABLE_THRESHOLD	ist der in der Fehlertabelle de erreichte Schwellwert
PM_DATABASE_THRESHOLD	ist der in der PM-Datenbank e

Anmerkung: Schwellwerte können über SNMP in der dbThreshold-Gruppe der erweiterten OpenScape 4000 MIB festgelegt werden.

OpenScape 4000 Manager-Backup-Alarme

HBR_DATA_BACKUP	Datensicherung ist fehlgesch

Wenn die logische Sicherung der Daten fehlschlägt, haben die Alarme das Format HBR_LOGICAL_BACKUPUNIT, z. B. HBR_LOGICAL_CDB

FM_COMMANDFILE_SEND

Der AMO-Auftrag kann nicht an die Anlage gesendet werden.

SSO_REPLICATION

Die Replikation während des Smart Switchover (SSO) war nicht erfolgreich.

SWA_ACTIVATION_FAILED

Die Aktivierung des Major/Minor/FixRelease oder des Hotfix schlug fehl.

CM_DB_SYNCH

Die Synchronisierung der Datenbank mit der Anlage war nicht erfolgreich.

PM_REPORT

Der zeitgesteuerte Reporterstellung durch Performance Management war nicht erfolgreich.

Collecting Agent-Alarme

COL_FETCH	Abruf von der Anlage (fetch-Anforderung) schlug feh
COL_RECEIVE	Konvertierung der empfangenen Datei (transform-A schlug fehl
COL_OUTPUT_FILE_PROD	Erstellung der Ausgabedatei schlug fehl
COL_PARTITION_FILLED	Abruf (fetch-Anforderung) wurde deaktiviert, da das Verzeichnis voll ist

Lizenzverwaltungsalarme

LICM_LICENSE_EXCEEDED	Die OpenScape 4000-Lizenz ist ausgeschöpft.

Die Lizenzverwaltung generiert Alarme ausgehend vom Zustand der Portzähler und ihrer Schwellwerte. Folgende Alarme können generiert werden:

- LICM_PORTCOUNT_EXCEEDED
- LICM_OS4K_PORTCOUNT_WARN_REACHED

DISK_SATURATION_THRESHOLD

Der Schwellwert auf einer der überwachten Festplattenpartitionen wurde erreicht.

Anmerkung: Die Partitionsauslastungsschwellwerte können über SNMP in der Tabelle fileSysTable der neuen OpenScape 4000 MIB festgelegt werden.

---

9 Neue SNMP-Leistungsmerkmale/Erweiterungen seit V7R2

Dieses Kapitel beschreibt die Anforderungen und die Architektur SNMP-Leistungsmerkmale für OpenScape 4000 Manager und Assistant V10 R1.

9.1 Verbesserte Alarm- und Fehlerbehandlung in OpenScape 4000

Mit diesem Leistungsmerkmal können Benutzer folgende Aktionen durchführen:

1) SNMPv3-Parameter für alle Hosts über den Assistant konfigurieren
2) SNMPv3-Konfigurationseinstellungen auf dem Hostportal überprüfen
3) hostMIF-Trap-Filter für alle Hosts über den Assistant konfigurieren
4) hostMIB-Trap-Filter-Konfigurationseinstellungen auf dem Hostportal überprüfen
5) das Senden von Fehlertraps vom Hostportal stoppen
6) Keep-Alive-Trap-Intervalle für alle Hosts konfigurieren und das Senden aller SNMP-Trap-Nachrichten von allen Hosts und RMX über die Assistant-Benutzeroberfläche stoppen
7) Keep-Alive-Traps auf dem Hostportal überprüfen
8) einen Test-Trap vom Hostportal senden
9) die Konfiguration von SNMPv3-Parametern, Keep-Alive-Traps und Trap-Filtern per Klick über die Benutzeroberfläche des Assistant/Manager auf allen Hosts speichern.
10) alle auf RMX ausgelösten Alarme per Klick über die Benutzeroberfläche des Assistant/Manager zurücksetzen.
11) die Host 4000 MIB über die Benutzeroberfläche des Assistant/Manager herunterladen
12) MIB2-Parameter für jeden Host über den Assistant konfigurieren
13) die SNMP-Einstellung auf jedem Host sichern/wiederherstellen
14) die Host 4000 MIB auf dem NMS verwenden, um die Bedeutung von Fehlermeldungen zu verstehen
15) die MIB-2 für die Hardwareüberwachung nutzen
16) die Hicom MIB (nicht HIM) verwenden, um eine Liste der Hosts/IP-Adressen im 4k-Bereich zu erstellen
17) die MIB2 verwenden, um Informationen zu Kontakt/Name/Standort vom Host abzurufen
18) OpenScape FM mit der 4k Host 4000 MIB und der neuen Hicom MIB verwenden

9.1.1 Hostportal – SNMP-Übersicht

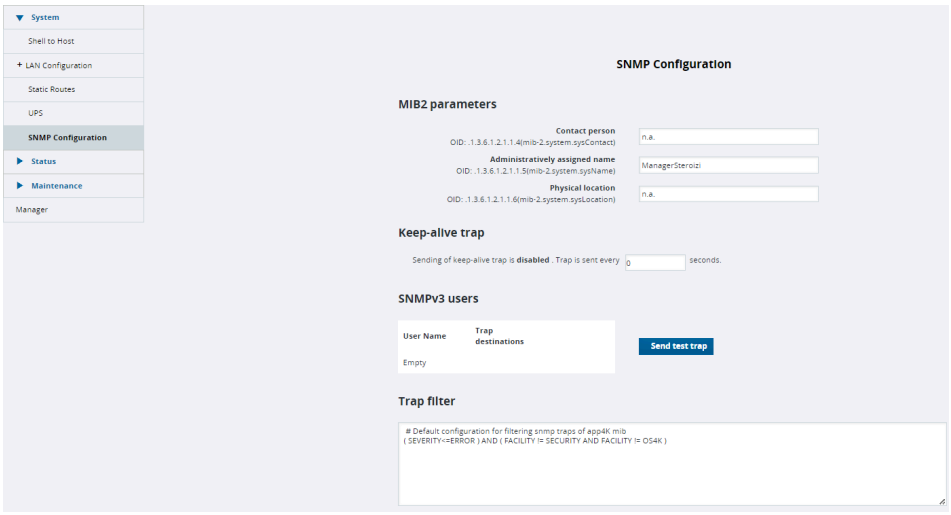


Abbildung 95: Hostportal – SNMP

9.1.1.1 SNMPv3-Benutzer

Die SNMPv3-Benutzer und ihre auf dem Host konfigurierten Trap-Ziele können in der SNMP-Konfigurationsansicht des Hostportals angezeigt werden. Diese Benutzer können auf die vom Host (hostMIB, MIB2,...) unterstützten MIBs zugreifen. Die Trap-Ziele sind IP-Adressen, an die die SNMP-Benachrichtigungen des Hosts gesendet werden.

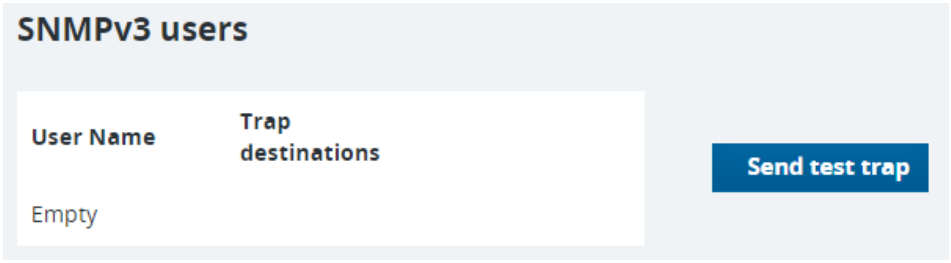


Abbildung 96: SNMP-Benutzer & Trap-Ziele – Beispiel

Die Konfiguration dieser Parameter (einschließlich der für die Autorisierung und Authentifizierung verwendeten Passwörter) erfolgt zentral über den Assistant. Derartige SNMPv3-Benutzer werden auf allen Hosts mit nur-Lesezugriff auf die MIB2 erstellt.

Die SNMP-Engine auf den Hosts ist so konfiguriert, dass SNMPv3-verschlüsselte, unbestätigte Traps gesendet werden. Die Engine-ID wird daher für den Empfang von Traps von 4k-Hosts nicht benötigt.

Per Klick auf die Schaltfläche "Test-Traps senden>können Sie einen Test-Trap an definierte Trap-Ziele senden. Test-Traps (.1.3.6.1.4.1.32804.1.9.1.10.13.0.1 - hostTestDebugEv) werden mit dem entsprechenden Benutzerschlüssel verschlüsselt und an alle definierten Trap-Ziele gesendet.

Sie können das Senden von SNMP-Traps vom Host oder zentral auf allen Hosts über die Benutzeroberfläche des Assistant aktivieren bzw. deaktivieren.

9.1.1.2 Trap-Filter

Sie können sich den von der SNMP-Engine auf dem Host verwendeten Filter anzeigen lassen und anschließend entscheiden, welche Ereignisse nicht als SNMP-Traps an vordefinierte Trap-Ziele gesendet werden sollten. Dieser Filter kann über die Benutzeroberfläche des Assistant festgelegt werden.

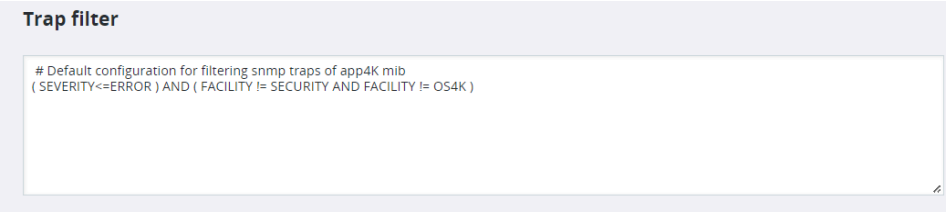


Abbildung 97: Trap-Filter – Beispiel

9.1.1.3 Keep-Alive-Trap

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

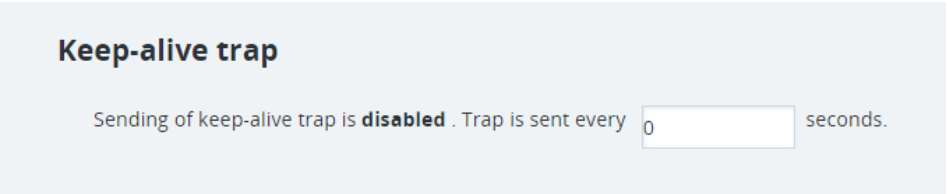


Abbildung 98: Keep-Alive-Trap-Filter – Beispiel

Standardmäßig sind die Keep-Alive-Traps deaktiviert (Feld leer oder 0). Die Zeitintervalle für das Senden von Keep-Alive-Traps können zentral über den Assistant so konfiguriert werden, dass Traps (.1.3.6.1.4.1.32804.1.9.1.10.13.0.2 - hostKeepAliveInfoEv) alle X Sekunden gesendet werden.

9.1.1.4 MIB2-Parameter

Jeder Host stellt über SNMP Informationen zum MIB-2-Modul bereit. Über die MIB2 kann der Benutzer drei Parameter aus dem Systemteil einrichten. Diese Parameter werden später von NMS verwendet, um die für den Dienst erforderlichen Systeminformationen zu ermitteln:

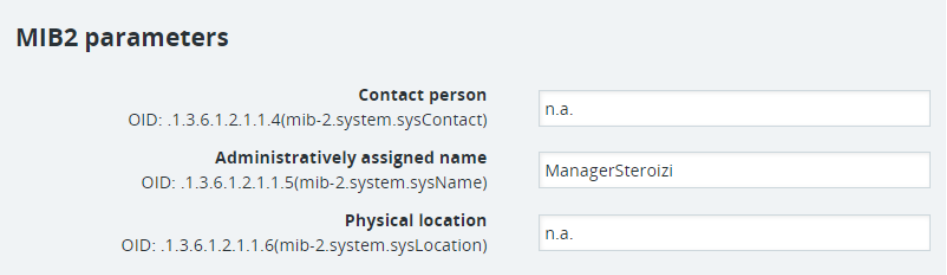


Abbildung 99: MIB2-Parameter– Beispiel

- sysContact
  - Textbezeichnung für diesen verwalteten Knoten sowie zusätzliche Angaben zur Kontaktperson.
- sysName
  - Ein vom Administrator zugewiesener Name für diesen verwalteten Knoten. Dies ist typischerweise der vollständig qualifizierte Domainname des Knotens.
- sysLocation
  - Der physische Standort dieses Knotens.

Diese MIB2-Parameter können nach der Installation des Knotens eingerichtet werden:

- Bei OpenScape 4000-Hostsystemen (Knoten A, Knoten B, Quorum-Knoten) können diese Parameter über die Systemverwaltung des Assistant eingerichtet werden.
- Bei SoftGate-basierten APs und SoftGate-basierten AP-E werden die sysLocation-Werte basierend auf den Angaben in der RMX-Datenbank (mittels AMO UCSU) automatisch verteilt.
- Bei IPDA-basierten AP-E-Systemen können diese Werte über die Assistant-Systemverwaltung auf AP-E eingerichtet werden.

Der MIB2 Standard lässt darüber hinaus eine Änderung dieser Werte über SNMP-Set-Anforderungen zu. Um eine stets konsistente Einrichtung der Parameter in der RMX, der Assistant-Datenbank und MIB2 zu gewährleisten, wird dieser Fall jedoch nicht unterstützt; ein Schreiben dieser Werte über SNMP ist nicht möglich.

Die Werte sysName und sysLocation sind Bestandteil jedes vom Hostsystem generierten SNMP-Traps.

MIB2 sysDescr

Der Wert sysDescr (Systembeschreibung) aus der MIB2 (OID .1.3.6.1.2.1.1.1) auf dem Host beinhaltet die genaue ID des Systems. Dieser Wert kann vom SNMP NMS verwendet werden, um Informationen zum Verwendungszweck des Hostsystems und seiner Hardwareplattform zu sammeln oder um das Hostsystem mit den Teilsystemen (Hosting-Software) in der Topologie-Ansicht (HPA500-Baugruppenerkennung) zu verknüpfen.

Dieser Wert kann mittels SNMP-Get-Anforderung vom Benutzer ausgelesen werden. Er ist Bestandteil jedes vom Hostsystem generierten SNMP-Traps.

Der sysDescr-Wert wird während der Installation automatisch konfiguriert und abhängig von der Konfiguration des Hosts, den Hosting-Applikationen und den SW-Update-Aktionen entsprechend angepasst.

Die Syntax der Hostbasissysteme (nodeA, nodeB, nodeQ) lautet wie folgt:

Hardware Type;Deployment Type;Business Name;Version
(Hardwaretyp;Bereitstellungstyp;Dienstname;Version)

(z. B.: VM; Simplex; OpenScape 4000; V7_R2.10.0)

Die Syntax der AP-basierten Hostsysteme lautet wie folgt:

Hardware Type;Deployment Type (LTU:ltu_number);Business Name;Version
(Hardwaretyp;Bereitstellungstyp (LTU:ltu_nummer);Dienstname;Version)

(z. B.: VM; Standalone-SoftGate (LTU:21); OpenScape 4000 SoftGate; V7_R2.10.0)

Werteliste:

- Hardware Type (Hardwaretyp) – Typ der Hardware, auf dem das System installiert ist. Mögliche Werte:
  - VM
  - OSA500i
  - OSA500a
  - DSCXL
  - ecoserver
  - Standard PC
- Deployment Type (Bereitstellungstyp)
  - Host NodeA (Host Knoten A)
  - Host NodeB (Host Knoten B)
  - Quorum Node (Quorum-Knoten)
  - Softgate
  - Survivable Softgate
  - AP Emergency (AP-Notfall)
- Business Name (Dienstname)
  - OpenScape4000
  - OpensScape4000 Softgate
  - .....
- Version – SWRM-Syntax-basierte Version des Hostsystems (Vmajor_minor.fixReleae.hotFixk, z. B. V7_R2.40.1)

Die möglichen Werte für sysDescr müssen im SNMP-Servicehandbuch dokumentiert werden.

9.1.2 SNMP-Benutzeroberfläche des Assistant

Mit dem Assistant-SNMP-Konfigurator können Sie:

- Host-SNMPv3-Parameter konfigurieren
- Trap-Filter erstellen und an alle Hosts verteilen
- Host-Keep-Alive-Traps auf allen Hosts aktivieren/deaktivieren
- MIB2-Parameter einrichten
- die Host-MIB-Datei herunterladen

9.1.2.1 Trap-Filter

Über die Benutzeroberfläche des SNMP-Konfigurators können Sie unter Trap-Filter -> Hostsystemereignisse den Trap-Filter für Hostsysteme definieren.

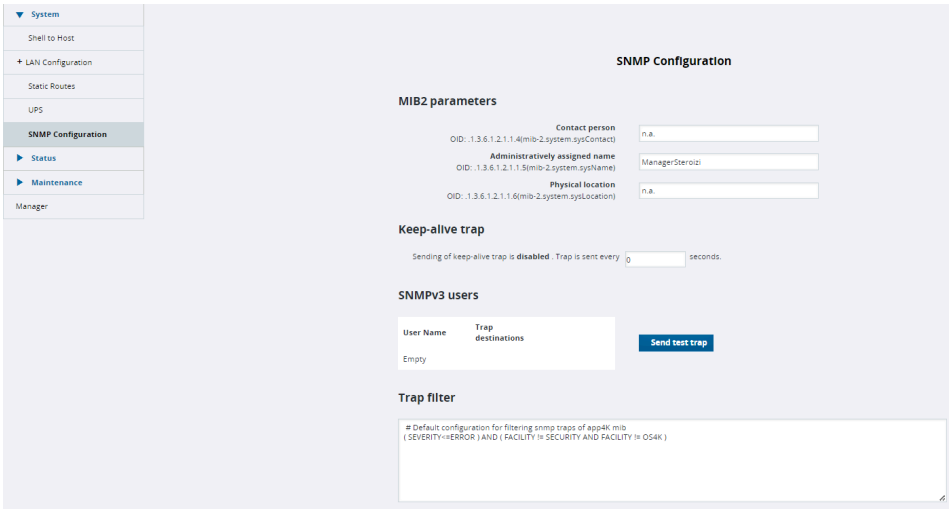


Abbildung 100: Hostsystemereignisse – Beispiel

Über die Trap-Filter-Benutzeroberfläche können Sie 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.

