A MITEL
PRODUCT
GUIDE

Unify OpenScape Fault Management

Unify OpenScape Fault Management V12, OpenScape Desktop

Bedienungsanleitung
10/2021

A31003-F30C0-U113-01-0019

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 Vorwort

In diesem Kapitel werden folgende Aspekte behandelt:

- Zweck und Adressatenkreis dieses Handbuchs
- Terminologie
- Aufbau dieses Handbuchs
- In diesem Handbuch verwendete Konventionen

1.1 Zweck

Dieses Handbuch beschreibt das OpenScape Fault Management (OpenScape FM).

Das OpenScape FM ist eine Netzwerk- und System Management Plattform. Dieses Handbuch gibt einen Überblick über die Funktionen des OpenScape FM und begleitet den Anwender auf seinen ersten Schritten mit der Management Plattform. Das OpenScape FM ist eine modular aufgebaute Software. Sie besteht aus einem Basis-Modul, das durch die Initialisierung von Plugins um Funktionen zum Netzwerk- und System Management erweitert werden kann.

Das Handbuch beschreibt die graphische Oberfläche und stellt detaillierte Erklärungen zur Arbeit mit dem OpenScape FM bereit. Die einzelnen möglichen Plugins werden in gesonderten Handbüchern beschrieben. Dieses Handbuch adressiert sowohl OpenScape FM-Anfänger wie auch fortgeschrittene Anwender.

Dieses Handbuch geht davon aus, dass der Leser grundlegende Kenntnisse über TCP/IP-Netzwerke sowie Netzwerk- und System-Management besitzt.

1.2 Adressatenkreis

Dieses Handbuch ist für Endanwender bestimmt, die erfahren wollen, wie OpenScape FM Desktop benutzt wird.

1.3 Aufbau dieses Handbuchs

Dieses Handbuch ist folgendermaßen aufgebaut:

- *Kapitel 1, „Vorwort“* zur Erläuterung der Gliederung dieses Handbuchs.
- *Kapitel 2, „Einleitung“* zur Information über den Desktop als Netzwerkmanagement-Applikation.
- *Kapitel 3, „Grundlagen“* zur Information über die theoretischen Grundlagen für den OpenScape FM Desktop.
- *Kapitel 4, „Erste Schritte“* zum Einrichten von Server und Client.

- *Kapitel 5, „Die Bedienoberfläche des Clients“* zur ausführlichen Erläuterung aller Komponenten der Client-Bedienoberfläche.
- *Kapitel 6, „Server-Konfiguration“* erklärt die einzelnen Konfigurationsmöglichkeiten des OpenScape FM Servers.
- *Kapitel 7, „Objekt- und Ereignis-Suche“* beschreibt wie nach Objekten im OpenScape FM Desktop gesucht werden kann.
- *Kapitel 8, „Ereignisaktionen“* erklärt, wie Aktionen für individuelle Ereignisse definiert werden können.
- *Kapitel 9, „Anzeige von Tray Bar Symbolen“* beschreibt wie ein Objekt im Windows Tray Bar überwacht werden kann.
- *Kapitel 10, „Drucken“* zur Erläuterung der Druckfunktionalität des Desktop.
- *Kapitel 11, „Anwendersitzungen“* zur Erklärung des Prinzips der Anwendersitzungen des OpenScape FM Desktop.
- *Kapitel 12, „Erstellen individueller Ansichten“* zeigt den Aufbau einer eigenen Submap-/Objekt-Hierarchie zur Darstellung der Datenbankobjekte.
- *Kapitel 13, „Symbole und Statusanzeige“* zur Beschreibung der Desktop-Symbole und der Funktionalität der dazugehörigen Kontextmenüs.
- *Kapitel 14, „Anwender- und Gruppenverwaltung“* zur ausführlichen Erläuterung der Anwendergruppen- und Anwenderverwaltung.
- *Kapitel 15, „Zugriffsrechte“* zur Erklärung der Zugriffsrechte-Hierarchie und der Zuordnung von Zugriffsrechten für Anwender.
- *Kapitel 16, „Netzwerk Topologie Verwaltung“* zur Beschreibung der hierarchischen Strukturierung der Netzwerkdarstellung und der Verbindungen zwischen Knoten.
- *Kapitel 17, „Hilfefunktionen“* zur Erklärung der im Desktop verfügbaren Hilfefunktionen.
- *Kapitel 18, „Protokollierung“* zur Beschreibung des OpenScape FM Protokollierungsmoduls für OpenScape FM Applikationen und -Komponenten.
- *Kapitel 19, „Backup und Wiederherstellung“* zur Informationen über Backup und Wiederherstellung der OpenScape FM-Datenbank.
- *Kapitel 20, „Zeitpläne“* erklärt wie über den OpenScape FM Desktop Zeitpläne erstellt und konfiguriert werden.
- *Kapitel 21, „Startup Manager“* zur Beschreibung der Funktionen des OpenScape FM Startup Managers.
- *Kapitel 22, „Plugin-Module“* zur Übersicht über die verschiedenen Plugins.
- *Kapitel 23, „Fehlerbeseitigung“* zur Beschreibung verschiedener möglicher Fehlerursachen.
- *Kapitel 24, „Datenbankdateien“* zur Beschreibung der Datenbankdateien des OpenScape FM.
- *Kapitel 25, „NAT-Umgebung“* zur Erklärung wie sich das OpenScape FM in einer NAT-Umgebung verhält.
- *Kapitel 26, „HTTPS und Zertifikate“* zur Erklärung wie HTTPS-Kommunikation zwischen OpenScape FM Server und Clients aktiviert werden kann.

- *Kapitel 27, „SSL-Verschlüsselung“* zur Beschreibung der Verschlüsselung von Daten mit SSL im OpenScape FM.
- *Kapitel 28, „Mobile Access“* erklärt das OpenScape FM Mobile Access App für den Zugang mit Smart-Phones.
- *Kapitel 29, „String-Formatierungssprache“* beschreibt die Sprache, die von unterschiedlichen Plugins verwendet wird, um Texte zu formatieren.

1.4 In diesem Handbuch verwendete Konventionen

In diesem Handbuch werden folgende Schriftkonventionen verwendet:

Fettgedruckte Schrift: Weist darauf hin, dass ein Wort ein wichtiger Begriff ist oder erstmals verwendet wird. Fettgedruckte Schrift wird außerdem für Schaltflächen, Menünamen und Menüeinträge verwendet.

Beispiel: **Proxy-Agent** oder **OK**.

Fettgedruckte Computerschrift: Weist auf Daten hin, die der Anwender eingeben muss.

Beispiel: **`Java`**.

Computerschrift: Weist auf Computerausgaben (einschließlich UNIX-Prompts), einen expliziten Verzeichnis- oder Dateinamen hin.

Beispiel: `Prompt%.`

Kursiv gedruckte Schrift: Kennzeichnet einen Hinweis auf ein anderes Handbuch oder einen anderen Abschnitt im vorliegenden Handbuch.

Beispiel: *siehe IP Manager Bedienungsanleitung.*

Kursiv gedruckte Schrift dient auch der Betonung.

Beispiel: *Alle* Anwender sind davon betroffen.

1.5 Terminologie

- **OpenScape FM** bedeutet OpenScape Fault Management.
- **Server** bezeichnet den OpenScape FM Server, d. h. den Server, auf dem der OpenScape FM Desktop installiert ist.
- **Client** bezeichnet den OpenScape FM Client; typischerweise einen Web-Browser, in dem OpenScape FM aufgerufen ist.
- **Desktop** bezeichnet den OpenScape FM Desktop.

Wichtiger Hinweis:
Der Begriff „Desktop“ wird im gesamtem Handbuch verwendet. Dabei ist es wichtig, zu beachten, dass der Desktop das OpenScape FM Framework UND die möglicherweise initialisierten Plugin-Module umfasst. Siehe auch *Kapitel 22, „Plugin-Module“.*

2 Einleitung

Unternehmen müssen sich darauf verlassen können, dass ihre IT-Infrastruktur und die darauf aufbauenden Geschäftsprozesse zuverlässig funktionieren. In einem derartigen Umfeld ist es wichtig, dass auftretende Infrastruktur-Probleme frühzeitig erkannt und beseitigt werden, bevor sie größeren Schaden anrichten können, oder besser noch, bevor sie sich überhaupt auswirken.

Das OpenScape FM ist eine System- und Netzwerk Management Plattform, die mit Hilfe des IP-Manager Plugins die IT-Infrastruktur überwachen kann (siehe *IP Manager Plugin Bedienungsanleitung*). Das System Management Plugin ergänzt den IP-Manager nahtlos um Funktionen, mit denen die Überwachung von System-Parametern realisiert werden kann (siehe *System Manager Plugin Bedienungsanleitung*).

Durch eine geeignete Konfiguration des IP-Manager Plugins und des System Management Plugins wird es möglich, auftretende Probleme frühzeitig zu erkennen, um die Störungen schnell und gezielt bearbeiten zu können.

Das OpenScape FM besteht aus einem Basis-Modul (u. A. die graphische Oberfläche), in das die Management-Plugins IP-Manager und System Management eingebunden werden. Das Basis Modul bietet hierbei einen einheitlichen Zugriff auf die Topologiedarstellung und die Funktionen dieser beiden Plugins.

Es sind eine Vielzahl weiterer Plugins verfügbar, die weitere Management-Funktionen und die Überwachung unterschiedlicher Technologien, wie HiPath 4000 oder OpenScape Voice, bereitstellen.

2.1 Logische Architektur

Bild 1 gibt einen Überblick über die modulare Struktur des OpenScape FM. Die Kern-Komponenten stellen die Basis-Features bereit, die von den anderen Komponenten (Plugins) verwendet werden.