Anmerkung: 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.

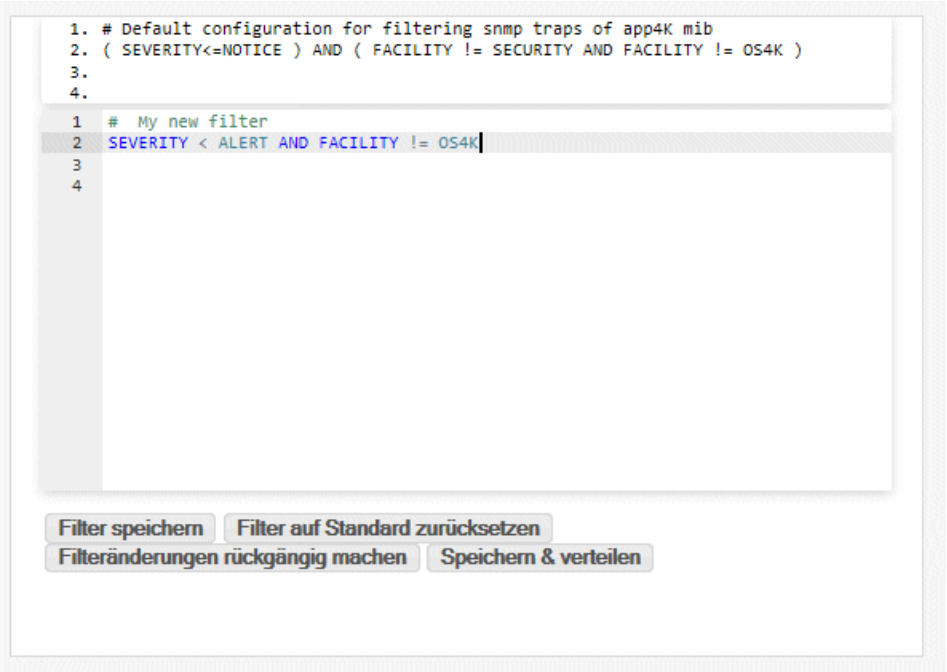


Abbildung 101: Hostsystemereignisse – Zuletzt gespeicherter Filter – Beispiel

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 OpenScape 4000-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 Hosts).

9.1.2.2 SNMP-Steuerungsparameter

Über die Benutzeroberfläche 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. Kontaktperson und Standort werden für die Einstellungen MIB2 sysLocation und sysContact verwendet.

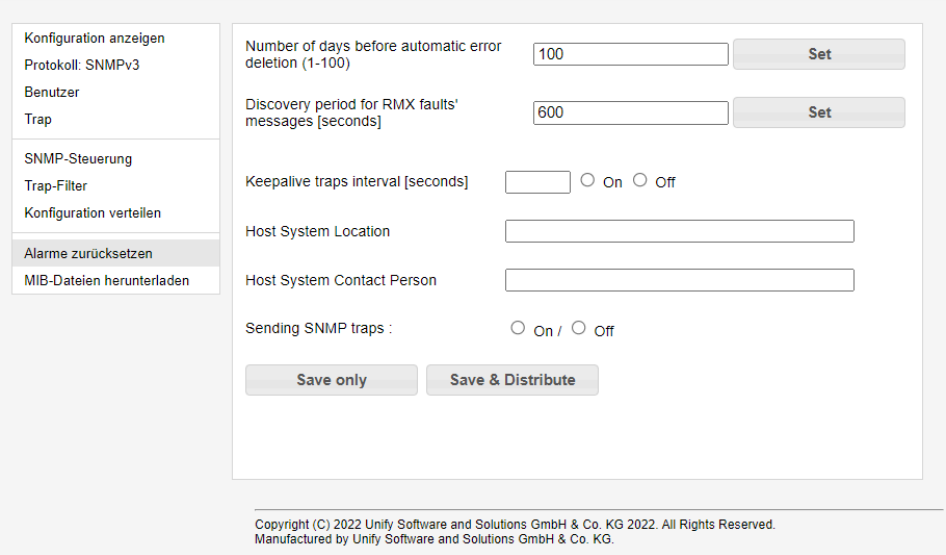


Abbildung 102: SNMP-Konfigurator – Beispiel für Speichern

- Sie können angeben, wie oft der Trap generiert werden soll.
- Über das Optionsfeld können Sie das Senden des SNMP-Traps vom Host deaktivieren.
- Sie können den physischen Speicherort des Hostsystems festlegen.
- Sie können eine Kontaktperson für das Hostsystem angeben.

Beschreibung der Aktionsschaltflächen:

- Nur speichern – Speichert Keep-Alive-Trap-Intervall, Standort, Kontaktperson und Sendeinformationen für Traps in der Assistant-Datenbank.
- Speichern & verteilen – Speichert Keep-Alive-Intervall, Standort, Kontaktperson und Sendeinformationen in der Assistant-Datenbank; die Seite "Konfiguration verteilen>wird geöffnet. Dort können Sie den Filter an alle Hosts im 4k-Bereich verteilen.

9.1.2.3 Verteilung an die Hosts

Über 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

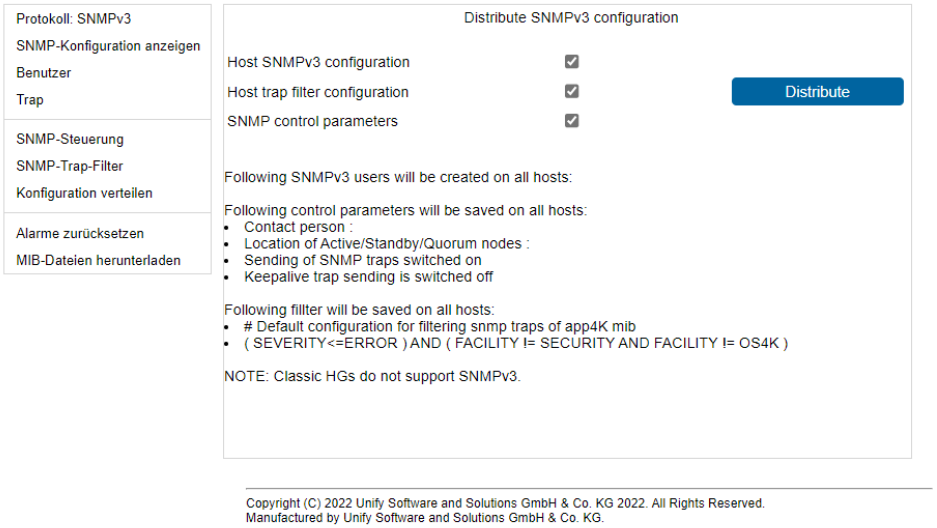


Abbildung 103: SNMP-Konfigurator – Beispiel für die Verteilung

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).

Anmerkung: Für die Verteilung an AP und APEs muss zwingend die NGS-IP-Adresse eingerichtet werden.

9.1.2.4 Alle auf dem RMX oder Assistant ausgelösten Alarme zurücksetzen

Über die Menüoption "Alarme zurücksetzen>links im SNMP-Konfigurator Sie alle auf dem RMX oder dem Assistant ausgelösten Alarme zurücksetzen (in den Status "Aus>setzen).

9.1.2.5 MIB-Datei herunterladen

Über die Option "MIB-Dateien herunterladen>links im SNMP-Konfigurator können Sie eine neue Host 4000 MIB-Datei gemeinsam mit allen von den Systemen im 4k-Bereich unterstützten MIB-Dateien herunterladen:

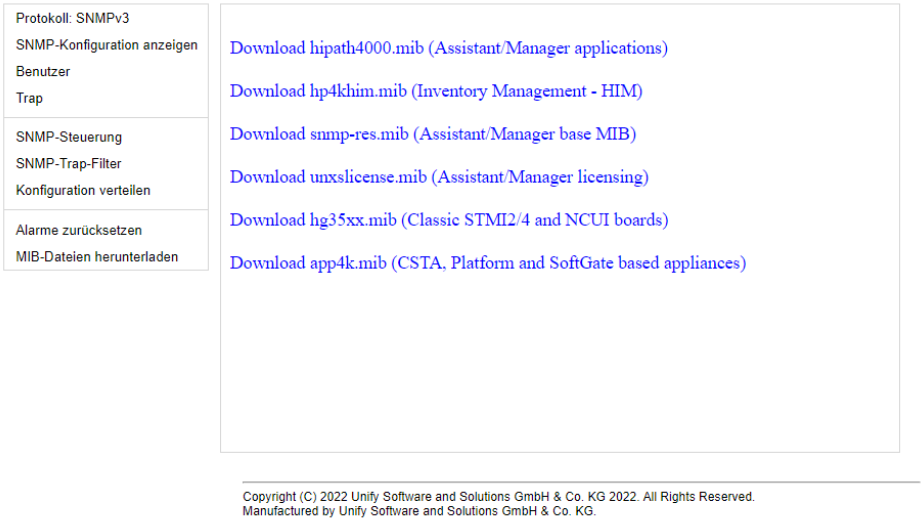


Abbildung 104: SNMP-Konfigurator – Download-Beispiel

9.1.3 Host 4000 MIB

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

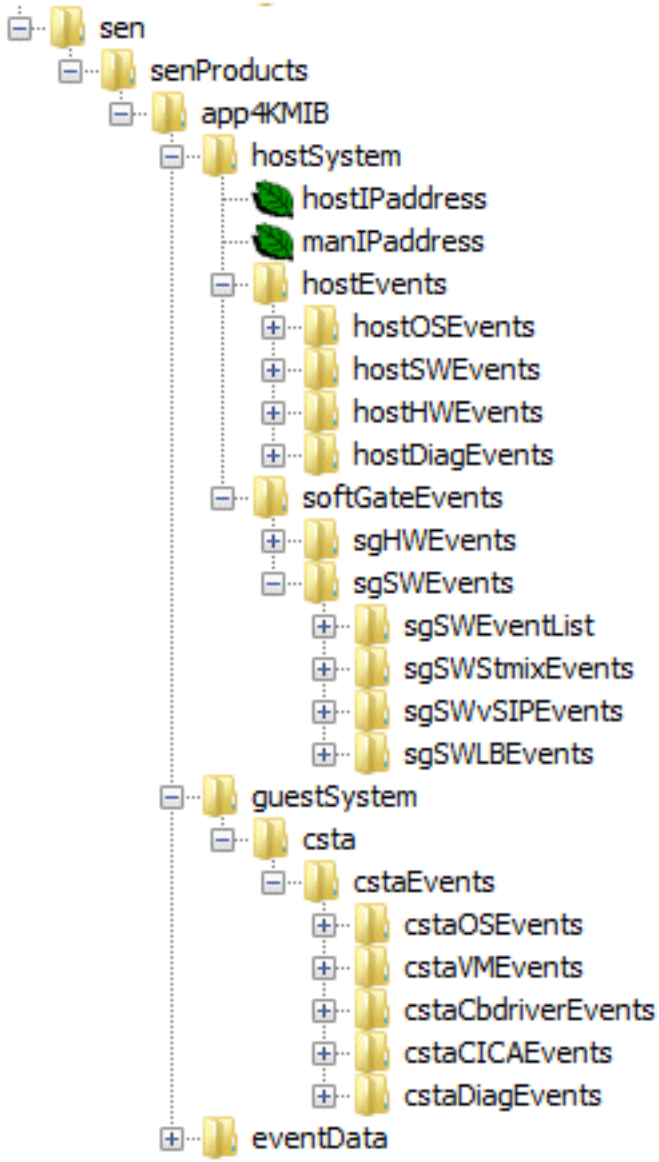


Abbildung 105: Host 4000 MIB-Struktur

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

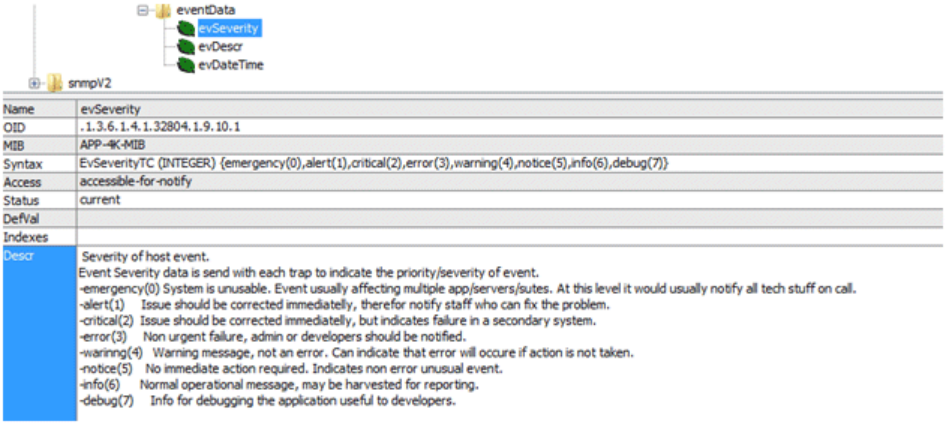
9.1.3.1 SeverityLevel (evSeverity)

Die Host 4000 MIB enthält die Severity-Informationen (Schweregrade) aus der syslog-ng (RFC 5424).

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

Abbildung 106: Host 4000 MIB-Struktur – Severity-Level (1)

Abbildung 107: Host 4000 MIB-Struktur – Severity-Level (2)



9.1.3.2 hostOSEvents

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

Abbildung 108: HostOSEvents – Protokolldatei

Die SNMP-Engine ist standardmäßig so eingestellt, dass vom Betriebssystem nur Trap-Meldungen mit Severity-Fehlern bis Schweregrad "emerg>gesendet werden. Meldungen, die eine niedrigere Priorität haben, werden nicht als SNMP-Traps gesendet.

hostOSEvents umfasst folgende Trap-Kategorien:

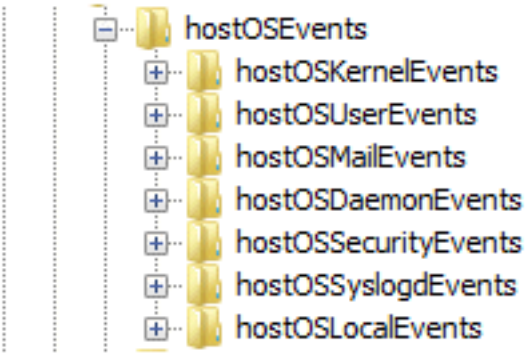


Abbildung 109: hostOSEvents – Kategorien

- hostOSKernelEvents – Kernel-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 - Von einem Administrator oder von Anwendungen des Host-Betriebssystems generierte Meldungen

9.1.3.3 hostSWEvents

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

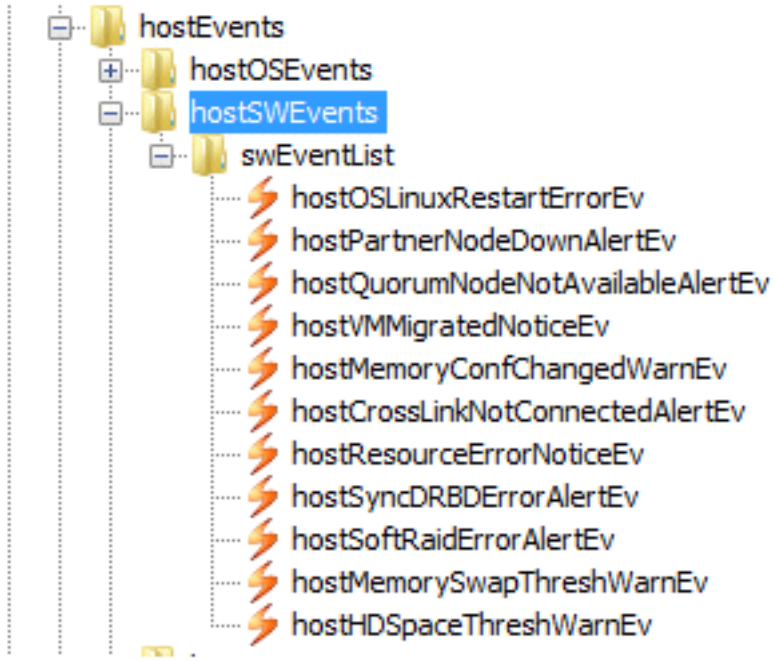


Abbildung 110: hostSWEvents

- 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

9.1.3.4 hostHWEvents

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

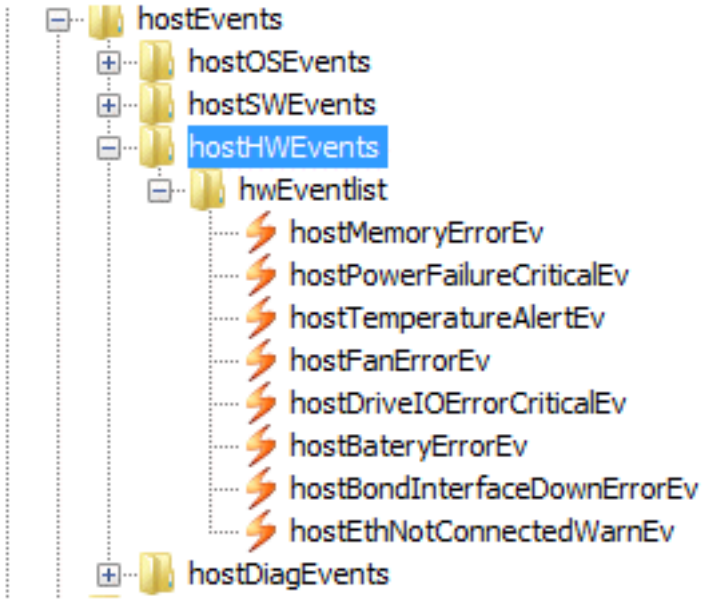


Abbildung 111: hostHWEvents

- 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

9.1.3.5 hostDiagEvents

Als Diagnostik-Traps verwendete SNMP-Traps. Dieser Teil enthält nur zwei Traps:

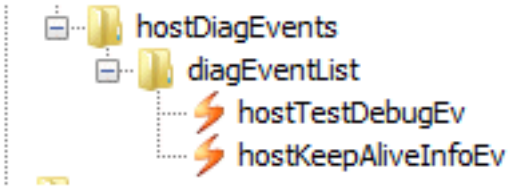


Abbildung 112: hostDiagEvents

- 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 die SNMP-Engine funktioniert, und Traps an vordefinierte Trap-Ziele sendet.