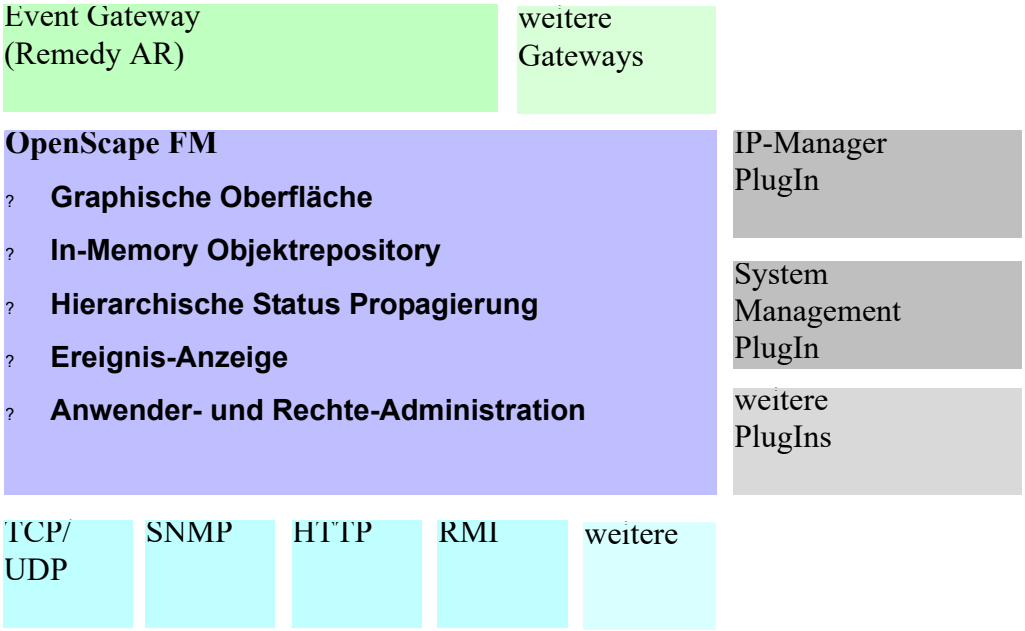


Bild 1 Logische Architektur

Durch **Plugins** werden die Funktionen des OpenScape FM um spezifische Funktionen erweitert. Sie binden spezifische Management Funktionalitäten für die zu überwachenden Ressourcen in das OpenScape FM ein.

Gateways ermöglichen die Integration mit anderen Applikationen wie z, B. Help-Desk-Applikationen oder Workflow-Processing.

2.2 Technische Architektur

Das OpenScape FM besteht aus einem Management-Server und aus Management-Clients. Die Clients stellen die verwalteten Objekte in einer graphische Oberfläche dar. Unterschiedliche Anwender können mit dem gleichen Management-Server arbeiten.

Bild 2 zeigt ein Beispiel-Szenario, das aus einem OpenScape FM-Server und zwei damit verbundenen OpenScape FM-Clients besteht.

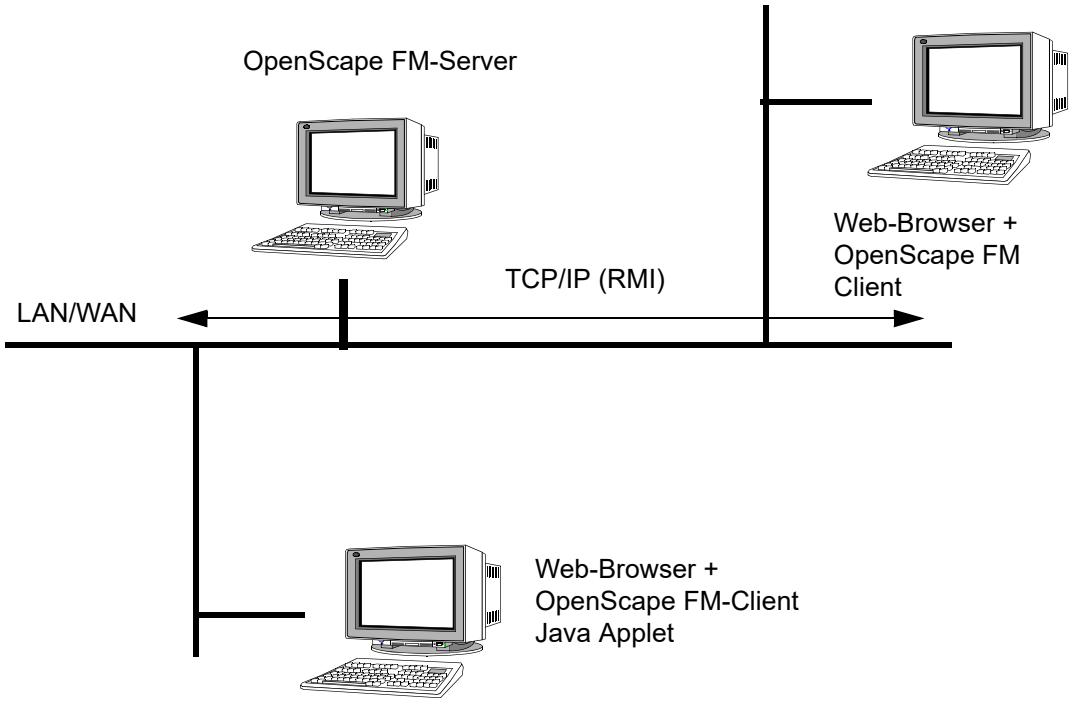


Bild 2 Client/Server-Architektur

Clients werden als Java-Applet in einem Web-Browser gestartet. Zusätzlich besteht die Möglichkeit eine eigenständige Clienten-Applikation zu installieren.

2.3 Funktionalität

Das OpenScape FM stellt die folgenden Funktionen zur Verfügung:

- **Graphische Oberfläche:** Die im OpenScape FM-Server verwalteten Objekte werden mit Hilfe des OpenScape FM-Clients graphisch dargestellt.
- **Objektrepository:** Jede vom OpenScape FM verwaltete Komponente wird als Objekt im Objektrepository des Servers abgelegt. Diese In-Memory Struktur wird im Hintergrund in einer persistenten Datenbasis abgelegt und ermöglicht einen schnellen Zugriff durch die Clients.
- **Hierarchisch strukturierte Sichten:** Die verwalteten Objekte werden durch Vater/Kind-Relationen zueinander in Bezug gebracht.
- **Einfache Navigation durch den Einsatz von Submaps und Objekt-Bäumen:** Die verwalteten Objekte und ihre Topologie werden durch den Einsatz von Submaps und Objekt-Bäumen repräsentiert.
- **Farbliche Status-Anzeige:** Jedem verwalteten Objekt ist ein Status zugeordnet. Bestimmte Objekte haben einen zusammengeführten Status, der aus der Zusammenfassung des Status der Kindobjekte berechnet wird.

- **Ereignis-Browser:** Ereignisse, welche die verwalteten Objekte betreffen, werden in einem Ereignis-Browser dargestellt.
- **Anwender- und Rechte-Verwaltung:** Um die Aktionen von Anwendern im System kontrollieren zu können, ermöglicht der OpenScape FM-Server die Administration von Anwendern und deren Rechten.
- **Definition eigener Sichten:** Es ist möglich, spezifische Sichten zu definieren. Auf einer derartigen Sicht können dann ausgewählte Objekte abgelegt werden.
- **Client als Java Applet:** Der Client wird zusammen mit dem Server installiert und läuft als Java-Applet in einem Web-Browser. Um einen Client starten zu können, ist keine weitere Installation notwendig.
- **Sichern und Wiederherstellen:** Das OpenScape FM bietet einen automatisierten Sicherungsmechanismus an. Hiermit ist es möglich das Objektrepository zu sichern und gesicherte Stände wieder einzuspielen.

3 Grundlagen

Dieser Abschnitt bietet einen Überblick über die grundsätzliche Funktionsweise von OpenScape FM Desktop.

3.1 Datenbanken und Objekte

Das Herzstück des OpenScape FM Managers ist die Datenbank. Alle verwalteten Instanzen wie Netzwerke, Teilnetzwerke, Server, Anwender, Zugriffsrechte und andere werden als Objekte mit eigenen Objektnamen in dieser Datenbank gespeichert. Die gesamte Datenbank ist hierarchisch strukturiert, d. h., jedes Objekt kann über untergeordnete Objekte (Kindobjekte) verfügen. Ist z.B. ein Server mit verschiedenen Ethernet-Adaptern gegeben, so wird jeder Adapter als untergeordnetes Objekt des Servers dargestellt. Ein Netzwerk mit Namen „Deutschland“, das über die beiden Teilnetzwerke „Nord“ und „Süd“ verfügt, wird mit den beiden Teilnetzwerken als dem Netzwerk untergeordnete Objekte dargestellt. Jedes Objekt wird in der Datenbank nur ein einziges Mal gespeichert.

3.2 Symbole

Innerhalb der Bedienoberfläche werden Symbole verwendet, um die Objekte darzustellen. Jedes dieser Symbole ist definiert durch eine Form, Bitmap und Bezeichnung.

Ist ein Symboltyp und ein Bezeichner für einen spezifischen Objekttyp festgelegt, so wird in der Voreinstellung über Form und Bitmap des Symbols der Objekttyp angezeigt, um über diese Darstellung einen schnellen Überblick über die verschiedenen Gerätetypen des Netzwerks zu ermöglichen. Beispielsweise würde ein PC mit Windows NT als Rechteck mit einem Windows-Symbol in der Mitte angezeigt.

Symbole, die ein Element repräsentieren, das einem anderen Objekt/Symbol untergeordnet ist, werden auf der Submap des übergeordneten Symbols dargestellt. So wird z.B. ein Interface-Symbol unterhalb des Symbols angeordnet, das den Host repräsentiert, dem das Interface zugeordnet ist.

Objekte können durch mehr als ein Symbol repräsentiert werden, sofern sich diese Symbole auf verschiedenen Submaps befinden (siehe *Abschnitt 3.4.1*).

Wird ein Objekt gelöscht, so werden alle Symbole, die das Objekt repräsentieren, entfernt, und das Objekt wird aus der Datenbank entfernt.

Wird ein Symbol gelöscht, so wird nur die einzelne Repräsentation des Objekts entfernt.

3.3 Ereignisse

Ereignisse beschreiben im OpenScape FMVorkommnisse, die sowohl von außen an das System herangetragen (durch z.B. SNMP-Traps), oder die durch interne Mechanismen vom OpenScape FM selbst erkannt wurden (siehe *Kapitel 8*).

Häufig beschreiben Ereignisse das Auftreten oder das Klarmelden eines Problems. So kann z.B. ein Ereignis durch die Nicht-Erreichbarkeit eines IP-Interfaces ausgelöst werden, und ein weiteres Ereignis beschreiben, dass das gleiche Interface wieder erreicht werden kann.

Ereignisse werden in der Regel dem Objekt im OpenScape FM zugewiesen, das inhaltlich zum Problem passt. Im Beispiel wäre dies das Objekt, dass das nicht erreichte Interface repräsentiert.

Jedem Ereignis wird automatisch ein Status zugeordnet, der die Schlimme des Problems repräsentiert. Für das Nicht-Erreichen des Interfaces ist dies der Status ‚*Critical*' für die später festgestellte erneute Erreichbarkeit der Status ‚*Normal*'.

Jedem Status ist eine Farbe zugeordnet. Für ‚Critical' ist dies z.B. rot, für ‚Normal' grün (siehe *Abschnitt 5.11*).