9.1.3.6 sgHWEvents

Hardware-basierte Ereignisse, die vom auf dem Host-Betriebssystem laufenden SoftGate-System generiert werden:

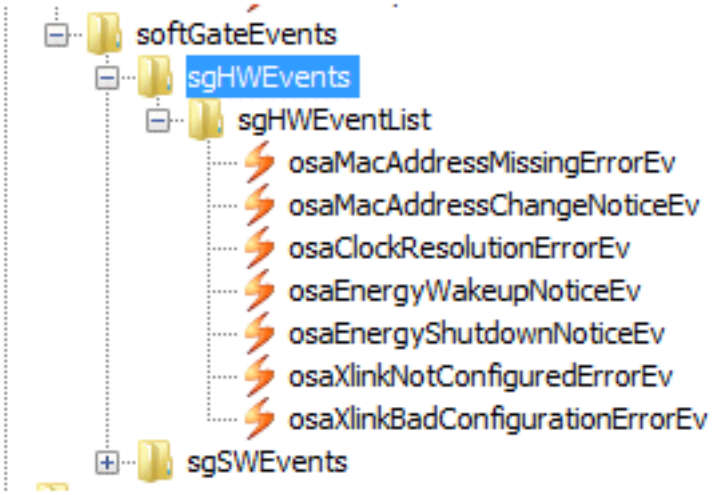


Abbildung 113: sgHWEvents

- 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

9.1.3.7 sgSWEvents

Software-basierte Ereignisse, die vom auf dem Host laufenden SoftGate-System generiert werden. Diese sind in vier Kategorien unterteilt:

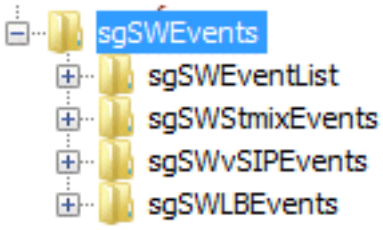


Abbildung 114: sgSWEvents

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

sgSWLBEvents

OpenSIPS-Load-Balancer-Ereignisse:

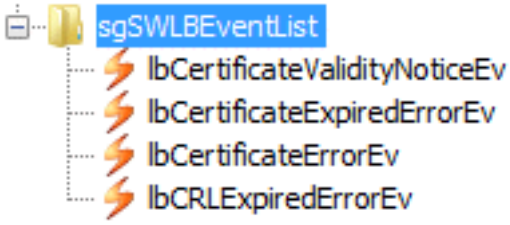


Abbildung 115: sgSWLBEvents

- 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

sgSWvSIPEvents

vHG3500 (SIP)-Ereignisse:

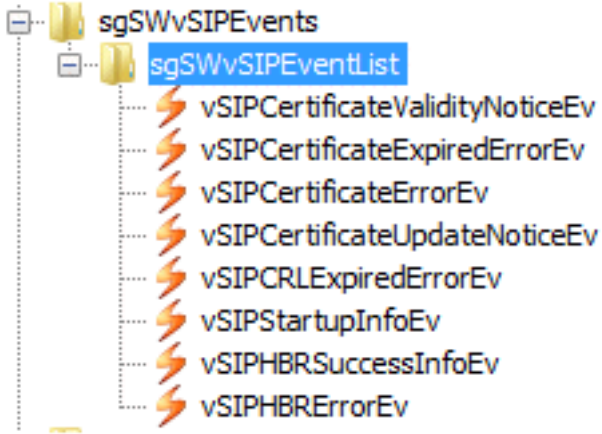


Abbildung 116: sgSWvSIPEvents

- 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.

sgSWStmixEvents

STMIX-Ereignisse:

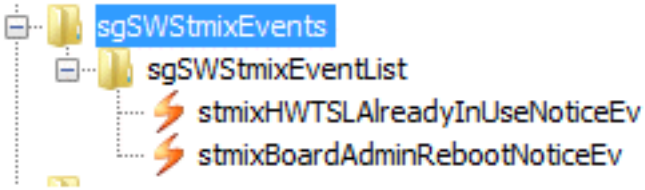


Abbildung 117: sgSWStmixEvents

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

sgSWEventList

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

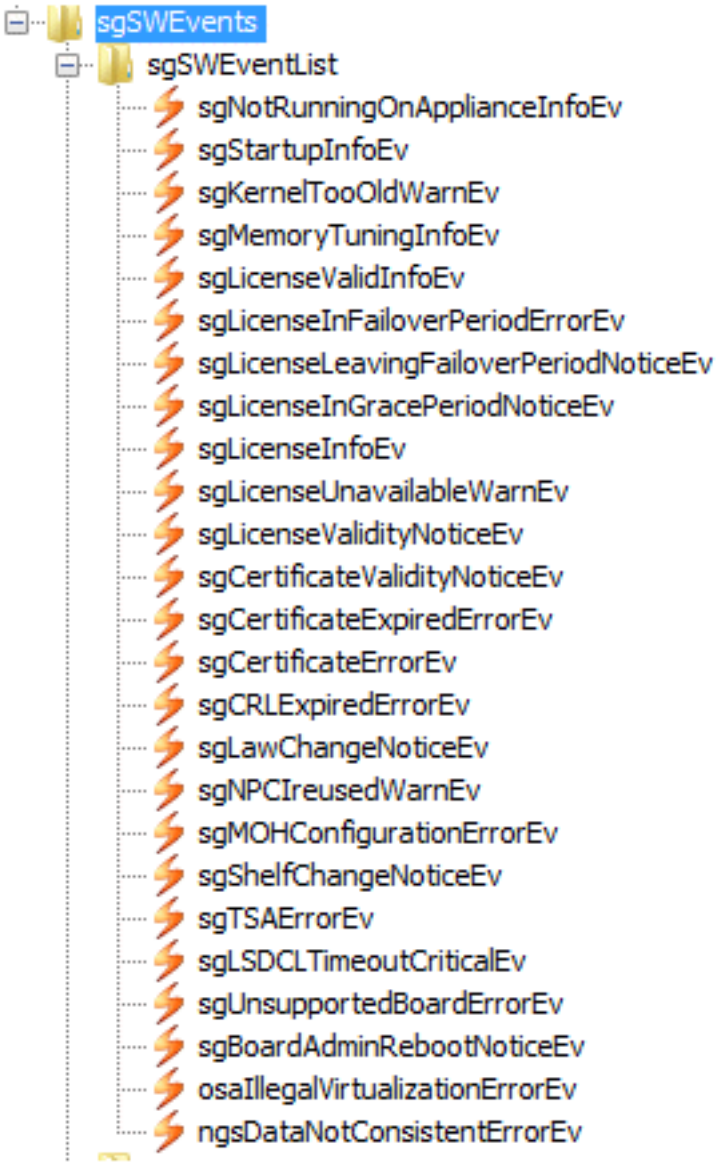


Abbildung 118: sgSWEventList

- sgNotRunningOnApplianceInfoEv – SoftGate läuft nicht auf einer Appliance
- sgStartupInfoEv – Informationen über die Plattform, die beim Hochfahren angezeigt werden. SG auf VM, UNKNOWNVM, OSA500A, OSA500I, 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.

9.1.3.8 cstaEvents

Die auf dem aktiven Knoten von OpenScape 4000 laufende CSTA wurde in V7R2 ebenfalls erweitert und kann nun SNMPv3-Traps von ihrem Betriebssystem und ihren CSTA-Prozessen senden.

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 Trap-Variablenbindung; diese wird verwendet, um die Ursache des Fehlers zu ermitteln. Am Trap-Namen ist nur der Schweregrad (d. h. die Priorität) des Traps und die Facility (d. h. das OS-Subsytem, das den Trap generiert hat) erkennbar.

Die SNMP-Engine ist standardmäßig so eingestellt, dass vom Betriebssystem nur Trap-Meldungen mit Schweregraden bis "emerg>gesendet werden. Meldungen mit niedrigerer Priorität werden nicht als SNMP-Traps gesendet.

cstaOSEvents umfasst folgende Trap-Kategorien:

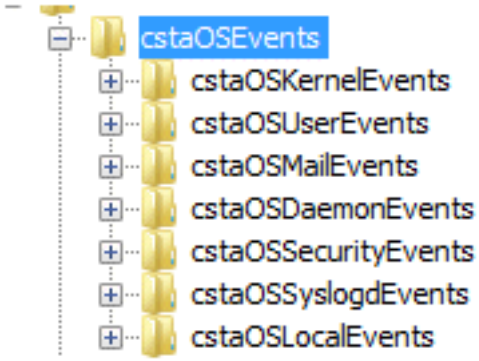


Abbildung 119: cstaOSEvents

- 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

cstaVMEvents

Ereignisse im Zusammenhang mit der Überwachung und Prozessen der virtuellen Maschine von CSTA:

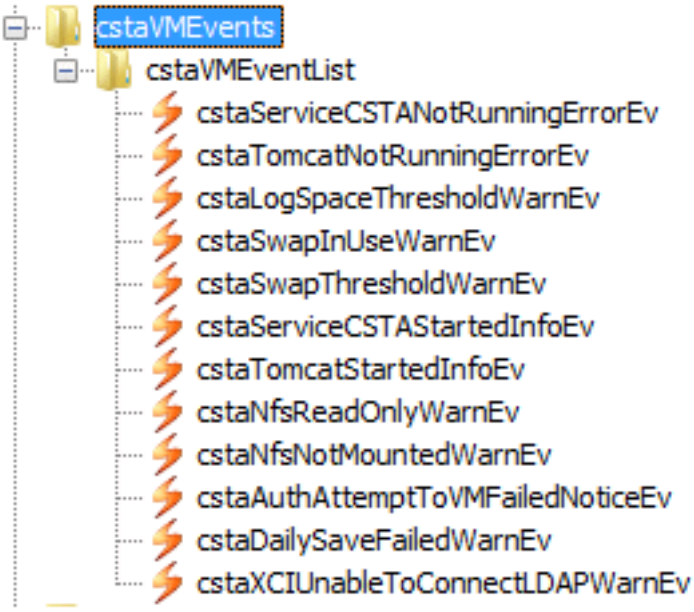


Abbildung 120: cstaVMEvents

- 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

cstaCdbDriverEvents

Zur cbdriver-Software von CSTA gehörige Ereignisse:

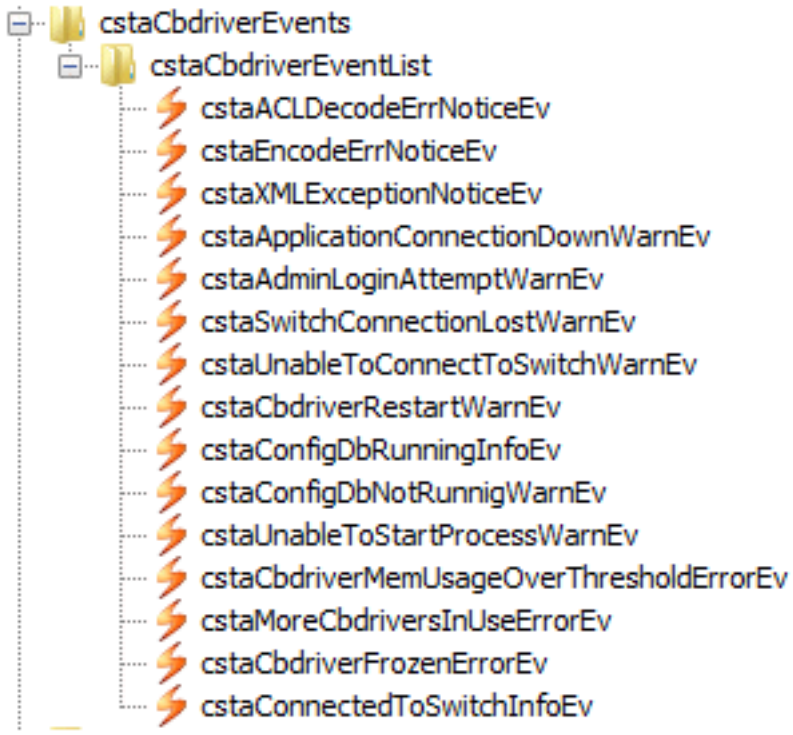


Abbildung 121: cstaCdbDriverEvents

- 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.

cstaCICAEvents

CICA-Ereignisse:

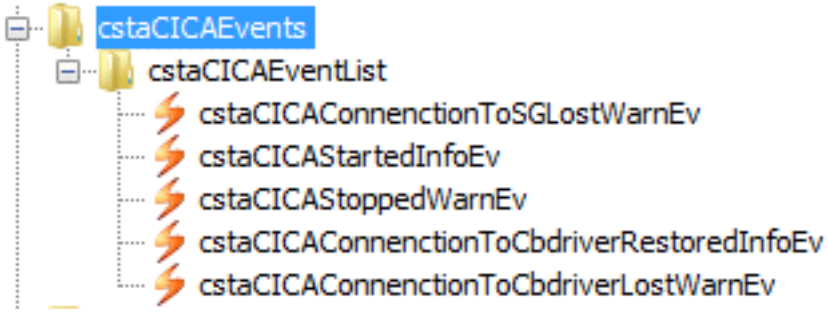


Abbildung 122: cstaCICAEvents

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

cstaDiagEvents

Ereignisse, die für CSTA-Diagnosezwecke verwendet werden:

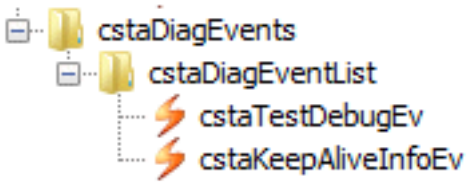


Abbildung 123: cstaDiagEvents

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

9.1.4 Überwachung mittels SNMP-Get-Anforderungen

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.

9.1.4.1 UCD-SNMP-MIB

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

Überwachung der Prozessorauslastung

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

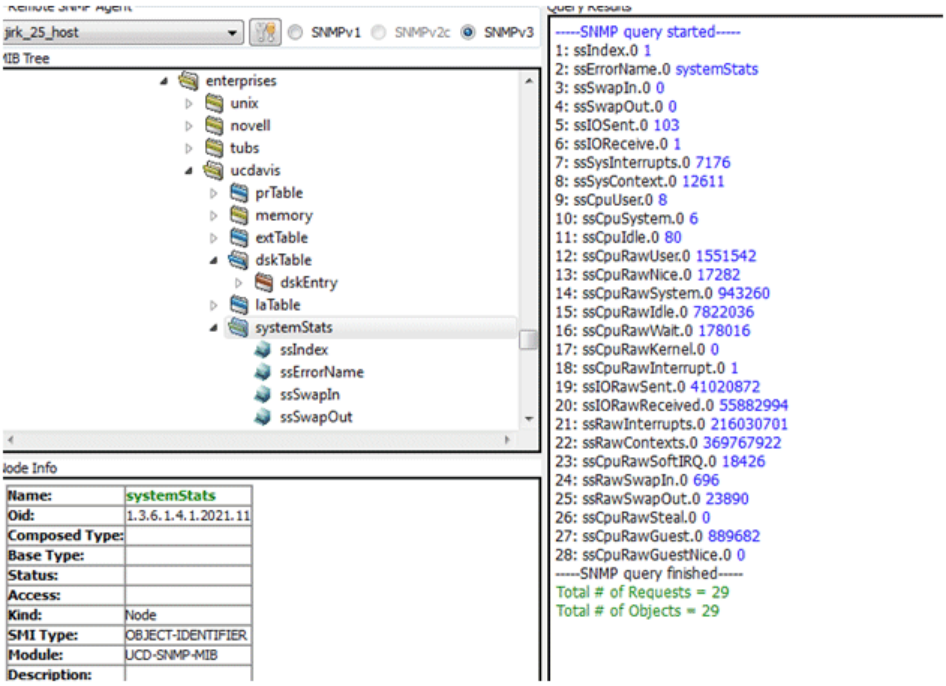


Abbildung 124: systemStats-OID

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.