Jedes neue Ereignis befindet sich initial im Zustand ‚*Unbestätigt*'. Dieser Zustand zeigt an, dass ein Problem akut ist und in der Oberfläche angezeigt werden soll.

Es kann durch einen Bearbeiter, oder durch automatische Gutmeldungen, in den Zustand ‚*Bestätigt*' versetzt werden.

Der Status und die Farbe eines Symbols in der Oberfläche ergeben sich in der Regel aus dem ‚schlimmsten' unbestätigten Ereignis, das dem zugehörigen Objekt zugewiesen ist.

Ein Ereignis kann zusätzlich von einem Benutzer ‚*In Arbeit*' genommen werden. Dies hat keinen Einfluss auf den Status des Objektes, es wird aber allen Benutzern angezeigt, welcher Bearbeiter sich aktuell um das Ereignis kümmert.

In der Server-Grundeinstellung führt das Bestätigen eines Ereignisses automatisch dazu, dass das Attribut *In Arbeit* vom Ereignis entfernt wird. Diese Voreinstellung kann innerhalb der Server-Administration geändert werden (**Server->Administration->Server-Eigenschaften - Ereignisbrowser** - siehe *Abschnitt 6.4*)

3.4 Ansichten

Die Beziehungen zwischen Objekten und den jeweiligen untergeordneten Objekten werden in der Bedienoberfläche auf zwei Arten dargestellt: als Submap und als Baum-Ansicht.

3.4.1 Submaps

Eine Submap ist eine zweidimensionale grafische Darstellung aller untergeordneten Objekte eines Objektes. Die Submap eines Objekts kann also geöffnet werden, um zu sehen ob sie untergeordnete Objekte enthält.

Wird beispielsweise die Submap eines Netzwerkobjekts geöffnet, dem drei Server untergeordnet sind, so werden diese drei Server auf der Submap des Netzwerks angezeigt.

Objekte werden durch ein Symbol auf einer Submap repräsentiert. Sie können aber auch durch andere Symbole auf anderen Submaps repräsentiert werden (siehe *Bild 1*). Das Verändern der Form und Bitmap eines Symbols ändert nicht das Objekt welches es repräsentiert.

3.4.2 Bäume

Ein anderes Verfahren zur Darstellung der hierarchischen Beziehungen von Datenbankobjekten ist die Baum-Ansicht. Die Objekte werden in einer Baumstruktur dargestellt, die den hierarchischen Status der Objekte widerspiegelt. Jedes Objekt wird mit einem Symbol dargestellt, das für die jeweilige hierarchische Position charakteristisch ist. Wenn ein Symbol an einer bestimmten Stelle innerhalb der Objekthierarchie geändert wird, erfolgt lediglich an dieser Stelle eine Änderung der Baum- und Submap-Darstellung (*Bild 1*). Eine detaillierte Erläuterung des Navigationsbaums finden Sie unter *Abschnitt 5.13, „Systemnavigation mit Hilfe des Navigationsbaums“*.

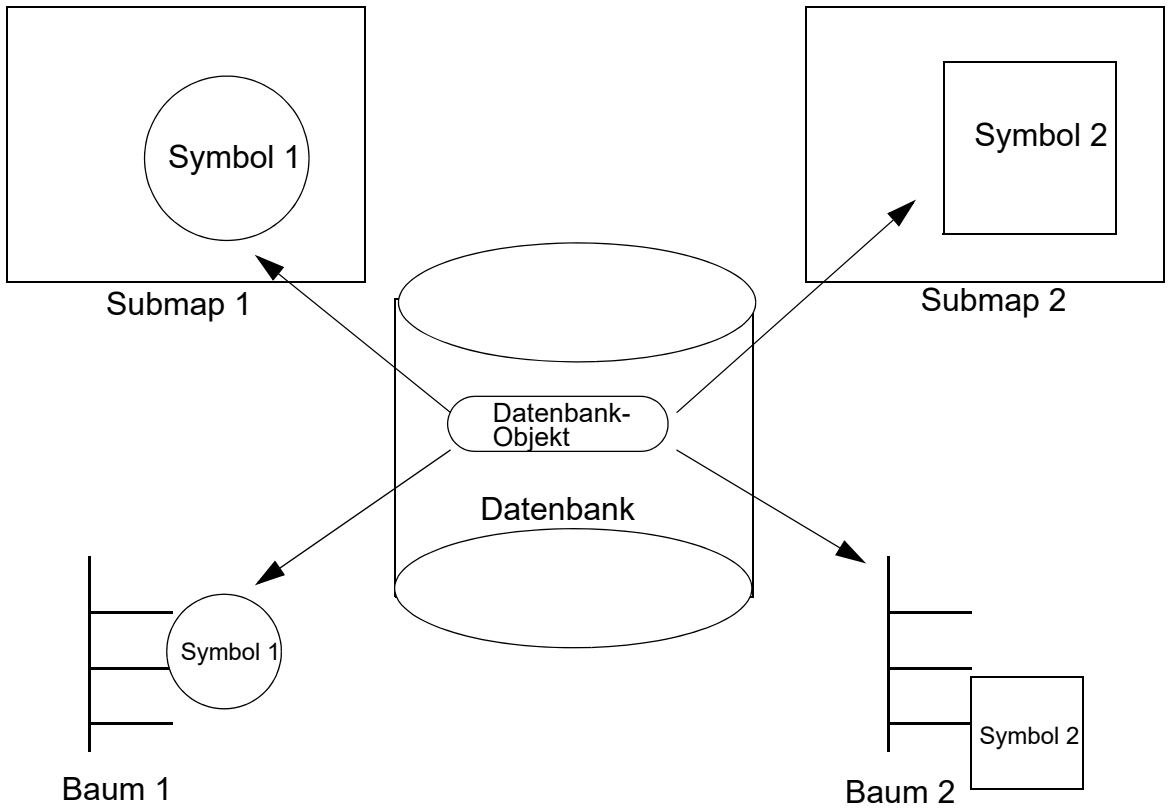


Bild 1 *Darstellung eines Objekts in zwei verschiedenen Submaps und einem Baum.*

3.5 Maps

Eine Map ist eine Sammlung von Submaps, die die Hierarchie der verwalteten Objekte darstellt. Es können gleichzeitig zahlreiche Maps existieren. Mit Hilfe der verschiedenen Maps können unterschiedliche Arbeitsumgebungen erzeugt werden, die durch folgende Kriterien gekennzeichnet sind:

- Symbolposition auf den Submaps
- Hintergrundbild von Submaps
- Skalierung von Submaps

- Symboltypen für die verwalteten Objekte

Es sei erneut angemerkt, dass auf einem OpenScape FM-Server nur eine Datenbank existiert. Daher beruhen alle Maps auf dem selben Datenbestand.

3.6 Anwender

Um eine Zugangskontrolle zu ermöglichen, unterstützt OpenScape FM Desktop eine Anwender- und Anwendergruppenverwaltung. Ein Anwender wird durch ein Objekt in der Datenbank repräsentiert. Jedem Anwender ist ein Login-Name und ein Paswort zugewiesenen. Eine Anwendergruppe wird ebenfalls durch ein Objekt in der Datenbank repräsentiert. Anwendergruppen werden benutzt um einer Menge von Anwendern in einem Schritt Zugriffsrechte zuzuweisen. Informationen zur Anwenderverwaltung finden Sie unter *Kapitel 14, „Anwender- und Gruppenverwaltung“*.

3.7 Zugriffsrechte

Die Funktion eines Anwenders definiert sich durch die ihm zugewiesenen Zugriffsrechte. Diese Zugriffsrechte können einem Anwender entweder direkt oder über eine Anwendergruppe, in der er enthalten ist, zugewiesen werden. Zugriffsrechte können für bestimmte Objektgruppen vergeben werden. Ferner ist es möglich, einem Anwender nur Zugang zu bestimmten Menüs zu gewähren oder Anwenderverwaltungsrechte für ein konkretes Objekt zu vergeben und gleichzeitig den Zugriff auf andere Objekte zu unterbinden. Eine detaillierte Erläuterung der Verwaltung von Zugriffsrechten finden Sie unter *Kapitel 15, „Zugriffsrechte“.*

4 Erste Schritte

In diesem Kapitel werden allgemeine Aspekte behandelt, welche die ersten Schritte in OpenScape FM Desktop unterstützen sollen.

Als Erstes muss der Server installiert werden. Mehr dazu findet sich in *Anhang C, „Installationsprozess“*.

Anschließend können der Server gestartet und ein oder mehrere Clients verwendet werden.

4.1 Server-Start

Der Startup Manager wird standardmäßig zusammen mit OpenScape FM installiert. Der Startup Manager sorgt dafür, dass der OpenScape FM-Server nach der Installation automatisch gestartet wird. Weiterführende Informationen zum Startup Manager finden sich in *Kapitel 21, „Startup Manager“*).

Eine detaillierte Beschreibung der Installation von OpenScape FM Desktop findet sich unter *Anhang C, „Installationsprozess“*. Es wird eine Java(TM)-Laufzeitumgebung (Java(TM) Runtime Environment, JRE) benötigt. Eine detaillierte Beschreibung der Erstkonfiguration finden sich unter *Anhang B, „Anforderungen an die Hardware- und Software-Umgebung“* und *Anhang D, „Systemkonfiguration“*.

4.1.1 Sicherer Datentransfer mit OpenScape FM

OpenScape FM nutzt standardmäßig die sichere Datenübertragung mit einer Verschlüsselung nach dem SSL/HTTPS-Standard. Mehr zu diesem Theme findet sich in *Kapitel 26, „HTTPS und Zertifikate“* und *Kapitel 27, „SSL-Verschlüsselung“*.

4.2 Starten des Clients

Es gibt verschiedene Verfahren für den Start des Clients. Diese Verfahren werden in den nachfolgenden Absätzen beschrieben. Unabhängig von der verwendeten Startmethode wird die gleiche Bedienoberfläche angezeigt.

4.2.1 Management über Web-Browser

Das Standard-Zugangsverfahren des OpenScape FMerfolgt über einen Web-Browser mit Java(TM)-Unterstützung (Versionsinfo unter *Anhang B, „Anforderungen an die Hardware- und Software-Umgebung“*). In diesem Fall startet die URL des OpenScape FM-Servers die Landing Page des OpenScape FM.

```
https://<OpenScape FM server>:3043/
```

Die Auswahl der Schaltfläche **Client Installer** installiert einen lokalen OpenScape FM Client im Home-Verzeichnis des Anwenders und legt einen Startmenüeintrag und einen Desktop-Link an. Über beide kann der Java-Client gestartet werden.
Clients, die mit dieser Methode installiert werden, sind Bestandteil des automatischen Update-Prozesses.