Überwachung der Speicherauslastung

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

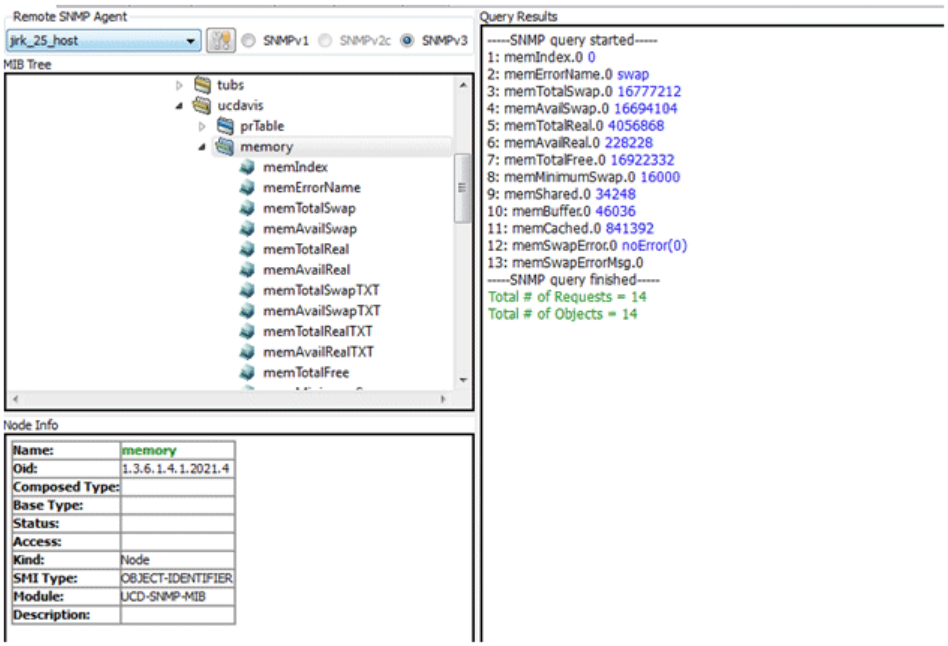


Abbildung 125: Memory Stats

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)	

Abbildung 126: Durchschnittliche Auslastung

9.1.4.2 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

Allgemeine Systeminformationen (hrSystem)

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

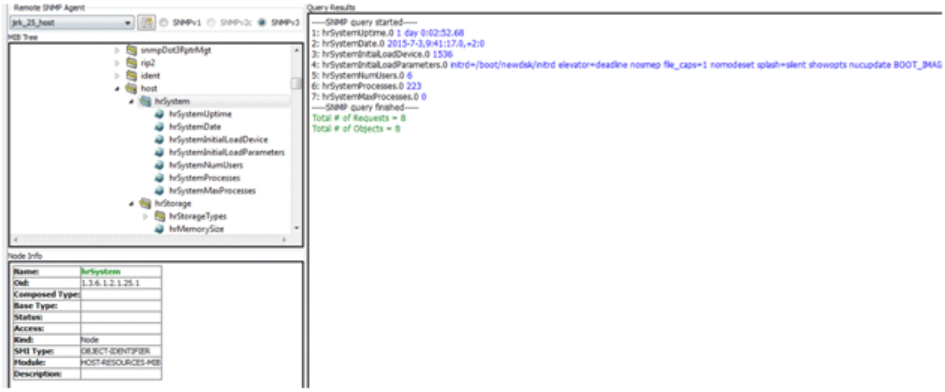


Abbildung 127: hrSystem

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:

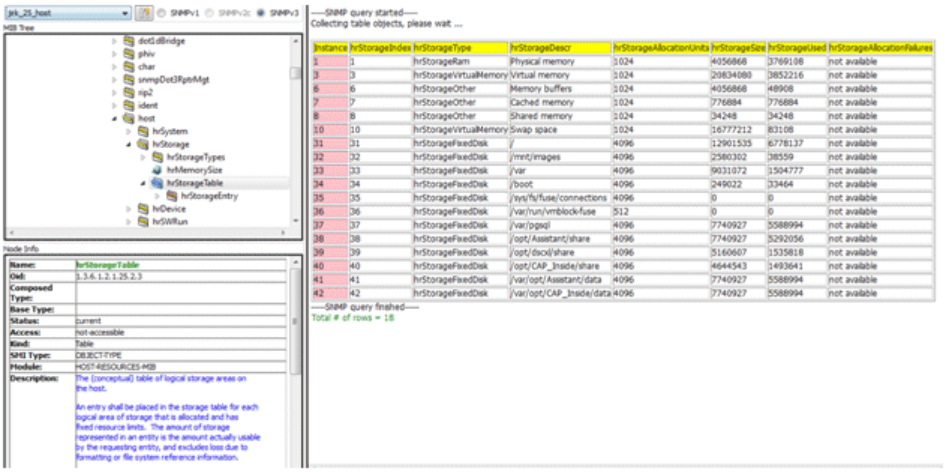


Abbildung 128: hrStorage

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:

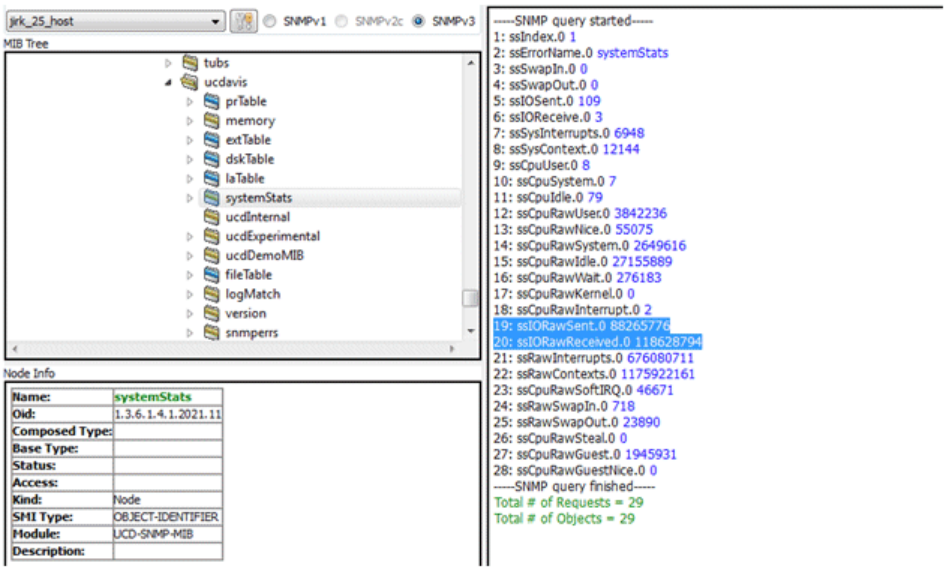


Abbildung 129: systemStats (ssIORawSent.0 und ssIORawRecieved.0)

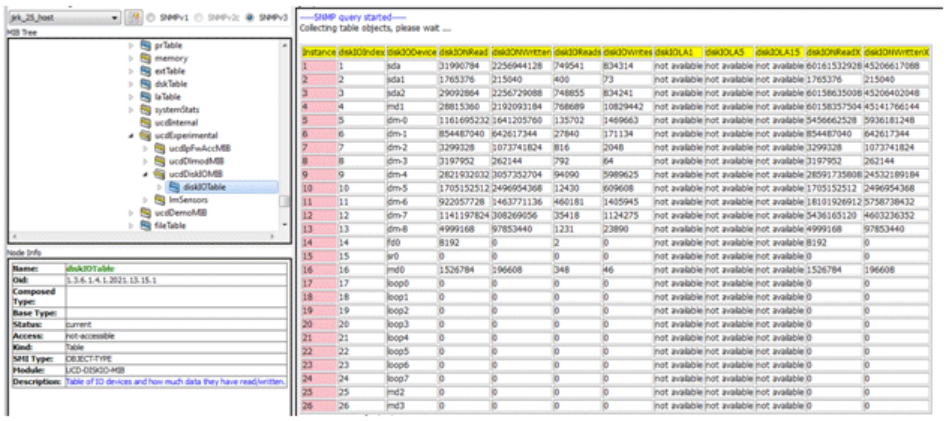


Abbildung 130: diskIOTable

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:

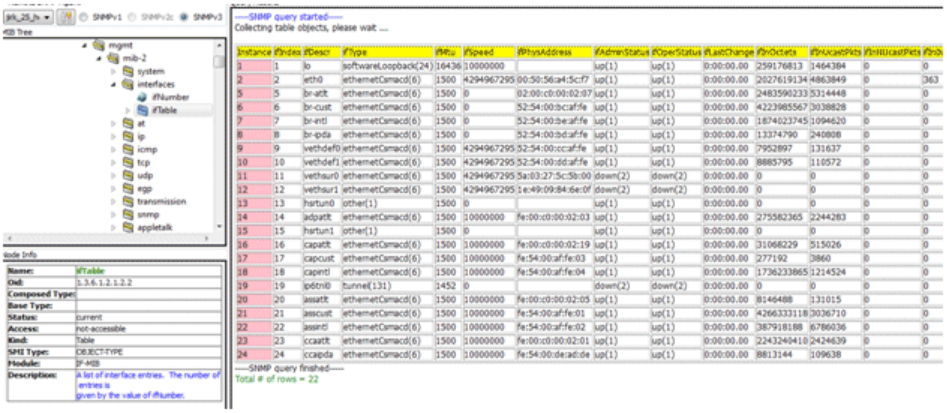


Abbildung 131: ifTable

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.

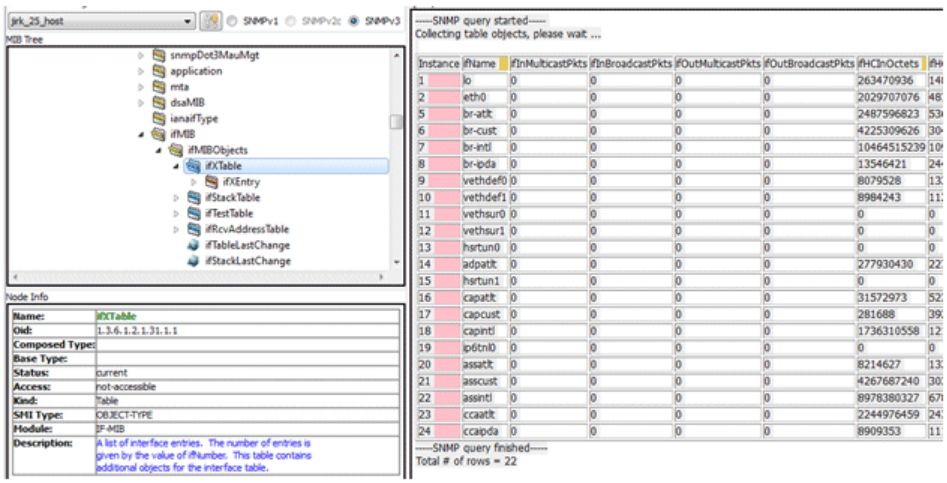


Abbildung 132: ifXTable

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

Instance	ifName	ifInMulticastPkts	ifInBroadcastPkts	ifOutMulticastPkts	ifOutBroadcastPkts	ifHCInOctets	ifHCInUcastPkts	ifHCInMulticastPkts	ifHCInBroadcastPkts	ifHCOutOctets	ifHCOutUcastPkts	ifHCOutMulticastPkts	ifHCOutBroadcastPkts	ifLinkUpDownTrapEnable	ifHighSpeed	ifPromiscuousMode	ifConnectorPresent	ifAlias	ifCounterDiscontinuityTime
1	lo	0	0	0	0	263470936	1486501	0	0	263470936	1486501	0	0	not availabl	10	false(2)	not availabl		00:00:0
2	eth0	0	0	0	0	2029707076	4876289	0	0	14756027201	6036477	0	0	not availabl	10000	false(2)	true(1)		00:00:0
5	br-alt	0	0	0	0	2487596823	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	73729058	595233	0	0	not availabl	0	true(1)	true(1)		00:00:0
7	br-intl	0	0	0	0	10464515239	1038169	0	0	16785410356	1054237	0	0	not availabl	0	true(1)	true(1)		00:00:0
8	br-ipda	0	0	0	0	13546421	244522	0	0	61038	711	0	0	not availabl	0	true(1)	true(1)		00:00:0
9	vethdef0	0	0	0	0	8079528	133738	0	0	8364243	112207	0	0	not availabl	10000	false(2)	true(1)		00:00:0
10	vethdef1	0	0	0	0	8364243	112207	0	0	8079528	133738	0	0	not availabl	10000	false(2)	true(1)		00:00:0
11	vethsur0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	10000	false(2)	true(1)		00:00:0
12	vethsur1	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	10000	false(2)	true(1)		00:00:0
13	hsrun0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00:0
14	adpalt	0	0	0	0	277930430	2270531	0	0	2286007836	3116796	0	0	not availabl	10	false(2)	true(1)		00:00:0
15	hsrun1	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00:0
16	capalt	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	3324	0	0	4267770636	3041044	0	0	not availabl	10	false(2)	true(1)		00:00:0
18	capintl	0	0	0	0	1736310558	1215111	0	0	8397023682	6866207	0	0	not availabl	10	false(2)	true(1)		00:00:0
19	ip6tnl0	0	0	0	0	0	0	0	0	0	0	0	0	not availabl	0	false(2)	true(1)		00:00:0
20	assalt	0	0	0	0	8214627	132266	0	0	14225988	139395	0	0	not availabl	10	false(2)	true(1)		00:00:0
21	asscust	0	0	0	0	4267687240	3039693	0	0	73812136	537120	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	coalt	0	0	0	0	2244976459	2437916	0	0	245225220	1839255	0	0	not availabl	10	false(2)	true(1)		00:00:0
24	coaipda	0	0	0	0	8909353	111240	0	0	7437320	126824	0	0	not availabl	10	false(2)	true(1)		00:00:0

Abbildung 133: 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.

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:

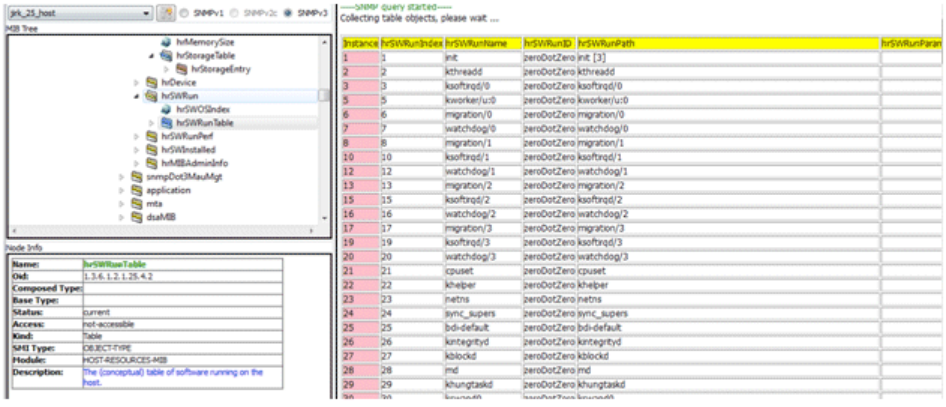


Abbildung 134: hrSWRun

Leistung der installierten Software

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

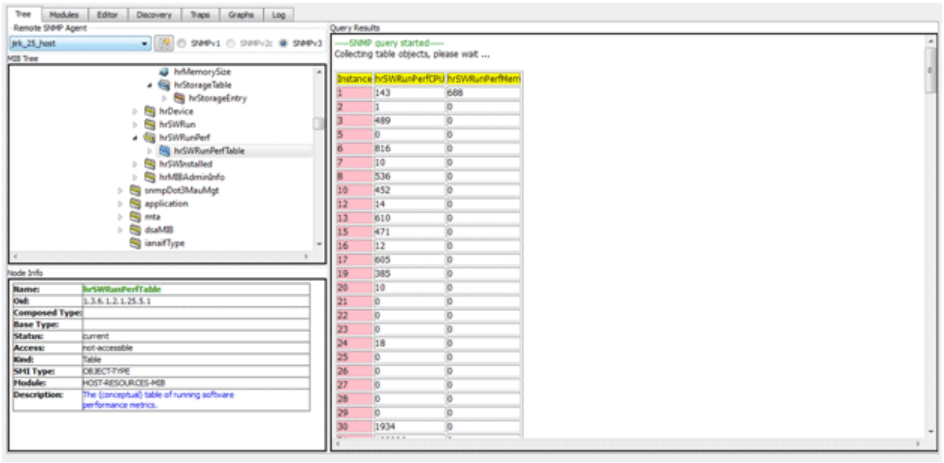


Abbildung 135: hrSWRunPerf

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:

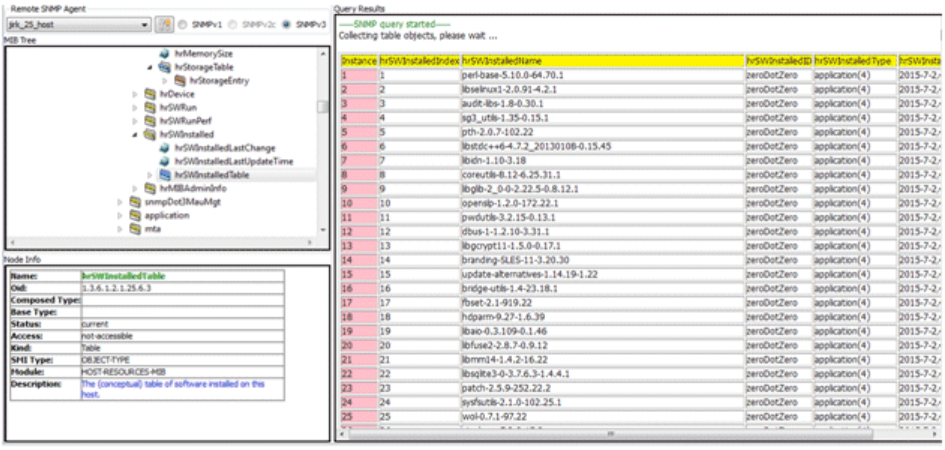


Abbildung 136: hrSWInstalled

9.1.5 Backup & Restore

Die SNMP-Einstellung ist Teil des Recovery-ISO-Image.

Im Assistant ist die SNMP-Einstellung Teil des CDB-Backups.

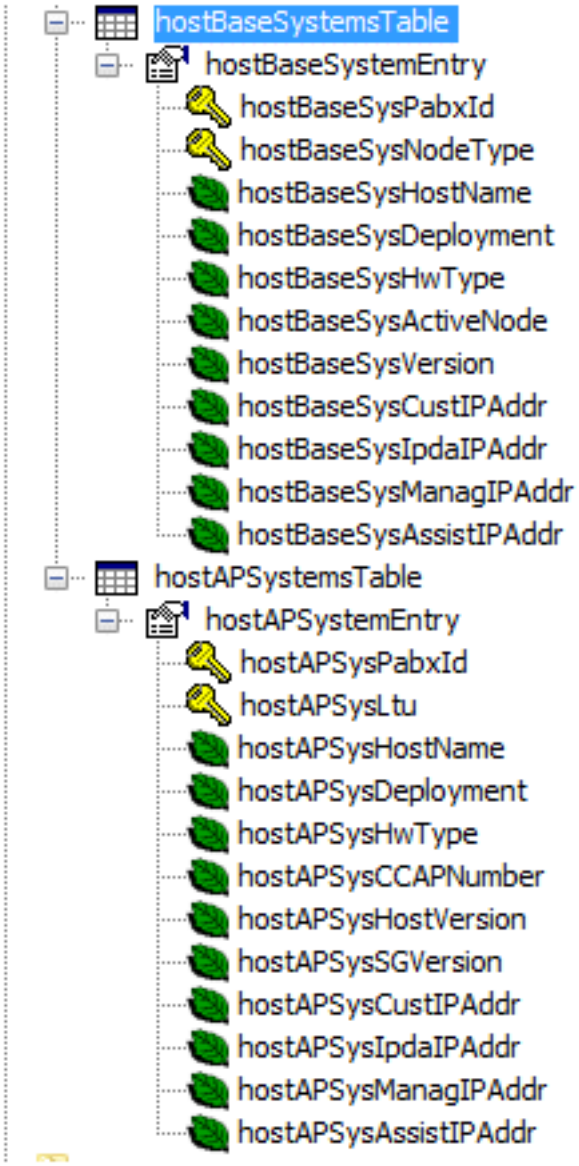
Während eines Assistant-Wiederherstellungsprozesses werden die Daten nicht an die verbundenen Hosts verteilt. Ggf. müssen Sie dies manuell tun, nachdem der Wiederherstellungsvorgang abgeschlossen ist.