Mit der Schaltfläche **Portabler Client** wird ein Download angestoßen, das den Client als eine Datei mit dem Namen `osfmPortableClient.exe` im Download-Verzeichnis des Anwenders ablegt. Diese Datei kann dann z.B. per USB-Stick auf einen anderen Rechner kopiert und dort für die Installation des Client verwendet werden. Portable Clients sind nicht Bestandteil des automatischen Update-Prozesses.

Die Schaltfläche **Web** startet den Web-Client in einem Web-Browser.

Für den Browser muss das Java(TM)-Plugin installiert sein (Versionsinfo siehe *Anhang B, „Anforderungen an die Hardware- und Software-Umgebung“*).

Es wird ein Browser-Fenster mit der Bedienoberfläche des OpenScape FM Desktop angezeigt. Informationen zum Login-Vorgang finden sich unter *Abschnitt 4.3, „Login“*.

4.2.2 Management über die Client-Applikation

Ein alternativer Weg zur Verwendung des Clients ist der Zugriff über die eigenständige Client-Applikation:

Der Befehl **Start->Programme->OpenScape FM->Start Client (HTTPS)** startet die Client-Applikation in der Java(TM)-Laufzeitumgebung (Java(TM) Runtime Environment, JRE) in dem bei der Installation festgelegten Pfad.

Dies aktiviert die Datei `index.jnlp`, die mit einem **Java(TM) Web Start Launcher** gestartet werden sollte.

Läuft bereits ein Client, kann mit Hilfe des Eintrages **Client->Neuer Client** aus dem Hauptmenü eine Client-Applikation gestartet werden.

4.2.3 Management über die Unify Common Management Platform

Innerhalb des Unify-Umfeldes kann der OpenScape FM Client auch über die Common Management Platform (CMP) gestartet werden.

Für die initiale Einrichtung des Single Sign-on (SSO) auf der CMP wird ein OpenScape FM Benutzerzugang mit Administrator-Rechten benötigt.

Wird die Verbindung zum OpenScape FM im CMP eingerichtet (**Maintenance->Inventory->Applications**) und gespeichert, akzeptiert das OpenScape FM das Zertifikat des CMP Webservers auf Port 4709 automatisch.

Dieses Zertifikat kann wie gewohnt im OpenScape FM Client über **Server->Administration->SSL Zertifikate->Zertifikate anzeigen** auf der Seite **Vertrauenswürdige Zertifikate** eingesehen werden (siehe *Abschnitt 27.3*).

4.3 Login

Ist der Client gestartet, muss eine Anmeldung auf dem OpenScape FM Server erfolgen. Auf der Login-Seite kann ein OpenScape FM Server ausgewählt werden. Außerdem auch der RMI-Port der zur Verbindung gewählt werden soll. Wurde für den Server kein bestimmter Port konfiguriert, erfolgt die Verbindung über den OpenScape FM Standardport 3042.

4.3.1 Anmeldung

Die Anmeldungen erfolgt mit einem Anwendernamen (**Kennung**) und dem zugehörigen **Passwort** auf dem angegeben OpenScape FM **Server**.

Ist während des Eintippens des Passwortes die Feststelltaste aktiv, erscheint als warnender Hinweis ein Dreieck rechts neben dem Passwort-Eingabefeld.

Über die Auswahlmenüs **Sprache** und **Look & Feel** kann das Erscheinungsbild des Clients bestimmt werden.

In der Bedienoberfläche des Clients wird der Server immer zusammen mit dem Namen des aktuell angemeldeten Anwenders und dem Namen der aktuell geöffneten Map in der rechten oberen Ecke angezeigt.

Beim ersten Login als Anwender „Root“, d. h. nach Beendigung des Installationsprozesses, erfolgt eine Aufforderung, ein Passwort für „Root“ festzulegen (*Kapitel 15, „Zugriffsrechte“*).

Bei der ersten Anmeldung als ’normaler’ Anwender, erfolgt ebenfalls eine Aufforderung ein (neues) Passwort festzulegen (*Kapitel 14, „Anwender- und Gruppenverwaltung“*).

Soll die Anmeldung mit einem anderen Anwendernamen erfolgen, kann dies über den Hauptmenüeintrag **Client**–>**Abmelden** erfolgen. Es ist kein Neustart des Clients und keine explizite Abmeldung erforderlich.

4.3.2 Client-Abmeldung

Um den aktiven Anwender abzumelden, kann der Hauptmenüeintrag **Client**–>**Abmelden** verwendet werden.

Der Hauptmenüeintrag **Client->Beenden** schließt zusätzlich den Client.

5 Die Bedienoberfläche des Clients

In diesem Kapitel wird die Bedienoberfläche des OpenScape FM Desktop-Clients beschrieben. Der erste Teil enthält allgemeine Informationen zur Organisation von Managementdaten sowie deren Anzeige im OpenScape FM Desktop-Client. Ferner erfahren Sie hier, welche Oberflächenelemente für die Navigation zwischen verschiedenen Informationsansichten zur Verfügung stehen.

Der Rest dieses Kapitels setzt sich detailliert mit den vier Hauptkomponenten des OpenScape FM Desktop auseinander: Topologie-Viewer, Baum-Viewer, Submap-Viewer und Ereignis-Browser. Sie erfahren hier, wie Sie die Netzwerkhierarchien durchsuchen und auf die Informationen zu den verwalteten Ressourcen zugreifen können.

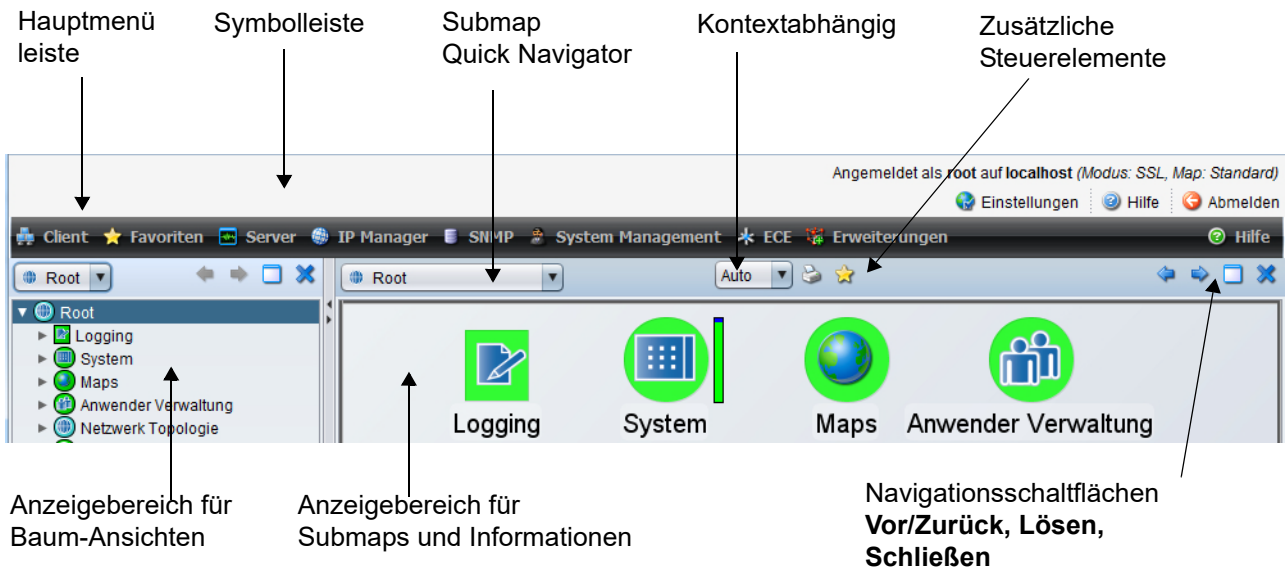


Bild 2 *Die Struktur der Client-Bedienoberfläche*

Bild 2 zeigt das Fenster des Clients. Das Fenster ist in vier Bereiche aufgeteilt. Im oberen Teil des Fensters befindet sich die Symbolleiste (mit dem Namen des aktuell angemeldeten Anwenders sowie der aktuell geöffneten Map auf der linken Seite). Darunter liegt die Hauptmenüleiste. Unter der Menüleiste werden die beiden Bereiche für die Baum-Ansicht und die Submap/Info-Ansicht angezeigt. In der oberen rechten Ecke beider Abschnitte befinden sich die Navigationsschaltflächen **Vor**, **Zurück**, **Lösen** und **Schließen**. Im Baum-Ansichtsbereich werden eine oder mehrere geöffnete Baum-Ansichten angezeigt. Im Submap/Info-Ansichtsbereich werden verschiedene Informationen angezeigt. Dazu zählen Submaps, Info-Browser, das Meldungsprotokoll usw. Wenn eine neue Submap geöffnet wird, erscheint sie im Submap/Info-Ansichtsbereich und wird zu den bereits im Submap/Info-Viewer geöffneten Karten hinzugefügt. Sie können die vorherige Karte aufrufen, indem Sie die Schaltfläche **Zurück** betätigen oder wechseln Sie über die Schaltfläche **Vor** zur nächsten Karte. Über die Schaltfläche **Lösen** können Sie Karten auch vom Kartennavigator lösen. Die gelöste Karte wird anschließend in einem separaten Fenster angezeigt. Der Quick Navigator des Submap/Info-Ansichtsbereichs führt eine Liste mit allen enthaltenen Karten, d. h. allen aktuell geöffneten Submaps, dem Ereignis-Browser und dem Meldungsprotokoll.

In den folgenden Abschnitten werden die Menükomponenten der Hauptmenüleiste und des Submap/Info-Ansichtsbereichs detailliert erklärt. Der Topologie-Viewer verwendet den Submap/Info-Ansichtsbereich zur Anzeige von Netzwerktopologien. Beim Topologie-Viewer handelt es sich um eine besonders wichtige Komponente von OpenScape FM. Daher widmen wir dem Topologie-Viewer zur Erklärung einen eigenen Abschnitt. Wie beim Submap/Info-Ansichtsbereich handelt es sich auch beim Baum-Ansichtsbereich um einen Karten-Viewer. Daher finden sich dort auch die gleichen Navigationsfunktionen. Allerdings stellt der Navigationsbaum eine recht komplexe Struktur dar und wird daher ausführlich in *Abschnitt 5.13, „Systemnavigation mit Hilfe des Navigationsbaums“* behandelt.

5.1 Symbolleiste

Auf der rechten Seite der Symbolleiste wird die aktuell geöffnete Map und der Name des aktuell angemeldeten Anwenders angezeigt.

Zusätzlich enthält die Symbolleiste Schaltflächen, um die graphische Darstellung auszuwählen, eine Übersicht über die Hilfen für alle Plugins zu öffnen und um den Client zu verlassen.

5.2 Hauptmenüleiste

Das Hauptmenü befindet sich im oberen Bereich der Bedienoberfläche. Je nach initialisierten Modulen kann das Menü zusätzliche Einträge enthalten. Der Aufbau hat die folgende Struktur:

- **Client:**

  Root Navigationsbaum: Öffnet eine Baumansicht beginnend mit dem Root-Objekt.

  Web: Öffnet den Web-Client (siehe OpenScape FM Web Bedienungsanleitung) in einem neuen Browser-Fenster.

  Neuer Client: Dies öffnet ein neues Browser-Fenster, das die Login-Seite des Clients anzeigt.

  Neue Map: Über diesen Befehl kann eine neue Map erstellt werden. Hierfür muss ein Map-Name spezifiziert werden. Wurde eine neue Map erstellt, wird ein neues Objekt mit dem gleichen Namen wie die neue Map in den **Maps**-Container auf der Root-Submap eingefügt.

  Maps Anzeigen: Öffnet eine Liste aller vorhandenen Maps, aus der eine zu öffnende oder zu löschende Map ausgewählt werden kann. In einer Map sind alle Ansichten (d. h. Submap und Bäume der Datenbankobjekte) zusammengefasst, *Abschnitt 3.5, „Maps“*. Um mit dem Desktop-Client arbeiten zu können, muss zunächst eine Map geöffnet werden. Die zuletzt bei der Abmeldung geöffnete Map wird standardmäßig wieder geöffnet, aber über diesen Menübefehl kann eine andere Map auswählt werden. Es kann jeweils nur eine Map geöffnet werden. Wird der Client zum ersten Mal gestartet und dabei keine Map erstellt, wird automatisch eine Standard-Map angelegt.

  Objektsuche...: Siehe *Kapitel 7, „Objekt- und Ereignis-Suche“*.

  Einstellungen: Dies öffnet ein Fenster, in dem einigen Einstellungen des Clients konfiguriert werden können:

  - Im Bereich **Aussehen** kann das allgemeine Erscheinungsbild des Clients aus einer Reihe von vordefinierten **Look & Feels** ausgewählt werden.

- Im Bereich **Einstellungen** definieren die ersten drei Auswahlmöglichkeiten, ob die entsprechenden Elemente (**Titel**, **Anmeldedaten**, **Toolbar**) im oberen Bereich des Client-Fensters angezeigt werden sollen.
  Ist **Submap-Pfad im Navigatinsbaum öffnen** ausgewählt, werden Objekte, deren Submap aktuell angezeigt wird, automatisch im Navigationsbaum ausgewählt.

  Die Einstellungen **Schließen minimiert in den System Tray** und **Alarmton für Überwachungsobjekt** konfigurieren das Verhalten der Überwachung durch das Tray Bar Symbol (siehe *Kapitel 9*).
  Konkret wird das Verhalten des Tray Bar Symbols bei Schließen des Clients und der Warnton bei Verschlechterung des Status des überwachten Objektes ausgewählt.

  Die Einstellung **Auto-Start Maximiert** bzw. **Auto-Start Deaktiviert** legt fest, ob bei der Anmeldung eines Anwenders in die Windows-Oberfläche automatisch ein OpenScape FM Client gestartet werden soll oder nicht.

Anmelden: Über diesen Befehl melden Sie sich am Server an.

Abmelden: Über diesen Menübefehl melden Sie sich ab, d. h. Ihre Sitzung wird geschlossen.

Passwort ändern: Über diesen Menüeintrag kann der momentan angemeldete Anwender das eigene Login-Passwort ändern.

Beenden: Rufen Sie diese Option auf, um sich vom Server abzumelden und die Bedienoberfläche zu verlassen.

- **Favoriten:**

  Submap: Ist eine Start-Submap definiert, können Sie diese über diesen Menübefehl aufrufen. (Wählen Sie zur Festlegung einer Start-Submap **Submap->Setzen Home** auf dem Hintergrund einer Submap.) Ist keine Start-Submap festgelegt, wird die Netzwerk Topologie Submap geöffnet.

  Netzwerk Topologie Navigationsbaum: Öffnet eine Baumansicht beginnend mit dem Netzwerk Topologie Objekt. Dieser Baum enthält alle Topologie-Objekte (siehe *Kapitel 16*) und ist in der initialen Sicht der einzige angezeigte Objektbaum.

  Netzwerk Topologie Submap: Öffnet die Submap des Netzwerk Topologie Objektes. Aus dieser Submap heraus können alle anderen Topologie-Submaps aufgerufen werden.

  Ereignisse.: Über diesen Befehl kann der Ereignis Browser geöffnet werden. Dies kann auch über den Quick-Navigator des Anzeigebereichs für Submaps und Info-Browser geschehen.

- **Server:**

  Administration:

  - **Server-Eigenschaften:** Dies öffnet ein Fenster mit Karteikarten, auf denen die Email-Voreinstellungen, die Verbindungsmethode für den Client und die Active Directory Einstellungen konfiguriert werden können. Außerdem werden allgemeine Informationen über den Server angezeigt. Mehr zu den einzelnen Konfigurationsmöglichkeiten findet sich in *Kapitel 6*.
  - **Anwenderverwaltung:** Dieser Eintrag zeigt den Anwenderverwaltungs-Baum im Baumfenster an. Mehr dazu findet sich in *Kapitel 14, „Anwender- und Gruppenverwaltung“*.
  - **Debug-Optionen...:** Über diesen Befehl kann ein Anwender mit Administrator Rechten die Debug- und Log-Mechanismen für Plugins konfigurieren, siehe *Abschnitt 23.2, „Log- und Debug-Konfiguration“.*

- **Domämen:** Über diesen Befehl können Sie sich eine Liste aller definierten Domänen anzeigen lassen, siehe *Abschnitt 15.8.4, „Schneller Überblick über alle Domänen“*.
- **Backup Manager:** Siehe *Kapitel 19, „Backup und Wiederherstellung“*
- **Startup Manager->Zeige Dienste:** Über diesen Befehl kann ein Anwender mit „Administrator“-Rechten alle Dienste einsehen, die über den Startup Manager gestartet wurden. Ferner können diese Dienste hier angehalten oder (neu) gestartet werden; siehe *Kapitel 21, „Startup Manager“*
- **Lizenz Manager:** Siehe *Anhang E, „Lizenzierung“*

Time Scheduler...: Mit Hilfe dieses Befehls können Zeitfilter erstellt und konfiguriert werden. Mehr über Zeitfilter findet sich in *Kapitel 20, „Zeitpläne“*.

Plugins: Über diesen Befehl kann ein Anwender mit „Administrator“-Rechten die vorhandenen Plugins initialisieren. Siehe *Anhang D, „Systemkonfiguration“*. Wenn alle Plugins initialisiert sind, ist diese Menüoption nicht mehr verfügbar.

- **Hilfe:**

Info über...: Dieser Befehl öffnet das „Info über“ Fenster. Dort werden Information über den installierten OpenScape FM Server, Copyright und Trademark angezeigt. Das „Info über“ Fenster kann auch über den Quick-Navigator des Ansichtsbereich für Submaps und Info-Browser aufgerufen werden.

Grundlagen: Öffnet die Online-Hilfe von OpenScape FM Desktop. Sind weitere OpenScape FM-Plugins aktiv, werden die entsprechenden Einträge angezeigt, über die die zugehörigen Online-Handbücher geöffnet werden können. *Kapitel 17, „Hilfefunktionen“*.

5.3 Objekte des Hauptmenüs

Auf der Root-Submap finden Sie zwei Objekte, die bestimmte Einträge des Hauptmenüs darstellen: **Maps** und **System**. In Kombination mit den Berechtigungen ermöglichen es diese Objekte einem Administrator, Anwenderkonten mit sehr spezifischen Einschränkungen einzurichten. So kann ein Anwender mit Administrator-Rechten beispielsweise einen anderen Anwender einrichten, für den das IP Manager-Hauptmenü nur einen Eintrag enthält. Detaillierte Informationen zu den Berechtigungen siehe *Kapitel 15, „Zugriffsrechte“*.

5.3.1 Maps

Das Symbol „Maps“ enthält alle vorhandenen Maps (detaillierte Informationen zu Maps enthält der *Abschnitt 3.5, „Maps“*). Über dieses Symbol können die folgenden auch im allgemeinen Objektmenü enthaltenen Funktionen aufgerufen werden:

- **Zeige Maps...** hat dieselbe Funktion wie der Eintrag **Client->Maps Anzeigen...** im Hauptmenü. Diese Option öffnet eine Liste aller vorhandenen Maps. Außerdem können Sie mit diesem Browser Maps öffnen und löschen.

- **Neue Map...** hat dieselbe Funktion wie die Option **Client->Neue Map...** im Hauptmenü. Diese Option öffnet ein Fenster, in dem Sie durch Spezifizierung eines Map-Namens eine neue Map erstellen können.

Standardmäßig enthält das „Maps“-Symbol mindestens die **Standard**-Map, die vom System erstellt wird. Wenn Sie eine weitere Map erstellen, wird ein neues Symbol, dass diese Map darstellt, unter dem **Maps**-Symbol eingeblendet. Die Kontextmenüs der Symbole auf der Submap des Symbols „Map“ enthalten zusätzlich zu den allgemeinen Objektmenüs noch folgende Optionen:

- **Map öffnen** öffnet diese Map. Dieser Menübefehl funktioniert exakt so, wie die Schaltfläche **Öffnen** in der **Map-Liste**.
- **Map löschen** löscht diese Map. Dieser Menübefehl funktioniert exakt so, wie die Schaltfläche **Löschen** in der **Map-Liste**.

5.3.2 System

Die **System**-Submap enthält die Symbole **Server**, **Plugins** und **Hilfe**.