9.1.6 hicomMIB-Erweiterungen

Die hicomMIB wurde um zwei Tabellen erweitert, die während der Erkennung des Systems (Discovery) 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

Abbildung 137: hostBaseSystemsTable/hostAPSystemsTable



9.1.6.1 hostBaseSystemsTable

Die Tabelle mit den Hostsystemen 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.

9.1.6.2 hostAPSystemsTable

Die Tabelle mit den Software-basierten APs 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.

9.1.7 OpenScapeFM-Erweiterungen

OpenScape Fault Management V8 wurde um eine bessere Beschreibung der vom Host generierten (in der host4000 mib definierten) SNMP-Trap-Nachrichten erweitert.

Die Änderungen in der hicomMIB werden zusammen mit den sysDescr-Werten aus MIB2 von der OpenScape Fault Management Autodiscovery-Funktion verwendet; durch Weitergabe der IP-Adresse des Assistant an das OpenScape Fault Management können nun alle verbundenen Knoten erkannt werden.

Fault Management ist nun in der Lage, alle Knoten in der IP-Ansicht und im 4000-Plugin anzuzeigen, wo die APs und ihre Hosts miteinander verknüpft sind.

Darüber hinaus kann OpenScape FM durch den vom MIB2-Agenten bereitgestellten sysDesc-Wert auf jedem Host den für die Nutzung der HPA500-Baugruppenerkennungsfunktion erforderlichen Hardwaretyp des AP erkennen.

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. Wenn die IP-Knoten in der OpenScape Fault Management-Datenbank nicht vorhanden sind (z. B. wenn sie wegen eines fehlenden IP-Netzwerks nicht automatisch erstellt werden konnten), wird der Alarm dem IP-Knoten des Assistant zugeordnet. Für diesen Zweck wird die in der Trap-Variablenbindung hinterlegte IP-Adresse des Assistant verwendet.

Wenn weder der Assistant noch der IP-Knoten des Hostsystems in OpenScape Fault Management vorhanden ist, wird der Alarm ohne Zuordnung zu irgendwelchen Objekten angezeigt.

9.1.7.1 OS4K

Die IP-Adressen der zu einer 4k gehörigen Hosts werden abgefragt und die IP-Knoten werden für alle Hostsysteme erstellt (nur möglich, wenn das IP-Netzwerk bereits vorhanden ist oder die Netzwerkmaske über SNMP bestimmt werden kann). Die 4k wird in der OSFM-Topologie als Container-Objekt angezeigt. Dieses Container-Objekt enthält das 4k (Assistant)-Objekt (das bereits in der aktuellen OSFM-Version vorhanden ist) sowie alle zugehörigen IP-Knoten der Hostsysteme.

Abbildung 138: Anzeige einer OS4k – Alte Version

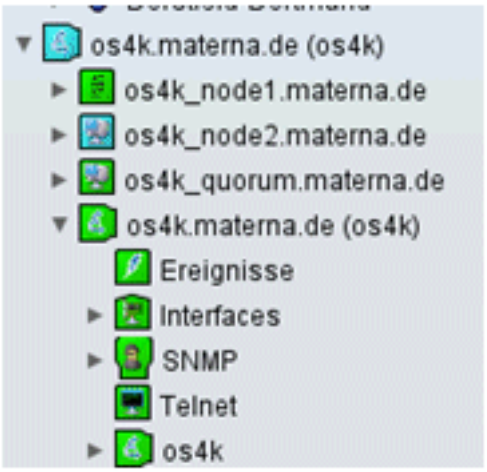


Abbildung 139: Anzeige einer OS4k einschließlich der Hostsysteme – Neue Version

Die OS4k (os4k.materna.de) befindet sich in einem Container-Objekt mit demselben Namen; dieses enthält darüber hinaus die IP-Knoten, die die Hostsysteme repräsentieren (node1, node2, quorum).

Für das OS4k-Objekt gibt es nun das neue Menüelement "Host-Systeme", das den Inhalt der Hostsystemtabelle in Textlistenform anzeigt.

9.1.7.2 AP/APE

Die IP-Adressen der AP/APEs werden abgefragt und für jede Adresse wird ein IP-Knoten erstellt (nur möglich, wenn das IP-Netzwerk bereits vorhanden ist oder die Netzwerkmaske über SNMP bestimmt werden kann). Die AP/APE-Objekte werden unter den zugehörigen IP-Knoten aufgeführt.

Abbildung 140: Darstellung einer AP – Alte Version

Abbildung 141: Darstellung einer AP (zusammen mit dem IP-Knoten) – Neue Version

9.1.7.3 Auswertung von sysDescription

Die SNMP-Variable "sysDescription>(MIB2) der Hostsysteme enthält eine Zeichenfolge, die den Hardwaretyp des Hostsystems beschreibt. Diese Zeichenfolge wird an die Symbolbezeichnung in OpenScape Fault Management angefügt.

9.2 HPA500-Baugruppenerkennung

Mit diesem Leistungsmerkmal können Sie den Hardwaretyp eines Access Points über SNMP erkennen. Sie können hierzu die hicomMIB (mittels SNMP-Get-Anforderung an den Assistant) oder die von den einzelnen Hosts unterstützte MIB2 (mittels SNMP-Get-Anforderung an das AP-Hostsystem) verwenden

9.2.1 hicomMIB

Vorhandene Version (in V7R1):

Wenn ein hicomErrorTrap mit Fehlermeldung zu einem bestimmten Fehler auf einer AP generiert wird, enthält er Informationen zur ID der Lage (PEN).

Wenn ein generierter Alarm durch ein AP-Problem hervorgerufen wurde, enthält der Trap die LTU-Nummern der betroffenen APs.

Fault Management ist so in der Lage, die betroffene AP zu identifizieren.

Neu in V7R2:

Dieses Leistungsmerkmal ermöglicht Fault Management die Erkennung des AP-Hardwaretyps. Fault Management ruft diese Informationen von dem Hardware-Agent ab, der auf dem Assistant/Manager ausgeführt wird. Die Informationen werden vom Hardware-Agent während der Hardware-Erkennung (Discovery) gesammelt.

Die IP-Adressen des Hostsystems für den Frame werden ebenfalls erkannt.

Die Frametabelle wurde um "realHardwareType>und drei Frame-IP-Adressen (ipAddrIPDA, custIpAddr, managIPAddr) erweitert. Die neuen Werte werden an das Ende der Tabelle/OIDs angehängt.

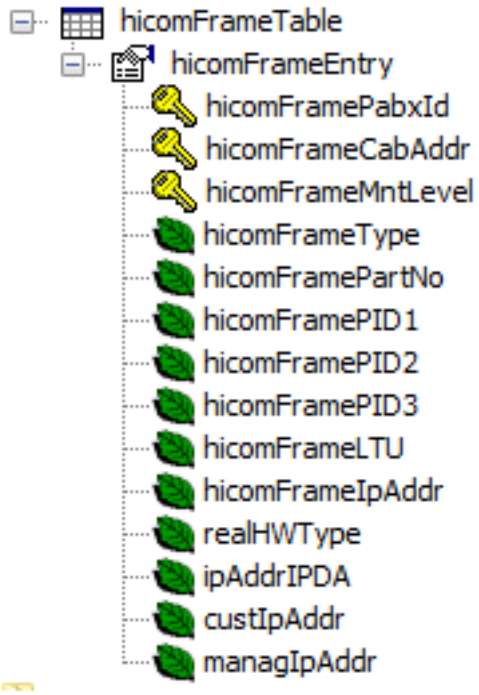


Abbildung 142: hicomFrameTable

- ipAddrIPDA – Die von der IPDA-Schnittstelle verwendete IP-Adresse des AP-Hostsystems.
- custIPAddr – Die IP-Adresse des Standalone-SG-Portals (optionaler Konfigurationsparameter).
- managIPAddr – Die Management-IP-Adresse des über AMO STMIB konfigurierten SG plus SG-WBM für die zu verwendende LAN-Schnittstelle (optionaler Konfigurationsparameter).

9.2.2 MIB2

Das NMS, dem keine Informationen zur Verwendung der hicomMIB und ihrer Discovery-Prozesse vorliegen, kann die erforderlichen HW-Informationen über den sysDescr-Wert des auf den einzelnen Hosts laufenden mib2agent ermitteln.

9.2.3 OpenScape Fault Management – Erweiterung

OpenScape Fault Management zeigt den "realHardwareType" eines Frames (Rahmens) als Bezeichnungserweiterung des zugehörigen IP-Knotens des Frames an. Zusätzlich wird für jede IP-Adresse des Frames ein IP-Knoten erstellt (nur möglich, wenn das IP-Netzwerk bereits vorhanden ist oder die Netzwerkmaske über SNMP bestimmt werden kann). Das Frame-Objekt wird mit dem zugehörigen IP-Knoten-Objekt verknüpft (d. h. das Frame-Objekt wird unterhalb des IP-Knoten-Objekts angeordnet).

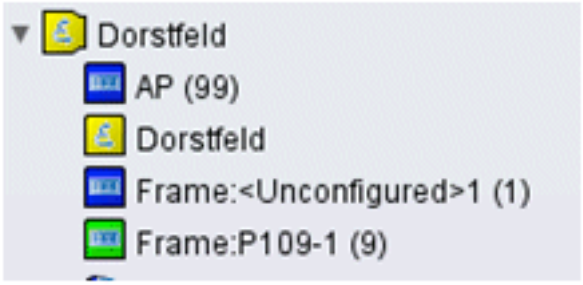


Abbildung 143: Darstellung von Frames in OSFM – Alte Version

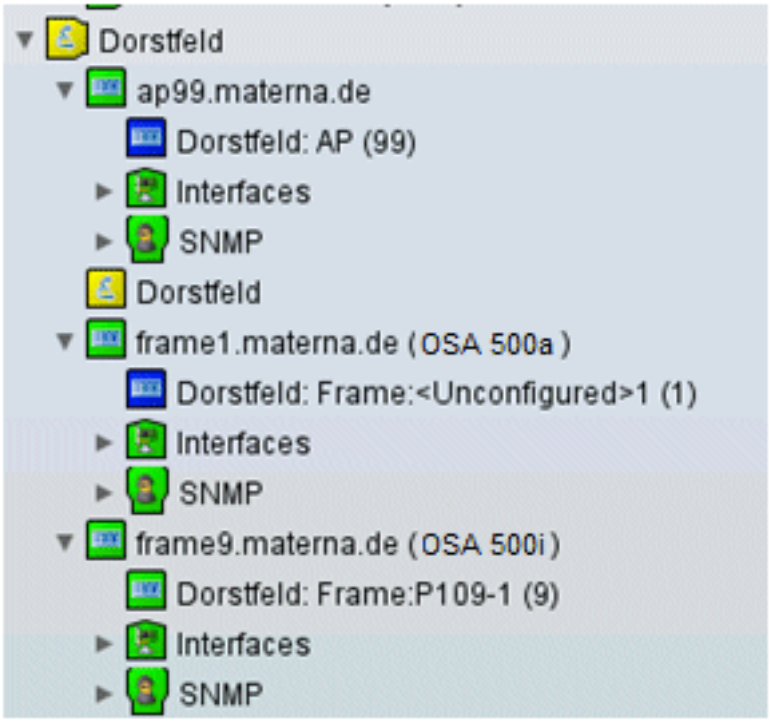


Abbildung 144: Darstellung von Frames in OSFM (Frame-Objekt verknüpft mit IP-Knoten) – Neue Version

9.3 Zentrale SNMP-Konfiguration

Mit diesem Leistungsmerkmal können Sie:

- die SNMPv3-Konfiguration (einschließlich Filter und Keep-Alive-Einstellungen) über den Assistant zu speichern und an alle Hosts auf allen Rechnern im OpenScape 4000-Bereich verteilen (IPDA-basierte AP-Es sind dadurch nicht abgedeckt; der Assistant muss auf einem IPDA-basierten AP-E verwendet werden, um SNMP auf dem Host zu konfigurieren).
- die SNMPv3-Konfiguration (einschließlich Filter und Keep-Alive-Einstellungen) über den Manager zu speichern und an alle Hosts auf allen Rechnern im OpenScape 4000-Bereich verteilen (IPDA-basierte AP-Es sind dadurch abgedeckt; der Assistant muss auf einem IPDA-basierten AP-E verwendet werden, um SNMP auf dem Host zu konfigurieren).
- Alarme auf allen/ausgewählten Systemen zurücksetzen (einschließlich Assistant/Manager-Alarme der Alarmgruppe 7)

- Über das Gateway-Dashboard des Assistant können Sie die SNMPv1-Konfigurationsparameter in der IP-Gateway-Liste anzeigen und speichern.
- Über das Gateway-Dashboard des Assistant können Sie die QDC (Quality of Service Data Collection)-Einstellungen in der IP-Gateway-Liste ändern.

9.3.1 SNMPv3-Konfiguration auf dem Assistant

9.3.1.1 SNMPv3-Benutzer für die Hosts definieren

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.

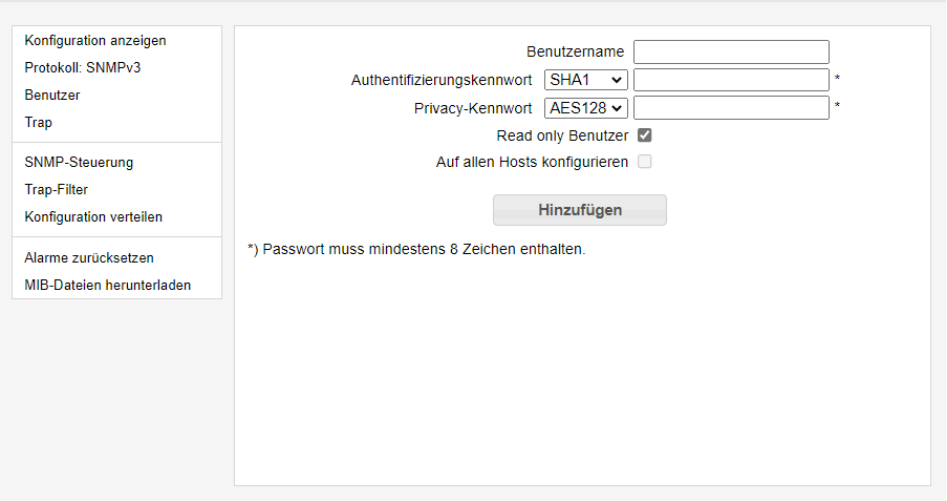


Abbildung 145: SNMP-Konfigurator – Auf allen Hosts konfigurieren

Bei der Verteilung der Konfiguration wird ein solcher Benutzer (einschließlich der diesem Benutzer zugewiesenen Trap-Ziele) auf allen Hostsystemen als Benutzer mit Lesezugriff konfiguriert.

9.3.1.2 SNMP-Steuerungsparameter für alle Hosts definieren

Siehe SNMP-Steuerungsparameter

9.3.1.3 SNMP-Filter für alle Hosts definieren

Siehe Trap-Filter

9.3.1.4 SNMPv3-Benutzereinstellungen an Hosts verteilen

Siehe Verteilung an die Hosts

9.3.1.5 Alle Alarme zurücksetzen

Siehe Alle auf dem RMX oder Assistant ausgelösten Alarme zurücksetzen

9.3.2 SNMPv3-Konfiguration auf dem Manager

Über den SNMP-Konfigurator des Manager können Sie SNMP-Profile (Domains) erstellen. Jedes SNMP-Profil hat seine eigene SNMP-Einstellung wie z. B. SNMPv3-Benutzer, SNMPv1-Communitys, Trap-Ziele, Trap-Filter (einschließlich Host-Trap-Filter und Filter für Fxxxx-Meldungen von RMX) und SNMP-Steuerungsparameter.

Jedes SNMP-Profil enthält eine Liste von OpenScape 4000 V7R2-Systemen (Eine OpenScape 4000 zu einem Profil hinzufügen – es kann auch das OpenScape 4000 eines IPDA-basierten AP-E sein), auf die diese SNMP-Konfiguration angewendet wird. (Alle Einstellungen, die im SNMP-Konfigurator des Assistant definiert sind, können daher auch im Profil des Manager definiert werden.)

Nachdem Sie auf dem Manager ein Profil erstellt haben, können Sie dieses Profils über das entsprechende Profil an die Assistants verteilen.

Im Dialog "Konfiguration verteilen" können Sie die zu verteilenden Profile auswählen. Sie können auch die Art der Verteilung für jedes Profil festlegen, d. h., ob der Assistant die Daten auch an alle Hosts verteilen soll, und, falls ja, ähnlich wie im Assistant-Dialog "Konfiguration verteilen>die Argumente für die Verteilung auswählen.

Sie können den Fortschritt der Verteilung im Dialog "Konfiguration verteilen" überwachen.

Darüber hinaus können Sie für alle verbundenen Systeme per Mausklick auf dem Manager Alle Alarme zurücksetzen.

9.3.2.1 SNMP-Profile

Mit dem SNMP-Konfigurator können Sie SNMP-Konfigurationsprofile erstellen/auswählen/ändern/löschen.