- Neben den allgemeinen Objektmenüs (siehe *Abschnitt 5.6.1, „Objekt-Kontextmenüs“*) enthält das **Server**-Symbol dieselben Optionen wie das Menü **Server** in der Hauptmenüleiste. Eine Beschreibung dieser Funktionen finden Sie in *Abschnitt 5.1, „Symbolleiste“*. Unterhalb des Server-Symbols sehen Sie eine Reihe von Objekten für die von OpenScape FM Desktop unterstützten Funktionen: **Backup Manager**, **Startup Manager**, und **Lizenz Manager**. Je nach Funktion/Objekt sind weitere untergeordnete Objekte verfügbar. Sämtliche Objekte unterhalb der Server-Objekte übertragen ihre Menüpositionen bis an das Server-Hauptmenü. Weitere Informationen zu diesen Funktionen finden Sie in folgenden Kapiteln dieses Handbuchs:
  Lizenz Manager: siehe *Anhang E*.
  Backup Manager: siehe *Kapitel 19, „Backup und Wiederherstellung“*.
  Startup Manager: siehe *Kapitel 21, „Startup Manager“*.
- Das Symbol **Plugins** verfügt lediglich über die allgemeinen Objektmenüs. In der **Plugins**-Submap finden Sie Objekte, welche die initialisierten Plugins darstellen. Die Kontextmenüs der einzelnen Plugin-Objekte enthalten dieselben Positionen wie der zugehörige Plugin-Menüeintrag in der Hauptmenüleiste.
- Das Symbol **Hilfe** enthält für jede verfügbare Hilfekategorie ein untergeordnetes Objekt, und ein Info Symbol für „Info über“ (das Objekt für „Info über“ lautet **Info**). Im Kontextmenü des Hilfe Symbols ist jeweils ein Eintrag enthalten, über den die zugehörige Hilfe geöffnet werden kann. Zusätzlich enthält es den Menüeintrag **Info über** mit dem das „Info über“ Fenster geöffnet werden kann. Die untergeordneten Hilfe-Objekte haben denselben Namen wie das Plugin, zu dem sie gehören. Über den Menüeintrag **Hilfe** öffnet sich nur die Hilfe des zugehörigen Plugins. Das Info Symbol bietet den Menü-Punkt **Info über** und öffnet sich das „Info über“ Fenster.

5.4 Anzeigebereich für Submaps und Informationen

Der Submap/Info-Ansichtsbereich ist immer sichtbar. In diesem Bereich befinden sich sechs Elemente: Quick Navigator, die Steuerelemente **Zoom-Wähler** und **Drucken** sowie die Schaltflächen **Vor**, **Zurück**, **Lösen** und **Schließen**, die alle in diesem Abschnitt beschrieben werden (siehe *Bild 2*).

Die Elemente des Navigationsbaums werden in einem separaten Abschnitt behandelt, *Abschnitt 5.13, „Systemnavigation mit Hilfe des Navigationsbaums“*.

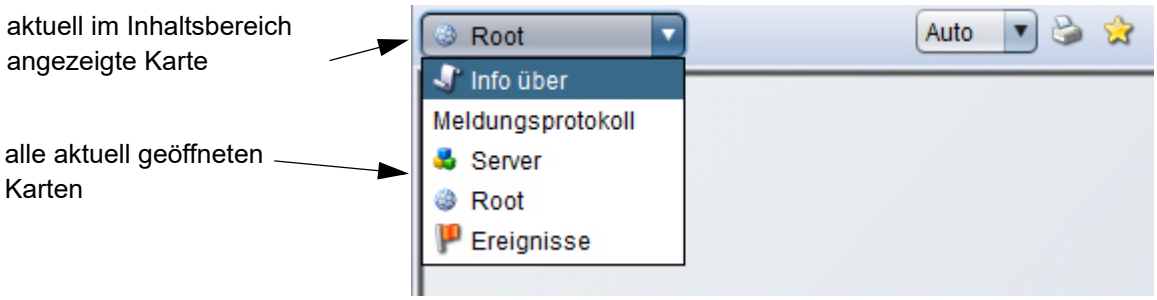


Bild 3 *Der Quick Navigator des Submap/Info-Ansichtsbereichs*

Quick Navigator (*Bild 3*):
Der OpenScape FM Desktop-Server führt auch eine Liste aller aktuell geöffneten Karten (d. h. Submaps und andere Infofelder). Einträge von gelösten Karten werden in Klammern aufgeführt Der Zugriff auf die Submap-Liste erfolgt über den Quick Navigator im linken oberen Fensterbereich. Die hier gewählte Submap wird umgehend geöffnet. Wenn Sie eine gelöste Karte auswählen, wird diese in den Vordergrund gestellt. Wenn eine Submap geschlossen wird, erscheint der Eintrag nicht länger in der Liste des Quick Navigators. Einige Karten wie das Meldungsprotokoll und der Ereignis-Browser lassen sich jedoch nicht schließen und stehen daher immer über das Pull-Down-Menü des Quick Navigators zur Verfügung.

Schaltflächen Vor/Zurück :
Die Schaltfläche **Zurück** öffnet die vorherige Karte aus der Liste der geöffneten Karten. Die Schaltfläche **Vor** wechselt zu der Submap, die vor dem Aufruf von **Zurück** angezeigt wurde.

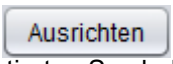
Schaltfläche Lösen :
Der Client zeigt standardmäßig alle Karten im Submap/Info-Ansichtsbereich seines Hauptfensters an. Soll eine Submap bzw. ein Info-Browser in einem separaten Fenster angezeigt werden, können Sie über die Schaltfläche **Lösen** ein neues Fenster öffnen, in dem die aktuelle Karte angezeigt wird. Außerdem können Sie in dem auf Symbolgröße verkleinerten (minimierten) Kartenfenster einen Kartentitel und/oder ein Symbol zuweisen. Siehe hierzu *Abschnitt 5.5, „Submap-Symbole und -Titel“*.

Schaltfläche Schließen :
Über diese Schaltfläche können Sie die aktuelle Submap bzw. den Daten-Browser schließen. Die Elemente im Inhaltsbereich werden geschlossen und stehen nicht mehr über den Quick Navigator zur Verfügung.

Die folgenden beiden Komponenten befinden sich in dem kontextabhängigen Bereich für zusätzliche Steuerelemente. Sie erscheinen nur auf Submaps (**Zoom** und **Drucken**) bzw. auf Info-Browsern.

Zoom-Wähler (nur bei Submaps) Auto :
Mit dem Zoom-Regler können Sie die Anzeigegröße der Symbole/Netzwerke im Topologie-Viewer festlegen. Hierfür stehen Zoom-Faktoren zwischen 25 und 200 Prozent zur Verfügung (in 25-%-Schritten). Wenn Sie hier **Auto** wählen, wird die Netzwerkansicht automatisch an die jeweilige Fenstergröße angepasst.
Bei Deaktivierung von „Auto-Zoom“ können Sie eine Submap manuell vergrößern bzw. verkleinern, indem Sie die Submap-Ränder mit der linken oder rechten Maustaste entsprechend verschieben. Links: Alle Symbole behalten ihre relative Position (gegenüber dem Hintergrund) bei. Rechts: Alle Symbole behalten ihre tatsächliche Position bei.

Schalter Am Raster Einrasten (nur bei Submaps) 
Ist dieser Schalter aktiviert, können Symbole bei manueller Verschiebung nur auf Rasterpunkte positioniert werden. Wird ein Symbol bei aktivierten Schalter manuell verschoben, springt das Symbol nach der Positionierung automatisch auf den nächstgelegenen Rasterpunkt.

Schaltfläche Ausrichten (nur bei Submaps) 

Diese Schaltfläche dient dazu, die aktuell selektierten Symbole der Submap untereinander auszurichten. Bei Auswahl der Schaltfläche öffnet sich ein Auswahlmenü mit den verschiedenen Ausrichtungsmöglichkeiten, wobei die Ausrichtung stets auf Basis des umschreibenden Rechteckes um alle selektierten Symbole erfolgt.
Die Symbole können an eine der Kanten des Rechteckes verschoben werden, oder sie können entlang der X- bzw. Y-Achse gleichmäßig verteilt werden.

Schaltfläche Bildschirmfoto 
Diese Schaltfläche kopiert den Anzeigebereich der aktuell angezeigten Submap in die Zwischenablage.

Schaltfläche Neu Laden 
Diese Schaltfläche aktualisiert den Inhalt der aktuell angezeigen Darstellung. So werden z.B. die Daten für eine dargestellte Tabelle neu ermittelt.

Schaltfläche **Drucken** (nur bei Submaps und Info-Browsern)  :
Bei manchen Karten befindet sich die Schaltfläche **Drucken** zwischen dem Quick Navigator und den Schaltflächen **Vor**/**Zurück**. Über diese Schaltfläche können Sie den Anzeigebereich der aktuell angezeigten Submap ausdrucken. siehe *Abschnitt 10.1, „Drucken aus einer Submap heraus“*.

Schaltfläche **Alles Auswählen** (nur im Info Browser verfügbar): 
Die Auswahl dieser Schaltfläche selektiert alle im Info Browser angezeigten Zeilen. Anschließend kann eine Aktion für alle diese Zeilen ausgeführt werden. Alternativ kann STRG-A betätigt werden um alle Zeilen zu selektieren. Einige Browser unterstützen keine Mehrfachselektion. In diesem Fall steht die Alles Auswählen Schaltfläche nicht zu Verfügung.

Schaltfläche **Kopieren** (nur im Info Browser verfügbar): 
Das Betätigen dieser Schaltfläche kopiert den Inhalt aller selektierten Zeilen in die Zwischenablage. Dies kann ebenfalls durch das Betätigen der Tastenkombination STRG-C erreicht werden. Um zusätzlich die Überschriften des Info Browsers zu kopieren muss bei Betätigung der Schaltfläche gleichzeitig die Umschalttaste gedrückt sein. Dies kann auch durch die Tastenkombination STRG-UMSCHALTEN-C erreicht werden. Das Kopieren aller Zeilen ohne zu selektieren kann durch drücken von ALT-C durchgeführt werden. Die Textwerte der ausgewählten Zeilen werden durch Tabulatoren getrennt. Die einzelnen Zeilen durch den systemabhängigen Zeilenseparator.

Schaltfläche **Hilfe** (nur im Info Browser verfügbar): 
Diese Schaltfläche öffnet die kontextsensitive Hilfe für den geöffneten Info Browser (siehe dazu auch *Kapitel 17, „Hilfefunktionen“*).

Schaltfläche **Favoriten**: 
Diese Schaltfläche fügt die aktuelle Sicht in die Liste der Favoriten ein. (siehe dazu auch *Abschnitt 5.15, „Favoriten“*). Je nach Konfiguration der Startsicht des Anwenders (siehe *Abschnitt 14.1.1*) werden die Favoriten dem Anwender oder seiner Startsicht-Gruppe zugewiesen.

5.5 Submap-Symbole und -Titel

Vom Quick Navigator verwaltete Karten können gelöst und in einem separaten Fenster angezeigt werden (siehe *Abschnitt 5.4*, **Schaltfläche Lösen**).

Im Allgemeinen erscheint als Titel einer gelösten Karte die standardmäßige Symbolbezeichner des Objektes. Wird die gelöste Karte minimiert, wird standardmäßig das OpenScape FM Logo als ihr Symbol angezeigt.

Für Karten, die Submaps und Bäume darstellen, kann ein individueller Kartentitel und ein individuelles Kartensymbol festgelegt werden, die angezeigt werden, wenn die betreffende Karte gelöst ist. Der Kartentitel wird dabei dem übergeordneten Objekt einer Submap oder dem Root-Objekt eines Navigationsbaums zugewiesen.

Symbol und Kartentitel werden mit Hilfe der Bedienoberfläche für die Kartenanzeige definiert. Um ein Symbol und/oder einen Kartentitel für ein Objekt zu definieren, kann aus dem Kontextmenü des Objektes der Eintrag **Eigenschaften** ausgewählt und die Seite **Symbol->Kartendarstellung** ausgewählt werden.

Die Seite enthält die Bedienoberfläche für die Kartenanzeige.

Links in diesem Fenster befindet sich eine Liste mit allen Symbolen, die bereits geladen wurden. Soll eines dieser Symbole für das aktuelle Objekt benutzt werden, muss dieses ausgewählt und **OK** angeklickt werden.

Soll der Liste ein weiteres Symbol hinzugefügt werden, kann dies mit Hilfe der Schaltfläche **Icon laden** geschehen. In diesem Fall öffnet sich ein Datei-Browser in dem das gewünschte Symbol gesucht und ausgewählt werden kann. Unterstützt werden derzeit die Formate gif, jpg und xpm. Die ausgewählte Bilddatei wird in die Liste der Kartensymbole eingefügt und kann dort, wie zuvor beschrieben. ausgewählt und zugewiesen werden.

Durch Anklicken der Schaltfläche **Zurücksetzen** werden die Einstellungen gelöscht. Eine Symboldatei kann aus dem OpenScape FM entfernt werden, indem ihr Name in der Liste ausgewählt und dann die Schaltfläche **Icon löschen** angeklickt wird.

Im rechten Bereich des Fensters kann die **Kartenüberschrift** für die gelöste Karte festgelegt werden.

Außerdem kann hier bestimmt werden, ob die Konfiguration nur für die aktuelle Map (**Map-spezifisch**) oder für **Alle Maps** gelten soll.

Das gewählte Icon für eine Submap und die Kartenüberschrift werden angezeigt, wenn die entsprechende Submap gelöst wird (Schaltfläche rechts/oben) und sie anschließend minimiert wird.

5.6 Kontextmenüs

5.6.1 Objekt-Kontextmenüs

Wenn Sie mit der rechten Maustaste auf ein Symbol oder eine Submap klicken, wird das zugehörige Kontextmenü geöffnet. Welchen Inhalt ein Kontextmenü hat, hängt somit davon ab, für welches Symbol bzw. welche Submap Sie dieses Menü aktiviert haben. Die Kontextmenüs für Symbole und Submaps enthalten eine Reihe von gemeinsamen Einträgen, andere Optionen sind wiederum symbolspezifisch. Im oberen Teil des Menüs befinden sich die allgemeinen Einträge. Der untere Teil enthält objektspezifische Einträge.
Darüber hinaus beeinflussen die Zugriffsrechte des Anwenders und der aktuelle Kontext den Inhalt von

Kontextmenüs. Wenn der Anwender nicht über die erforderlichen Rechte für bestimmte Funktionen verfügt, werden die dazugehörigen Einträge nicht im Menü angezeigt.
Da jedes Objekt eine Vielzahl von Funktionen bietet, werden alle Objekt-Kontextmenüs in eigenen Abschnitten beschrieben.

Im Folgenden werden die allgemein verfügbaren Objekt-Menüpositionen beschrieben:

- **Ereignisse:**

  Bestätigen...: Bestätigt alle Ereignisse dieses Objekts, wenn Ereignisse für dieses Objekt existieren. Hat das Objekt einen Gesamtstatus, werden auch die Ereignisse seiner untergeordneten Objekte bestätigt. Siehe auch *Abschnitt 5.9, „Der Ereignis-Browser“*. Detaillierte Informationen zum Gesamtstatus finden Sie in *Kapitel 13, „Symbole und Statusanzeige“.*
  Hinweis:
  Wird ein Ereignis bestätigt, das auch anderen Objekten zugewiesen ist, wirkt sich die Bestätigung auch auf diese Objekte aus.

  Anzeigen...: Öffnet den Ereignis-Browser mit den objektspezifischen Einträgen. Diese Menüposition ist verfügbar, wenn Ereignisse für dieses Objekt existieren.
  Wenn das Objekt einen Gesamtstatus hat, wird diese Menüposition angezeigt, auch wenn das Objekt keine Ereignisse hat. In diesem Fall erhalten Sie nach Auswahl dieser Menüposition auch objektspezifische Ereigniseinträge der untergeordneten Objekte. Detaillierte Informationen zum Gesamtstatus finden Sie in *Kapitel 13, „Symbole und Statusanzeige“*.
  Um erneut alle Ereignisse im Ereignis-Browser einzusehen, sollten Sie die Ereignis-Kategorie „Alle Ereignisse“ wählen.

- **Öffnen:**

  Objekt Suchen: öffnet das Dialogfenster „Objektsuche“, in dem nach bestimmten Objekten gesucht werden kann, die sich unterhalb der Hierarchie des aktuellen Objektes befinden. Nähere Informationen bietet das *Kapitel 7, „Objekt- und Ereignis-Suche“*.

  Baum: Richtet das ausgewählte Objekt als Root in einem neuen Baum ein und zeigt diesen im Baum-Ansichtsbereich an.

  Submap: Öffnet die Submap eines Objekts. Sie können wahlweise diese Option aufrufen oder auf dem Objekt doppelklicken.

  Baumpfad: Öffnet die Baumansicht und selektiert das aktuelle Objekt in dieser (nicht im Baum-Ansichtsbereich verfügbar).

- **Bearbeiten:**

  Verstecken: versteckt das aktuelle Symbol (siehe *Abschnitt 12.1, „Versteckte Objekte“*).

  Zeige Versteckte Objekte: setzt alle auf der Submap enthaltenen versteckten Symbole auf sichtbar (siehe *Abschnitt 12.1, „Versteckte Objekte“*).

  Kopieren: Bereitet dieses Objekt für das Kopieren vor, siehe *Kapitel 12, „Erstellen individueller Ansichten“*.

  Ausschneiden: Bereitet dieses Objekt für das Verschieben vor.

  Einfügen: Wurde ein Objekt für das Kopieren vorbereitet, wird es, falls möglich, in die Submap des aktuellen Objektes kopiert. Wurde ein Objekt für das Verschieben vorbereitet, wird versucht es in die Submap des aktuellen Objektes zu verschieben. Beachten Sie, dass es nicht möglich ist, ein Objekt manuell auf durch

Applikationen eingerichtete Submaps einzufügen. Siehe auch *Kapitel 12, „Erstellen individueller Ansichten“*.

Verknüpfen: Stellt eine Verbindung zwischen zwei Symbolen her. Siehe hierzu *Abschnitt 5.11.1, „Anwenderdefinierte Verbindungen“*.

Zielsystem angeben: Definiert das Ziel für die bestehende Verbindung [nur verfügbar, wenn bereits eine Verbindung hergestellt worden ist]. Siehe hierzu auch *Abschnitt 5.11.1, „Anwenderdefinierte Verbindungen“*.

Verbindung abbrechen: Trennt eine zuvor hergestellte Verbindung [nur verfügbar, wenn eine Verbindung besteht]. Siehe hierzu auch *Abschnitt 5.11.1, „Anwenderdefinierte Verbindungen“*.

Objekt Löschen...: Löscht dieses Objekt und alle Symbole, welche dieses Objekt repräsentieren. Ereignisse, die dem Objekt zugewiesen wurden, bleiben jedoch erhalten.

Symbol Entfernen: Entfernt das einzelne Symbol.

Verwalten/Nicht verwalten: verwaltet das Objekt bzw. hebt die Verwaltung auf. Wenn für ein Objekt die Verwaltung aufgehoben wurde, werden alle Technology-Typ-spezifischen Menübefehle deaktiviert. Außerdem werden für dieses Objekt keine IP-Polls mehr durchgeführt, d.h. es werden keine Status- und Konfigurationsänderungen mehr angezeigt. Ereignisse werden ignoriert. In einigen Fällen werden auch die Kind-Objekte gelöscht, die zusätzliche Funktionalitäten anbieten. Sobald das Objekt wieder verwaltet wird sind die Technology-Typ-spezifischen Menü-Punkte und Objekte wieder erreichbar und die IP-Polls werden wieder ausgeführt. Wenn für einen IP-Knoten die Verwaltung aufgehoben wird bzw. dieser verwaltet wird, wird auch die Verwaltung für alle Kind-Objekte dieses IP-Knotens aufgehoben bzw. verwaltet.

- **Neu:** Dieses Menü enthält Einträge für die unterschiedlichen Objekttypen, die auf der Submap des aktuellen Objektes angelegt werden können. Die Auswahl eines Eintrages erzeugt ein entsprechendes Objekt manuell.
- **Konfigurieren:** Die öffnet ein Fenster, in dem das Objekt konfiguriert werden kann. Der Inhalt des Fensters ist abhängig vom Objekttyp und den erkannten Objekteigenschaften.
- **Eigenschaften:** Öffnet ein Fenster mit u.A. den folgenden Karteikarten:

  Domänen: Hier kann ein Objekt einer Mandantendomäne zugewiesen werden. Näheres hierzu siehe *Abschnitt 15.8, „Domänen“*.

  Symbol->Symbol Eigenschaften: Öffnet das Dialogfenster „Eigenschaften bearbeiten“, in dem das Erscheinungsbild des Symbols und der Map-spezifische Beschriftung geändert werden kann. Hier kann beispielsweise eine neue Form zugeordnet werden. Siehe auch *Kapitel 13, „Symbole und Statusanzeige“*.

  Symbol->Kartendarstellung: Öffnet das Dialogfenster „Card Display“, in dem ein Symbol und/oder ein Titel für ein Objekt ausgewählt werden kann. Siehe hierzu *Abschnitt 5.5, „Submap-Symbole und -Titel“*.

  Kommentare: Als Administrator oder Operator kann hier ein Kommentar dem Objekt hinzugefügt werden (siehe *Abschnitt 5.16, „Objekt-Kommentare“*).

  Info: Öffnet den „Info-Browser“, wo allgemeine Objekteigenschaften angezeigt werden. Weitere Informationen zu Browser-Funktionen finden sich in *Abschnitt 5.7, „Standard-Info-Browser“*.