Abbildung 146: SNMP-Konfigurationsmanager

Es gibt auf dem Manager ein lokales Standardprofil, das vom Benutzer bearbeitet werden kann und als SNMP-Konfiguration auf dem Manager verwendet wird. Dieses lokale Profil kann nicht gelöscht werden.

Jedes Profil enthält:

- einen Satz mit den definierten SNMPv1/v3-Konfigurationseinstellungen (SNMPv1-Communitys, SNMPv3-Benutzer, Trap-Ziele)
- die SNMP-Steuerungs-Einstellungen
- den Filter für Fehlertraps (hierzu zählt auch der Filter für die von den 4k-Hosts verwendete app4Kmib)
- eine Liste der Assistants (Eine OpenScape 4000 zu einem Profil hinzufügen), an die das Profil verteilt werden soll

Sie können ein Profil entweder aus einem Kombinationsfeld oder direkt durch Anklicken des Profilnamens auswählen. Über Profil -> Löschen können Sie ein Profil löschen.

SNMPv3-Benutzer

Über das Menü auf der linken Seite (SNMPv3-Benutzer -> Hinzufügen/Ändern/Entfernen) können Sie SNMPv3-Benutzer zum Profil hinzufügen, ändern oder daraus entfernen.

Ein Profil kann mehrere Benutzer enthalten. Ein SNMPv3-Benutzer wird identifiziert durch seinen Namen und geschützt durch zwei Passwörter (Authentifizierungs- und Datenschutz-Passwort). Standardmäßig wird ein SNMPv3-Benutzer mit Lese-/Schreibzugriff erstellt. Dies kann durch Auswahl der Option "Benutzer mit Lesezugriff>geändert werden.

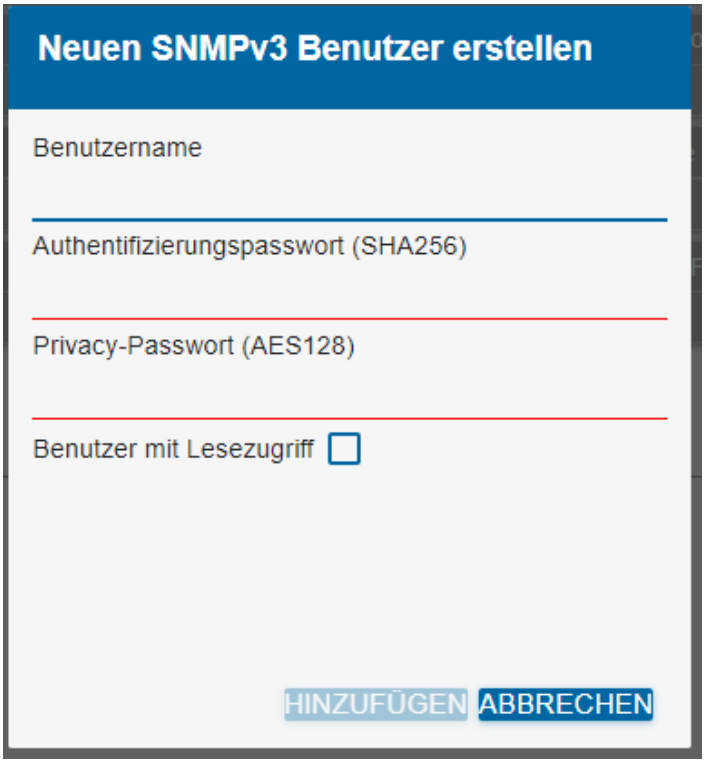


Abbildung 147: Neuen SNMPv3-Benutzer erstellen

SNMPv1-Communitys

Über das Menü auf der linken Seite können Sie eine Community zum Profil hinzufügen oder daraus entfernen: SNMPv1-Community -> Hinzufügen/Entfernen.

Abbildung 148: SNMPv1-Community hinzufügen/entfernen

Ein Profil kann mehrere Communitys enthalten. Eine SNMPv1-Community wird identifiziert durch ihren Namen; nur-Lesezugriff ist möglich.

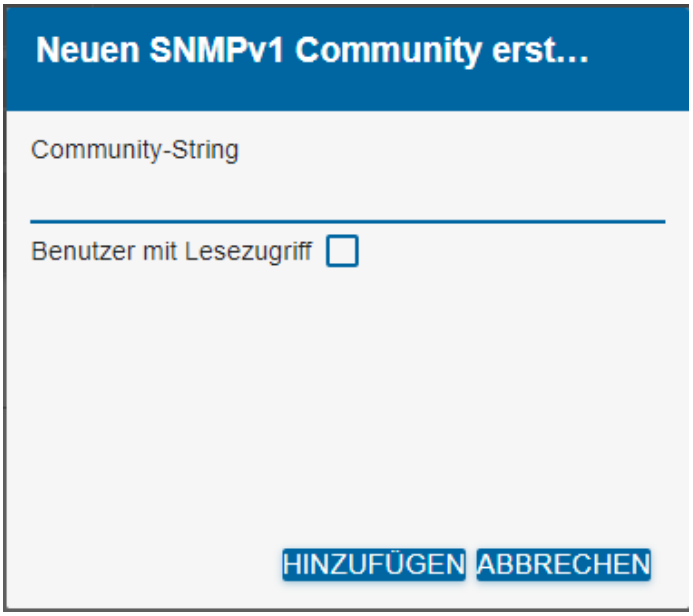


Abbildung 149: Neue SNMPv1-Community erstellen

Trap-Ziele

Über das Menü auf der linken Seite (Trap -> Hinzufügen) können Sie ein neues Trap-Ziel hinzufügen. Über Trap-> Entfernen im Menü auf der linken Seite können Sie ein ausgewähltes Trap-Ziel löschen.

Abbildung 150: Trap hinzufügen/entfernen

Die IP-Adresse eines Trap-Ziels muss einem Benutzer bzw. einer Community zugeordnet werden, der bzw. die beim Senden von SNMP-Traps an das Trap-Ziel verwendet wird. Ein Benutzer bzw. eine Community kann verwendet werden, um Traps an mehrere Trap-Ziele zu senden.

9.3.2.2 Neuen Trap erstellenEine OpenScape 4000 zu einem Profil hinzufügen

Beim Hinzufügen einer OpenScape 4000 zu einem Profil können Sie angeben, dass die im Profil auf diesem OpenScape 4000-System definierte SNMP-Konfiguration verwendet werden soll.

So fügen Sie eine OpenScape 4000 zu einem Profil hinzu:

1) Wählen Sie das Profil (über das Kombinationsfeld oder auf der Registerkarte) aus.
2) Profil auswählenWählen Sie im Menü auf der linken Seite die Option OpenScape 4000-> In Profil verschieben.
3) In Profil verschiebenWählen Sie das System aus, das in das ausgewählte Profil verschoben werden soll, und klicken Sie auf die Schaltfläche VERSCHIEBEN.

Host in Profil verschiebenEin OpenScape 4000-System kann immer nur einem Profil zugeordnet sein. Wenn ein OpenScape 4000-System in ein Profil verschoben wird, wird es automatisch aus dem vorherigen Profil entfernt.

9.3.2.3 SNMP-Steuerung

Über die Option "SNMP-Steuerung>im Menü auf der linken Seite können Sie das Verhalten des SNMP-Fehler-Agenten auf dem OpenScape 4000 Assistant/ Manager steuern.

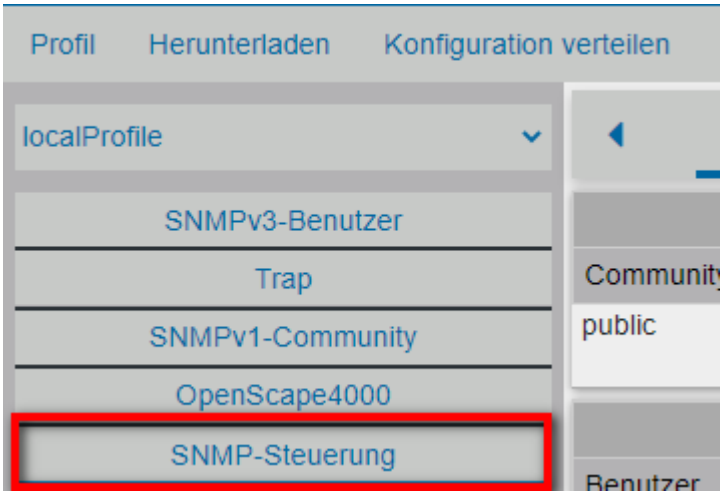


Abbildung 151: Menüpunkt "SNMP-Steuerung"

Folgende Werte können eingestellt werden:

Anzahl der Tage vor der automatischen Fehlerlöschung – RMX Fxxxx-Nachrichten, die älter sind als die angegebene Anzahl von Tagen, werden automatisch aus der Datenbank (lerror-Tabelle) gelöscht.

Erkennungszeitdauer für RMX-Fehlermeldungen – 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.

Abbildung 152: Dialog "SNMP-Steuerung"

9.3.2.4 RMX-Fehlertrap-Filter und Host-Systemereignisse-Filter

In jedem Profil können Sie Filter definieren für:

- Von RMX über die Assistant/Manager-SNMP-Engine als hicomErrorMsg-Traps (aus der hipath4000.mib) gesendete Fxxxx-Meldungen
- Von den einzelnen Hostsystemen im 4k-Bereich gesendete Hostsystem-Ereignisse (aus der app4K.mib)

Filter für Fehlertraps

Mit der Option "Filter für Fehlertraps>im Menü auf der linken Seite können Sie auswählen, welche Fxxxx-Meldung gefiltert werden sollte.

Abbildung 153: Menüpunkt "Filter für Fehlertraps"

Standardmäßig ist der Filter für alle Fxxxx-Meldungen aktiviert.

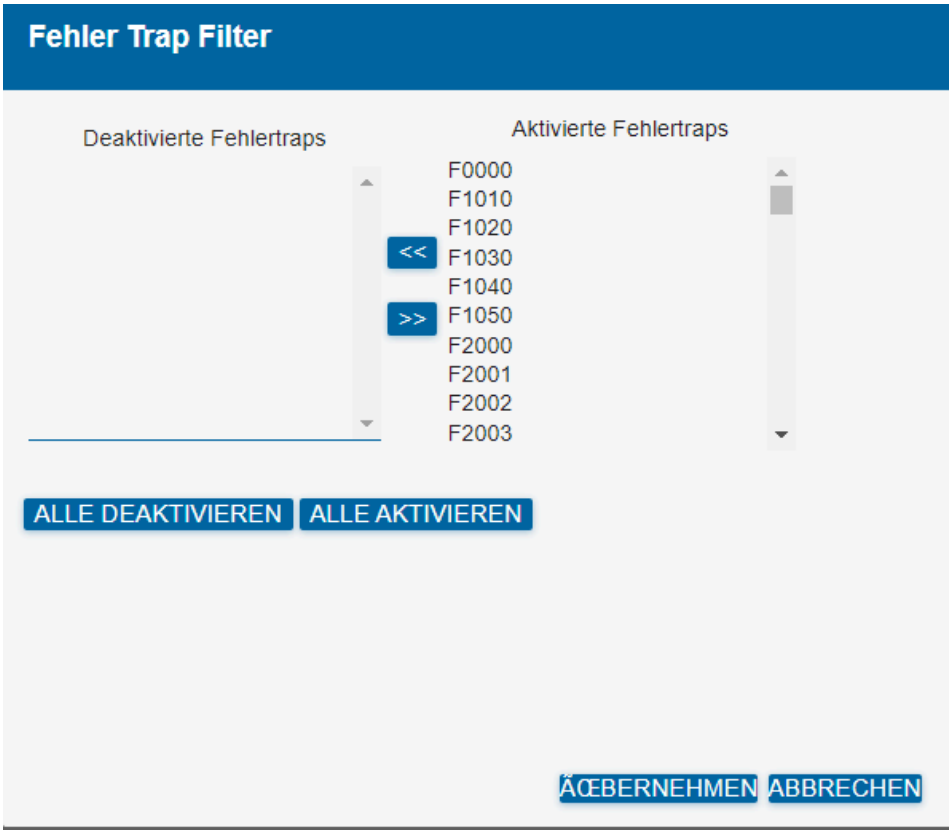


Abbildung 154: Dialog "Fehler Trap Filter"

Host-Systemereignisse-Filter

Klicken Sie auf "Anzeigen Filter", um den für das Profil im Teil "Host-Systemereignisse-Filter>definierten Filter ein- oder auszublenden':

Klicken Sie auf "Ändern Filter", um den Filter zu ändern.

```
# create your filter here
SEVERITY < ERROR
( OID = ".1.3.6.1.4.1.32804.1.9.1.10.10.*" ) AND ( SEVERITY < ALERT )
```

Abbildung 155: Dialog "Host-Systemereignisse-Filter"

9.3.2.5 Änderungen speichern/zurücksetzen

Nach Durchführung der Änderungen erscheint am unteren Seitenrand eine entsprechende gelbe Warnmeldung:

Abbildung 156: Warnmeldung

Solange die Änderungen nicht gespeichert wurden, sind die Änderungen nur im Browser sichtbar; wenn Sie das Browserfenster schließen, ohne Ihre Änderungen zu speichern, gehen alle Änderungen verloren.

Folgende Optionen stehen zur Verfügung:

- Alle (Änderungen) speichern
- (Alle) Änderungen zurücksetzen
- Auf Standard zurücksetzen

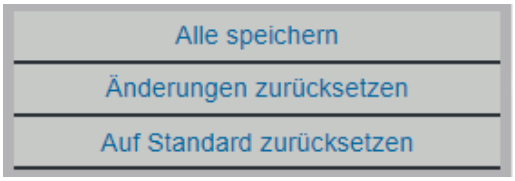


Abbildung 157: Menü "Alle speichern/Änderungen zurücksetzen/Auf Standard zurücksetzen>

Alle (Änderungen) speichern

Über die Option "Alle speichern>im Menü auf der linken Seite können Sie alle über den SNMP-Konfigurationsmanager durchgeführten Änderungen in der Datenbank des Managers speichern.

Die am lokalen Profil durchgeführten Änderungen werden ebenfalls in der SNMP-Engine des Managers gespeichert.

(Alle) Änderungen zurücksetzen

Über die Option "Änderungen zurücksetzen>im Menü auf der linken Seite können Sie alle seit der letzten Speicheraktion durchgeführten Änderungen rückgängig machen – die Wirkung ist dieselbe wie beim Speichern des Browserfensters (ohne vorheriges Speichern).

Auf Standard zurücksetzen

Wenn Sie im Menü auf der linken Seite die Option "Auf Standard zurücksetzen>auswählen und anschließend auf "AUSGEWÄHLTE ZURÜCKSETZEN>klicken, werden alle ausgewählten (oder alle) Profile in den Ausgangszustand (Standard) zurückgesetzt; dabei werden alle im Profil definierten Daten aus der Manager-Datenbank gelöscht.

Abbildung 158: Dialog "Zurücksetzen auf Standardeinstellungen"

Wenn Sie auf die Schaltfläche "ALLES LÖSCHEN>klicken, werden auch alle Profile und alle Einstellungen aus dem lokalen Profil gelöscht. Bei Verwendung dieser Option wird das System in denselben Zustand wie nach einer Neuinstallation zurück versetzt.

9.3.2.6 Herunterladen

Mit der Option "Herunterladen>in der oberen Menüleiste können Sie alle von OpenScape 4000-Systemen unterstützten MIBs herunterladen:

Abbildung 159: Menü "Herunterladen"

9.3.2.7 Konfiguration verteilen

Mit der Option "Konfiguration verteilen>in der oberen Menüleiste verteilen Sie die im Profil angegebenen Konfigurationseinstellungen an die OpenScape 4000

Assistants und alle mit dem OpenScape 4000-System verbundenen Hosts (Aktiv, Standby, Quorum, SoftGates ...).

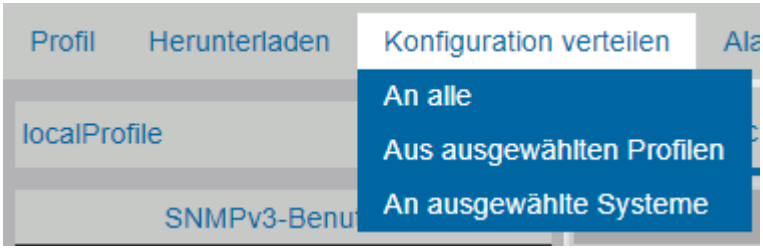


Abbildung 160: Menü "Konfiguration verteilen"

Sie können die Konfiguration verteilen an:

- alle Systeme
- ausgewählte Systeme (aus den kompletten Satz)
- alle Systeme in ausgewählten Profilen

Für jedes System/Profil können Sie auswählen, was verteilt werden soll:

- SNMP-Konfiguration (Benutzer, Communitys, Traps)
- Trap-Filter-Konfiguration (Host-Ereignisse-Filter und RMX-Fxxxx-Filter)
- SNMP-Steuerungs-Parameter (Fehlerlöschungsintervall und Fehlererkennungszeitdauer)

Die Verteilung nimmt normalerweise einige Zeit in Anspruch; öffnen Sie daher den Verteilungsdialog erneut, um die Fortschrittsanzeige anzuzeigen. Der Verteilungsprozess kann einen der folgenden Zustände annehmen: noch nicht gestartet, läuft, abgebrochen, erfolgreich abgeschlossen, mit Fehler beendet.

Eine bereits laufender Verteilungsprozess kann nicht noch einmal gestartet werden.

9.3.2.8 Alarme zurücksetzen

Sie können die Alarme der Systeme zurücksetzen. Diese Aktion hat keine weiteren Auswirkungen, wie dies bei der Verteilung der Konfiguration der Fall ist. Sie können Folgendes zurücksetzen:

- alle Alarme
- die Alarme für das ausgewählte System.

Abbildung 161: Alarme auf ausgewählten Systemen

Der Status für das Rücksetzen von Alarmen wird in der Spalte "Letzter Status" angezeigt (noch nicht gestartet, läuft, abgebrochen, erfolgreich abgeschlossen, mit Fehler beendet). Das Rücksetzen eines Alarms auf einem bestimmten System ist erst dann möglich, wenn für den rückzusetzenden Alarms als letzter Status "Läuft>angezeigt wird.

9.3.3 Konfiguration von Gateways

Mit diesem Leistungsmerkmal können Sie das Gateway-Dashboard verwenden, um:

- die SNMPv1-Konfiguration für eine Liste mit ausgewählten IP-Gateways zu ändern
- die QDC (Quality of Service Data Collection)-Einstellung für eine Liste mit ausgewählten IP-Gateways zu ändern

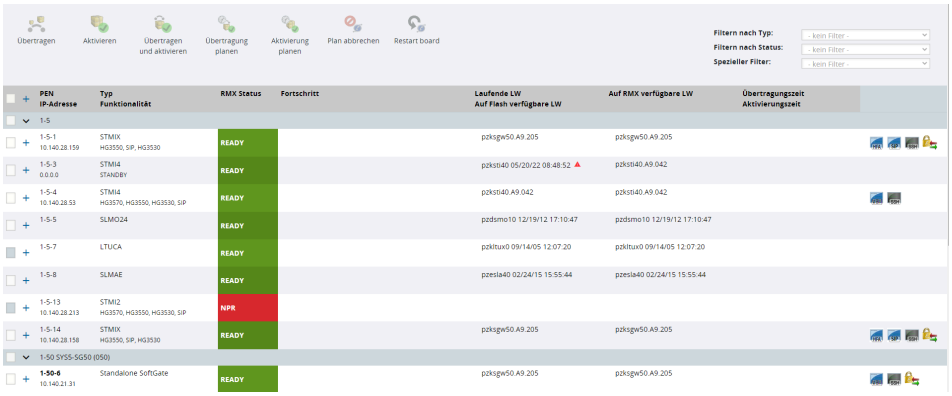


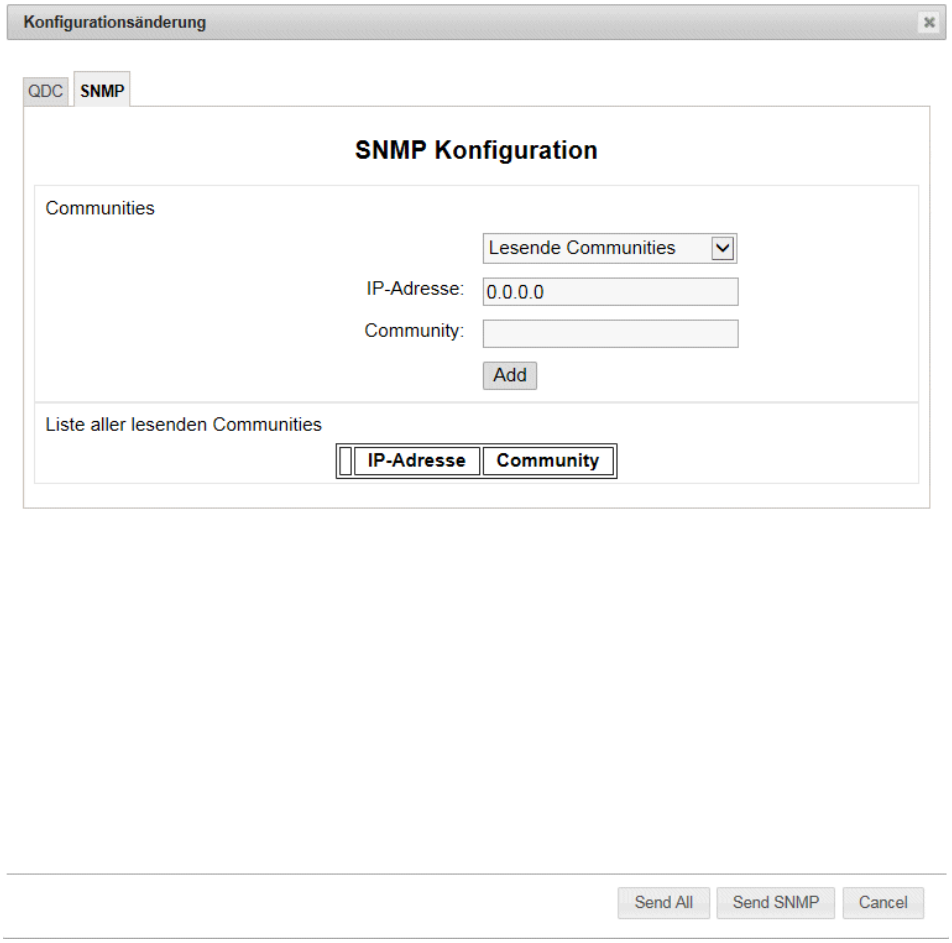
Abbildung 162: Gateway Dashboard

9.3.3.1 Konfiguration ändern

Nachdem Sie einige Baugruppen ausgewählt haben, klicken Sie auf die Schaltfläche "Konfiguration ändern", um das Konfigurations-Widget aufzurufen. Dort können Sie:

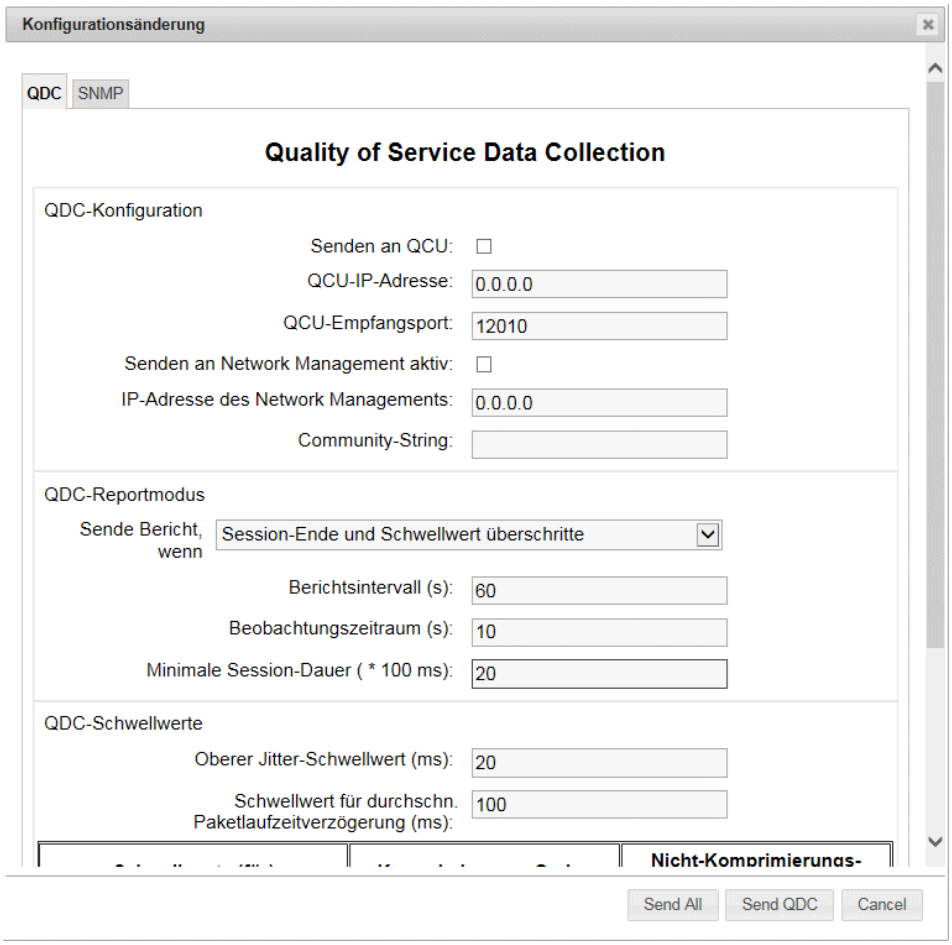
- die SNMP-Konfiguration einrichten – dies geschieht in ähnlicher Weise wie beim Web-Based Management von hardwarebasierten Gateways

Dialog "Konfigurationsänderung"



- die QDC-Daten ändern – dies geschieht in ähnlicher Weise wie beim Web-Based Management des Gateways

Dialog "Konfigurationsänderung"



Nach Übernahme der Änderungen werden diese gespeichert und an alle ausgewählten Baugruppen gesendet ("gespeichert>bedeutet, dass die neue Konfiguration die aktuelle Baugruppenkonfiguration ersetzt). Wenn Sie eine Baugruppe ausgewählt haben, die eine derartige Konfiguration nicht unterstützt, wird die Konfiguration dieser Baugruppe einfach übersprungen.

Sie können folgendes Änderungen übernehmen:

- QDS-Änderungen – nur durch Klicken auf die Schaltfläche "QDC senden"
- SNMP-Änderungen – nur durch Klicken auf die Schaltfläche "SNMP senden"
- QDC- und SNMP-Änderungen – durch Klicken auf die Schaltfläche "Alle senden"

9.4 Manager-Alarme vom OpenScape 4000 Assistant zum OpenScape 4000 Manager weiterleiten

Der OpenScape 4000 Assistant kann Alarme auslösen, die für die OpenScape 4000 Assistant-Software relevant sind (lokale Assistant-Alarme der Alarmgruppe 7, sog. Manager-Alarme). Diese Alarme verwenden das generische Daten-Trap-Modell der HiPath4000.mib (das auch für durch die AFR-Funktion auf RMX ausgelöste Alarme verwendet wird). Diese Alarme werden jedoch nur von der Assistant-SNMP-Engine gemeldet (AFR auf RMX kann so konfiguriert werden, dass Alarme auch auf dem OpenScape 4000-Manager gemeldet werden).

Mit diesem ab Assistant V7R2 verfügbaren Leistungsmerkmal können die Alarme des Assistant als SNMP-Traps gesendet und vom OpenScape 4000 Manager verwaltet werden.

Das heißt, Sie können jetzt:

- vom OpenScape 4000 Assistant ausgelöste Alarme als SNMP-Trap vom OpenScape 4000 Manager empfangen
- die OpenScape 4000 Assistant Alarmstatuseinträge aus dem OpenScape 4000 Assistant-Cache (Datenbank) mittels SNMP-Set-Anforderung auf dem Manager zur OpenScape 4000 Manager-Datenbank (Alarmtabelle) hochladen
- einen Alarm auf dem OpenScape 4000 Assistant mittels SNMP-Set-Anforderung auf dem OpenScape 4000 Manager zurücksetzen

Um dieses Leistungsmerkmal zu aktivieren, müssen Sie auf dem OpenScape 4000 Manager die folgenden zwei Einträge zur Datei /opt/ncc/bin/options hinzufügen (d. h. dort auskommentieren):

STORE_LOG=ON; export STORE_LOG

MANAGER_TRAP=ON; export MANAGER_TRAP

und auf dem OpenScape 4000 Assistant den folgenden Eintrag zur Datei /opt/ncc/bin/options hinzufügen (d. h. dort auskommentieren):

STORE_LOG=ON; export STORE_LOG

9.4.1 Vom OpenScape 4000 Assistant ausgelöste Alarme vom OpenScape 4000 Manager empfangen

Je nach Schweregrad des Alarms, können Sie die folgenden Alarmmeldungen aus der HiPath4000.mib vom OpenScape 4000 Manager empfangen:

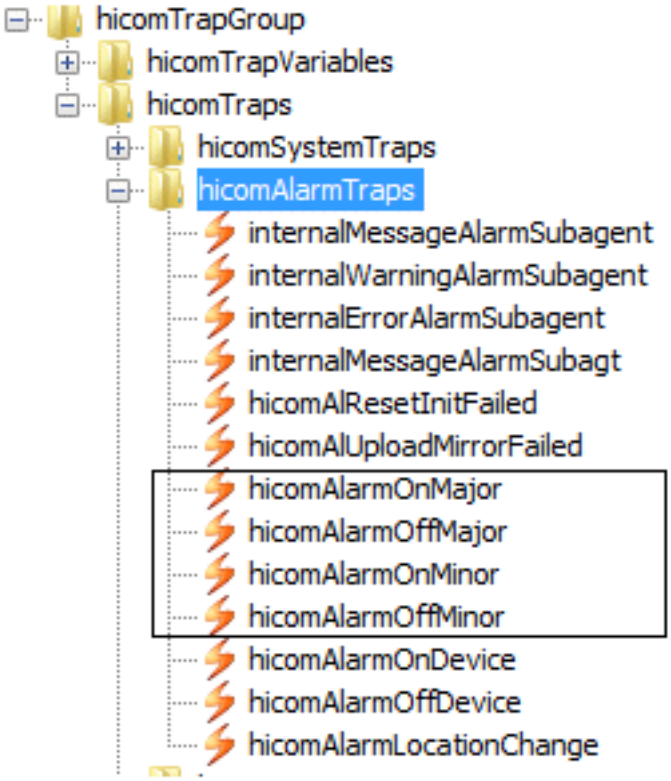


Abbildung 163: hicomAlarmTraps

Jeder Trap enthält Variablenbindungen, über die Ursprung (Assistant) und Art des Problems ermittelt werden können:

- hicomAlTrpSysPabxId ... pabxid aus der hicomSysTable (beziehbar über SNMP .1.3.6.1.4.1.231.7.2.1.1.3) auf dem OpenScape 4000 Assistant – konfiguriert über die OpenScape 4000 Manager Systemverwaltung
- hicomAlTrpSysMnemonic ... in der Systemverwaltung von OpenScape 4000 Manager angegebene System-ID
- hicomAlGroup ... 7 für sog. Manager-Alarme
- hicomAlSubId ... numerische ID des Alarms (1-116)
- hicomAlPriority ... Schweregrad (Severity) des Alarms (1 - Nebenalarm, 2 - Hauptalarm) – redundanter Wert – Schweregrad kann aus dem Trap-Namen ermittelt werden
- hicomAlAbsMod ... der Teil des Assistant, der den Alarm auslöst
- hicomAlStatus ... Status des Alarms (1 - zurücksetzen/aus, 2 - setzen/ein) – redundanter Wert – Status kann aus dem Trap-Namen ermittelt werden
- hicomAlTimDat ... Zeitstempel (Unix-Epochenzeit)
- hicomAlName ... Textbeschreibung des Alarms

9.4.2 Assistant-Alarme auf den Manager hochladen

Wenn Sie die Assistant-Alarme mit der OpenScape 4000 Manager-Datenbank synchronisieren möchten, können Sie dies durch eine SNMP-Set-Anforderung auf dem OpenScape 4000 Manager erreichen:

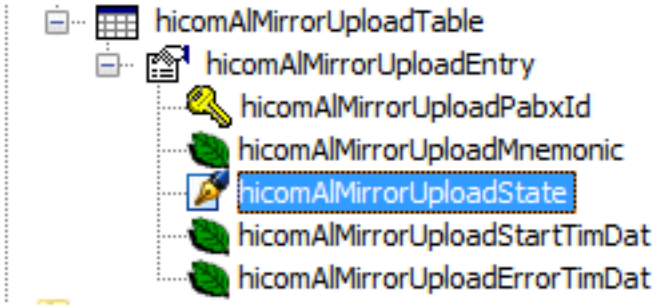


Abbildung 164: hicomAlMirrorUploadState

Wenn Sie den Status hicomAlMirrorUploadState auf "Busy (Besetzt)>(3) setzen, werden die vom Assistant ausgelösten Alarme (in der Set-Anforderung angegeben mit hicomAlMirrorUploadPabxID) mit der Manager-Datenbank synchronisiert (hochgeladen).

9.4.3 Alarme zurücksetzen

Sie können den vom Assistant in der Manager-Datenbank ausgelösten Alarmstatus durch Senden einer SNMP-Set-Anforderung an den OpenScape 4000 Manager im Feld hicomAlReset in der hicomAlTable auf den Wert "Busy (Besetzt)"(3) zurücksetzen.

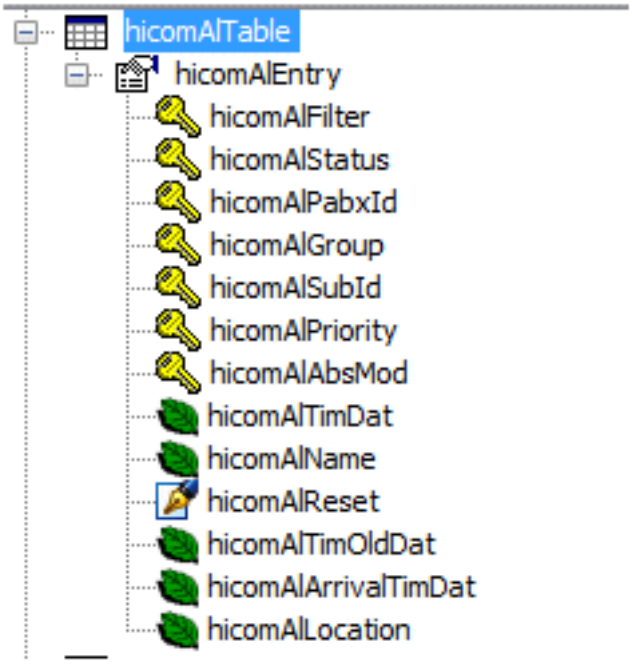


Abbildung 165: hicomAlTable

10 Eingrenzung von Problemen

10.1 Behebung von SNMP-Fehlern

Wenn Subagenten sich nicht problemlos starten lassen bzw. während des Betriebs Störungen auftreten, stehen Informationen zur Verfügung, mit denen sich die Ursachen eingrenzen lassen. Die wichtigste Quelle für solche Informationen ist das Verzeichnis /opt/hipath_agents/log oder /var/hipath_agents/log.

Dieses Verzeichnis enthält für jeden Subagenten eine aktuelle Logdatei, in der die Ausgaben des Agenten seit dessen letztem Start aufgezeichnet werden. Der Name der Datei ergibt sich aus:

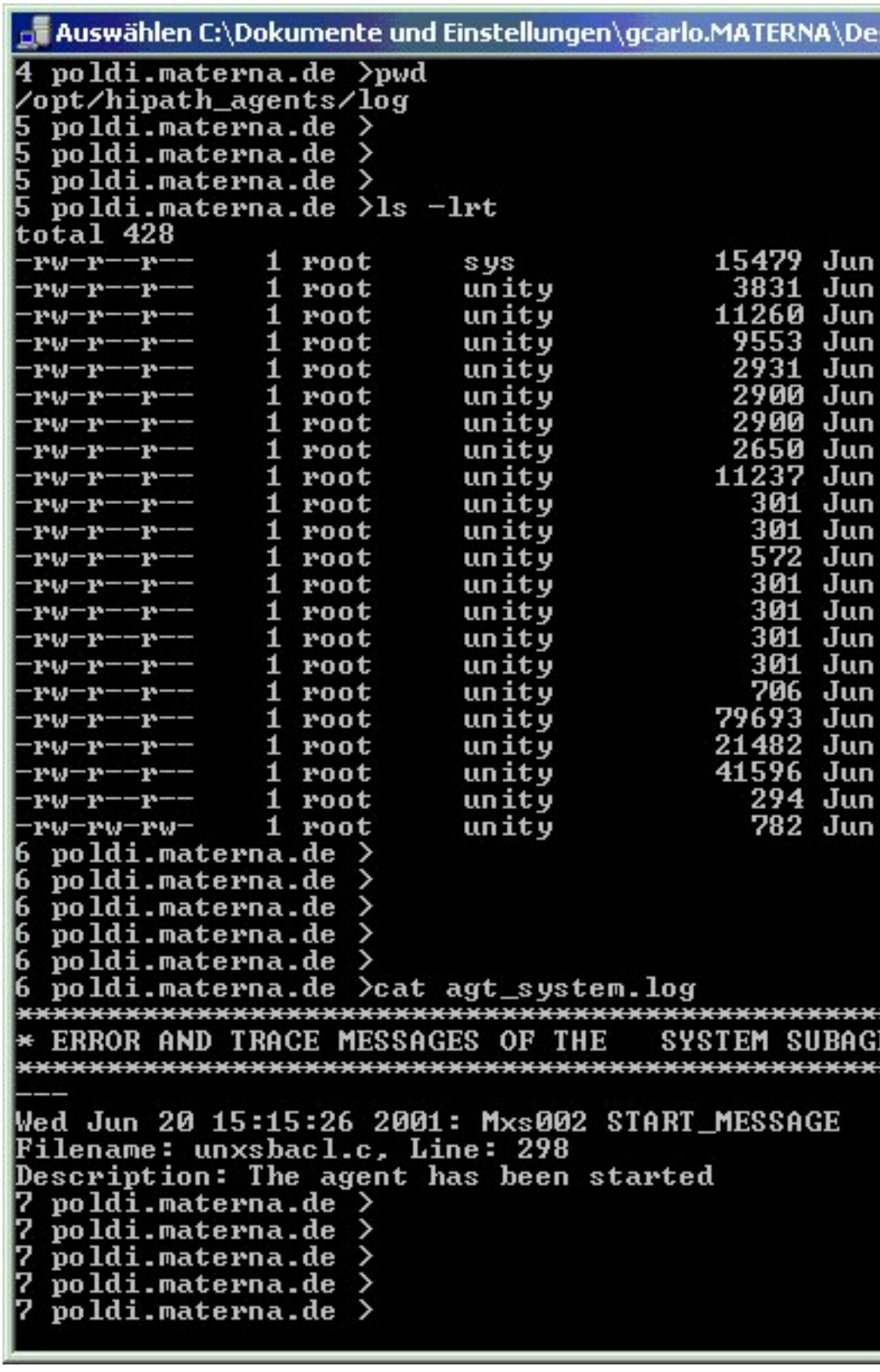
"agt_"+Subagentenname+".log"(+"."+LaufNr)

Pro Subagent werden bis zu zwei alte zusätzlich zur aktuellen Logdatei in diesem Verzeichnis aufgehoben. Die Logdatei ohne laufende Nummer ist jeweils die aktuellste. Bei jedem erneuten Startversuch des Subagenten wird jeweils eine neue Datei erzeugt und alte Dateien werden umbenannt bzw gelöscht.

Wenn ein Subagent nicht startet oder mit einem Fehler abbricht, dann stehen in diesen Logfiles die zugehörige Fehlermeldung sowie die letzten zehn internen Meldungen des entsprechenden Subagenten.

Falls Anhand dieser Meldungen die Fehlerursache nicht direkt klar wird, dann sichern Sie diese Dateien bitte so, daß sie dem Service bzw. Support zur Verfügung gestellt werden können.

Screenshot Log-Verzeichnis


Auswählen C:\Dokumente und Einstellungen\gcarlo.MATERNA\De
4 poldi.materna.de >pwd
/opt/hipath_agents/log
5 poldi.materna.de >
5 poldi.materna.de >
5 poldi.materna.de >
5 poldi.materna.de >ls -lrt
total 428
-rw-r--r-- 1 root sys 15479 Jun
-rw-r--r-- 1 root unity 3831 Jun
-rw-r--r-- 1 root unity 11260 Jun
-rw-r--r-- 1 root unity 9553 Jun
-rw-r--r-- 1 root unity 2931 Jun
-rw-r--r-- 1 root unity 2900 Jun
-rw-r--r-- 1 root unity 2900 Jun
-rw-r--r-- 1 root unity 2650 Jun
-rw-r--r-- 1 root unity 11237 Jun
-rw-r--r-- 1 root unity 301 Jun
-rw-r--r-- 1 root unity 301 Jun
-rw-r--r-- 1 root unity 572 Jun
-rw-r--r-- 1 root unity 301 Jun
-rw-r--r-- 1 root unity 301 Jun
-rw-r--r-- 1 root unity 301 Jun
-rw-r--r-- 1 root unity 301 Jun
-rw-r--r-- 1 root unity 706 Jun
-rw-r--r-- 1 root unity 79693 Jun
-rw-r--r-- 1 root unity 21482 Jun
-rw-r--r-- 1 root unity 41596 Jun
-rw-r--r-- 1 root unity 294 Jun
-rw-rw-rw- 1 root unity 782 Jun
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >
6 poldi.materna.de >cat agt_system.log
****
* ERROR AND TRACE MESSAGES OF THE SYSTEM SUBAG
****

Wed Jun 20 15:15:26 2001: Mxs002 START_MESSAGE
Filename: unxsbacl.c, Line: 298
Description: The agent has been started
7 poldi.materna.de >
7 poldi.materna.de >
7 poldi.materna.de >
7 poldi.materna.de >
7 poldi.materna.de >

11 Abkürzungen

Dieser Abschnitt bietet einen Überblick über die wichtigsten Abkürzungen, die in diesem Handbuch verwendet werden.

Abkürzung	Definition
A&S	Administration & Serviceability
A-LAN	Atlantic LAN
AAAT	Application Access Activation Table
AC	Alternating Current
ACD	Automatic Call Distribution
ACD-G	Automatic Call Distribution Global
ACE	Adaptive Communication Environment
ACX	Administration Center SiniX (SNI-Tool)
ADC	Analog/Digital Converter
ADP	Administration Data Processor; Prozessorkarte im OpenScape/HiPath-
ADS	Administration & Data Server
AFR	Automatic Fault Report
AGP	Accelerated Graphics Port
AM	Administration & Maintenance
AMD	Advanced Micro Devices
AMO	Administration & Maintenance Order; betriebstechnischer Auftrag
AOL	Alert on LAN
API	Application Programming Interface; Anwendungsprogrammierschnittste
ARC	Access Right Configuration; grafische SecM-Oberfläche für die Verwalt Benutzerzugriffsrechten
ASCII	American Standard Code for Information Interchange
ASIC	Application-Specific Integrated Circuit
BDE	Borland Database Engine
Bellcore	Bell Communications Research
BIOS	Basic Input Output System
BVC	BusinessView Composer
BVfT	BusinessView for Telemanagement
BVO	BusinessView Observer

CAC	Carrier Access Code
CAN	Controller Area Network
CAP	Common Application Platform
CBX	Computerized Branch eXchange
CC	Communications Controller
CCP	Communications Controller Program
CD-R	Compact Disc Recordable
CDR	Call/Charge Data Recording; Gebührendatenerfassung
CD-ROM	Compact Disc Read-only Memory
CDB	Common Database
CE	1. Customer Engineer (intern) 2. ConformitÃ© EuropÃ©enne (Eu Kennzeichnung)
CGI	Common Gateway Interface
CHAP	Challenge-Handshake Authentication Protocol
CHD	Customer Header Data; Dienstprogramm für die Konfiguration de
CIF	CMX Interface Facility
C-LAN	Customer LAN; Kunden-LAN
CLA	Customer License Agent
CLI	Command Line Interface; Befehlszeilenschnittstelle
CLS	Central License Server (zentraler Lizenzierungsserver)
CLUC	Cluster Coordinator
CM	Configuration Management
CMS	Communication Management System
CMX	Communications Manager Unixware
COMTES	COMmand TEst Simulator
ComWin	COMTES für Windows
CORBA	Common Object Request Broker Architecture
COS	Class of Service; Berechtigungsklasse
CPU	Central Processing Unit
CRL	Certificate Revocation List (Zertifikatssperrliste)
CRYCO	CRYpted Container and Other crypting functions
CS	Communications Server

CSA	Canadian Standards Association
CSC	Customer Support Center
cusa	**CU**stomer Security Administrator; vordefiniertes Benutzerkonto und Sic Benutzerebene "customer"
cust	CUSTomer; vordefinierte Sicherheitsstufe für Benutzerebene "custome
DAD	Direct AMO Dialog
DAT	Digital Audio Tape
DB	Datenbank
DC	Direct Current; Gleichstrom
DCI	Data Communications Interface
DCM	Data Communications Module
DCO	Data Communications Option
DDR	Double Data Rate
DDR-SDRAM	Double Data Rate Synchronous DRAM
DEP	DEPendability
DF	DiFferential
DID	Direct Inward Dialing, Durchwahl (Telefonie)
DIMM	Dual Inline Memory Module
DISA	Direct Inward System Access
DLL	Dynamic Link Library
DLT	Digital Linear Tape
DMS	Domain Management Service
DMT	Data Migration Tool; Datenmigrationstool
DNIS	Dialed Number Identification Service
DNS	Domain Name Service
DPC5	Data Processor Common Pentium
DRA	Duration of Repair Action
DRAM	Dynamic Random Access Memory
DSCX	Data Processor and Serial Channel Controller Extended (Pentium)
DTD	Document Type Definition
DTE	Data Terminal Equipment; Datenendeinrichtung (DEE)
DTR	Data Terminal Ready

ECC	Error Correcting Code
EEA	Enhanced Error Analysis; erweiterte Fehleranalyse
EEPROM	Electronically Erasable Programmable Read-Only Memory
EIDE	Enhanced Integrated Drive Electronics
EIA	Electronics Industries Association
EISA	Extended Industry Standard Architecture
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMML	Extended Man-Machine Language
EN	Europäische Norm
engr	Engineer; vordefiniertes Benutzerkonto und Sicherheitsstufe für E "service"
EPNP	Enhanced Private Numbering Plan; erweiterter privater Rufnumm
ESD	1. ElectroStatic Dscharge 2. Electrostatic Sensitive Device
ESQL	Embedded Structured Query Language
ESQL/C	Embedded SQL API für Programmiersprache "C"
ETD	Electronic Telephone Directory
FAA	Feature & Account Administration
FAC	Feature Access Code
FAMOS	Fern (= remote) AMO Start
FCC	Federal Communications Commission
FM	Fault Management
FRU	Field Replaceable Unit
FSB	1. Datenbank für FSS 2. Front Side Bus
FSS	Forwarding Support Service: Routing-Komponente von CMX
FTP	File Transfer Protocol
GB	GigaByte
GOSIP	Government Open Systems Interconnection Profile
GUI	Graphical User Interface
HBA	Host Bus Adapter
HD	Hard Disk; Festplatte
HF	HotFix

HXC	HDMS-Xpressions Connector
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HUBC (Hub-C)	hub controller
I2C (I2C, IIC)	Intra Integrated Circuit
IA-32	Intel-Architektur, 32 Bit
IA-64	Intel-Architektur (64 Bit)
IC	Integrated Circuit
ID	IDentifizierung
IDE	Integrated Drive Electronics
IDF	Intermediate Distribution Frame
IDL	Interface Description Language
IDS	Informix Dynamic Server
IE	Internet Explorer (Microsoft)
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IG	Isolated Ground
IGRP	Interior Gateway Routing Protocol
IIOP	Internet Inter ORB Protocol
IP	Internet Protocol
IPDA	Internet Protocol Distributed Architecture (ehemals NBCS)
IS	Installation Specialist
ISA	Industry Standard Architecture
ISDN	Integrated Services Digital Network
ISp	Integrated Server, primary
ISs	Integrated Server, secondary
ISDN	Integrated Services Digital Network
ISN1	Integrated Services Network
IX-BIOS	Unix BIOS auf ADP
JDK	Java Development Kit
JRE	Java Runtime Environment

KV	Korrektur-Version
LAN	Local Area Network
LBU	Line Bus Unit
LCS0	Line Controller S0
LC-Win	Local Configuration - Windows (Name eines Softwareprodukts)
LCR	Least-Cost Routing
LCT	Local Configuration Tool
LED	Light-Emitting Diode
LicM	License Management
LTG	Line Trunk Group
LTU	Line Trunk Unit
LVD	1. Low Voltage Differential (SCSI-Technologie) 2. Low Voltage Di Standards)
LVM	Logical Volume Manager
MAPs	Maintenance Analysis Procedures
MB	MegaByte
MDR	Message Detail Recording
MDSS	Management Decision Support System
MIB	Management Information Base
MLS	Multiple Language Support
MOD	Magneto Optical Disk
MP	MultiProcessor
MPCID	Multi-Purpose Client Interface Daemon
MSAU	MultiStation Access Unit
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NANP	North American Numbering Plan
NAT	Network Address Translation
NBCS	Network-Based Communication System
NIC	1. Network Interface Card 2. Network Information Center
NLS	National Language Support
NM	Network Management

NMI	Non-Maskable Interrupt
NS	NetScape
NSL	Network Security Level
NVMEM	Non-Volatile MEMory
NVRAM	Non-Volatile Random Access Memory
OCSP	Online Certificate Status Protocol
OD	Optical Disk
ODBC	Open DataBase Connectivity
ODF	Object Description File
OLR	Online Replacement
OMC	Operation & Maintenance Center
OpenFT	File Transfer Tool (SNI-Tool)
OPS	Off-Premises Station
ORB	Object Request Broker
OS	Operating System; Betriebssystem
OSI	Open Systems Interconnection
PBX	Private Branch eXchange; Nebenstellenanlage (NstA)
PC	Personalcomputer
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PEN	Port Equipment Number
PID	Process ID; eindeutige numerische Kennung eines Unix-Prozesses
PIN	Personal Identification Number
PL	Private Line
PLD	Programmable Logic Device
PM	1. Performance Management 2. Project Manager
PP	Patch Package
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PROM	Programmable Read-Only Memory
PSTN	Public Switched Telephone Network; öffentliches Vermittlungsnetz
PSIO	Peripheral Serial IO

PSM	Platform Support Module
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Service
RegSvc	Registration Service
REN	Ringer Equivalency Number
RIP	Routing Information Protocol
RLC	Revision Level Complete
RISC	Reduced Instruction Set Computing
RMA	Remote Administration & Maintenance
RMAID	Remote Administration & Maintenance Identification
RPS	Redundant Power System
rsca	remote service customer assistance; vordefiniertes Benutzerkont für Benutzerebene "service"
rsta	remote service technical assistance; vordefiniertes Benutzerkont für Benutzerebene "service"
SAF-TE	SCSI Accessed Fault-Tolerant Enclosure
SAP	Service Agreement Policy
SASH	Stand-Alone SHell
SCSI	Small Computer System Interface
SCO	Santa Cruz Operation
SCU	Server Configuration Utility
SD	System Designer
SDE	Single Data Entry
SDK	Software Development Kit
SDRAM	Synchronous DRAM
SE	1. Single-Ended (SCSI-Abschlussmodus) 2. Systems Engineer
SEA	Strong Encryption & Authentication
SecM	Security Management
SID	System Identification Disk
SIP	Set Installation Package
SIS	Software Information System
SLC	Second Level Cache

SLES	SuSE Linux Enterprise Server
SMP	Symmetric MultiProcessing
SMR	System Maintenance Release
SNM	System & Network Management
SNMP	Simple Network Management Protocol
SNS	System & Network Solutions
SP1	Serviceability Pack 1
SP(o)A	Single Point of Access
SPD	Service Profile Definition
SPOC	Single Point of Configuration
SQL	Structured Query Language
SS	Single System
SSL	Secure Socket Layer
SSO	Smart Switchover
SSSC	Systems/Service & Support Center
STM	SCSI Terminator Module
STM-LVD	SCSI Terminator Module für Low Voltage Differential
STM-SE	SCSI Terminator Module für Single-Ended-Modus
SWA	SoftWare Activation
SWS	SoftWare Supply
SWM	SoftWare Transfer
SWU	SWitching Unit
SysM	System Management
TA	1. Terminaladapter 2. Transportadresse (CMX)
TAO	The ACE ORB
TAP	Techniker Arbeitsplatz
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	Telephony Diagnostics System
TFT	Thin Film Transistor
TIA	Telecommunications Industries Association
TNS	Transport Name Service
TSP	Transport Service Provider

UBA	Unix Basis Administration
UDSC	Uniform Data Security Concept; Benutzer- und Zugangsverwaltu
UI	User Interface
UL	Underwriters Laboratories
ULCT	UNIX Local Configuration Tool
UNA	User & Network Administration
URI	1. Unix RMX Interface 2. Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
USM	UDSC Session Manager
USV	1. Unix Supervisor 2. Unterbrechungsfreie Stromversorgung
UTC	Universal Time Coordinated
UW7	UnixWare 7
VGA	Variable Graphics Array
VPN	Virtual Private Network
WAML	Zugangsmodul für Wide Area Network
WAN	Wide Area Network; Weitverkehrsnetz
WOL	Wake on LAN
XIE	Import/Export Interface
XML	eXtensible Markup Language

Index

N

O

P

Q

S

T

W

Z