- **Statuserlärung:** Begründet den aktuellen Status des Objektes (siehe *Abschnitt 5.17, „Statuserklärung“*).

5.6.2 Kontextmenü für Submaps

Das Kontextmenü einer Submap entspricht dem Kontextmenü des Objektes zu dem die Submap gehört. Die einzelnen Funktionen verhalten sich dabei so, als würden sie für das entsprechende Objekt ausgeführt.

Eine Ausnahme sind die Funktionen **Objekt Löschen** und **Symbol Entfernen**. Diese können nicht aus dem Kontextmenü der Submap ausgeführt werden, sondern nur aus dem Kontextmenü des Objekts selbst.

Zusätzlich werden eine Reihe von Submap spezifischen Funktionen angeboten. Diese sind im Einzelen:

- **Nach oben:** Öffnet die übergeordnete Submap, von der aus diese Submap geöffnet wurde.
- **Nach unten:** Öffnet die untergeordnete Submap, von der aus diese Submap geöffnet wurde.
- **Submap:**

  Neu-Ausrichten: Richtet die Symbole auf der Submap so aus, dass sie nicht überlappen.

  Layout: In diesem Menü kann ausgewählt werden, wie verbundene Objekte automatisch zueinander angeordnet werden sollen. Auf nicht verbundene Objekte hat die Auswahl keinen Einfluss.

  Setzen Home: Definiert diese Submap als Home-Submap. Über den Favoriten **Submap** kann direkt zu dieser Submap navigiert werden.

  Eigenschaften: Öffnet die Bedienoberfläche für Submap-Eigenschaften. Hier kann ein Standard-Hintergrundbild für alle Submaps und ein Hintergrundbild für diese Submap auswählt werden. Siehe hierzu auch *Abschnitt 5.8, „Hintergrundbild wählen“*.

  Überwachungsobjekt zuweisen: Setzt die aktuelle Submap als Überwachungsobjekt für das Tray Bar Symbol des aktuellen Benutzers. Nähere Informationen zum Tray Bar Symbol bietet das *Kapitel 9, „Anzeige von Tray Bar Symbolen“*.

5.7 Standard-Info-Browser

Wenn Sie ein Objekt-Kontextmenü öffnen und **Eigenschaften** wählen, wird auf der Seite **Info** ein Browser-Fenster mit grundlegenden Informationen über das Objekt geöffnet. Dies ist jedoch nur eine von vielen Gelegenheiten, bei denen diese Info-Browser zum Einsatz kommen. Sie bieten einige Funktionen, welche die Arbeit mit dem OpenScape FM Desktop und seine Plugins erleichtern.

Durch Klicken auf den entsprechenden Spaltentitel kann der Inhalt des Browsers sortiert werden. Um die Standard-Sortierung zurück zu erhalten, klicken Sie den entsprechenden Spaltentitel während Sie die „Strg“-Taste drücken.

Wenn im Browser mehr als eine Spalte angezeigt wird, können Sie die Spalten der Tabelle/des Browsers durch Ziehen des Titels (und der dazugehörigen Spalte) mit der Maus nach Ihren Wünschen anordnen. OpenScape FM sichert diese Konfiguration als anwenderspezifische Daten. Haben Sie also die Spalten in einer bestimmten Anordnung sortiert, werden diese bei der nächsten Verwendung dieses Browsers wieder genau so angezeigt.

Wenn eine Spalte zu schmal ist, um den kompletten Inhalt anzuzeigen, können Sie auf den entsprechenden Spaltentitel klicken während sie die „Umschalt“-Taste gedrückt halten: Die Spalte wird dann auf die ideale Spaltenbreite gesetzt, so dass der komplette Titel und alle Informationen angezeigt werden.

Um die ideale Spaltenbreite für alle Spalten in einem Schritt zu setzen, markieren Sie eine Zeile in der Tabelle und drücken Sie gleichzeitig „Strg“ und „d“.

Plugins wie HiPath 4000 oder HiPath 3000/5000 verwenden eine Vielzahl von Info-Browsern, um alle relevanten Informationen zu den verwalteten Komponenten anzuzeigen. An vielen Stellen finden Sie die Schaltfläche **Stopp**, über die Sie die aktuelle Anfrage abbrechen können, und die Schaltfläche **Aktualisieren**, um eine neue Anfrage zu initiieren und die aktuellsten Daten anzuzeigen.

Oberhalb der Liste befindet sich die Schaltfläche **Kopieren**, wird diese betätigt, wird der Inhalt der in der Liste ausgewählten Zeilen in die Zwischenablage kopiert.

Wird die daneben befindliche Schaltfläche **Tabelle drucken/speichern** betätigt, öffnet sich ein Fenster um alle aktuell im Info-Browser befindlichen Daten zu exportieren. **Drucken** überträgt die Daten an einen Drucker, **Speichern** exportiert die Daten in Form von Komma-separierten-Werten (csv-Format) in eine Datei.

Die folgende Tabelle enthält eine Auflistung der vorhandenen Tasten-Funktionen. Für die Auslösung muss der Eingabe-Fokus auf einer der Zeilen im Info-Browser liegen.

Belegte Taste	Funktion
F1	Online Hilfe starten
F3	vorwärts suchen (nachdem ein Suchstring definiert wurde)
Shift + F3	rückwärts suchen (nachdem ein Suchstring definiert wurde)
F4 oder ALT + F4	Browser schließen
F5	Inhalt aktualisieren
CTRL + D	Optimale Spaltenbreite anzeigen
CTRL + E	Alles löschen
CRTL + F	Suche definieren
CTRL + L	Layout auf maximale Breite stellen
CTRL + klicken	Default Anzeigereihenfolge wiederherstellen
X	Ausschneiden
Y	Kopieren

Tabelle 1 Tastenfunktionen im Info-Browser

5.8 Hintergrundbild wählen

Für jede Submap in der OpenScape FM Umgebung kann ein anderes Submap-Hintergrundbild konfiguriert werden. Dieses Bild wird jedesmal wenn die Submap geöffnet wird als Hintergrundbild angezeigt.

Zusätzlich kann ein einzelnes Standard-Hintergrundbild für eine Map ausgewählt werden. Dieses Standard-Hintergrundbild, wird für alle Submaps dieser Map angezeigt, für die kein spezifisches Submap-Hintergrundbild konfiguriert worden ist

Wichtige Information:
Die Zuweisung von spezifischen oder Standard-Hintergrundbildern gilt nur für die aktive Map. Dadurch ist es möglich verschiedene Hintergrundbilder für dieselbe Submap in verschiedenen Maps zu definieren, (siehe *Abschnitt 3.5*).

Die Hintergrundbilder können verwendet werden um weitere Informationen zu einer Submap hinzuzufügen. So kann beispielsweise eine Landkarte oder der Grundriss einer Fabrik verwendet werden. Die Objekte können dann so angeordnet werden wie sie in Realität auch stehen. Oder einfach ein Bild von einem schönen Sonnenuntergang um Ihre Management-Plattform aufzulockern.

Beides, die Konfiguration eines Hintergrundbildes und die Konfiguration eines Standard-Hintergrundes erfolgen über das „Submap-Hintergrund-Fenster“. Um das Fenster zu öffnen, kann aus dem Kontextmenü der Submap der Menüpunkt **Submap->Hintergrund** ausgewählt werden.

Das „Submap-Hintergrund-Fenster“ enthält folgende Elemente:

- Die **Hintergrund Bild** Liste ist die Liste der Hintergrundbilder, die von einem Anwender hochgeladen worden sind. Nur diese Bilder können als Hintergrundbilder benutzt werden. Wenn der „Submap-Hintergrundbild-Manager“ initial geöffnet wird, wird in der Liste das Submap-Hintergrundbild ausgewählt, welches für die aktive Submap definiert worden ist.
- Die **Bild laden...** Schaltfläche kann betätigt werden, um ein Hintergrundbild zur Liste hinzuzufügen. Wenn diese Schaltfläche gedrückt wird, öffnet sich ein Dateisystem-Browser-Fenster, in dem ein Bild ausgewählt werden kann. Wenn das Dateisystem-Browser-Fenster über das OK Auswahlfeld geschlossen wird, wird das aktuell selektierte Bild zur Liste hinzugefügt. Zur Zeit werden die Bildformate GIF und JPEG unterstützt. Wenn ein anderes Bildformat oder ein Nicht-Bildformat ausgewählt wird, erscheint eine Fehlermeldung.
- Das **Bereich** Auswahlmenü kann benutzt werden, um einen Anwendungsbereich für die nächste „OK“ oder „Leeren“ Aktion, wie unten beschrieben, festzulegen. Beim Öffnen des „Submap-Hintergrund-Manager“ Fensters ist der Bereich auf „Submap“ gesetzt.
  - Wenn der Bereich auf **Submap** gesetzt ist, wird das für die aktive Submap aktuell zugewiesene Bild in der „Hintergrund Bild“ Liste selektiert. Die nächste „OK“ oder „Leeren“ Aktion wirkt sich nur auf die aktive Submap aus.
  - Wenn der Bereich auf **Global** gesetzt ist, wird das aktuell definierte Standard-Hintergrundbild in der „Hintergrund Bild“ Liste selektiert. Die nächste „OK“ oder „Leeren“ Aktion wirkt sich nur auf das Standard-Hintergrundbild aus.
- Wenn die **Speichern** Schaltfläche ausgewählt wird, werden, abhängig vom aktuellen Bereich, folgende Aktionen durchgeführt:
  - Wenn der Bereich auf **Submap** gesetzt ist, wird das aktuell in der „Hintergrund Bild“ Liste selektierte Bild als spezifisches Hintergrundbild für die aktive Submap gesetzt. Das selektierte Bild wird angezeigt.
  - Wenn der Bereich auf **Global** gesetzt ist, wird das aktuell in der „Hintergrund Bild“ Liste selektierte Bild als Standard-Hintergrundbild gesetzt. Es wird auf allen Submaps angezeigt, denen kein spezifisches Hintergrundbild zugewiesen worden ist.

In beiden Fällen wird das „Submap-Hintergrund-Manager“ Fenster geschlossen.

- Wenn die **Zurücksetzen** Schaltfläche betätigt wird, werden, abhängig vom ausgewählten Bereich, folgende Aktionen durchgeführt:
  - Falls der Bereich auf **Submap** gesetzt wird, ist kein Bild mehr als spezifisches Hintergrundbild für die aktive Submap definiert. Wenn ein Standard-Hintergrundbild definiert ist, wird dieses angezeigt. Falls kein Standard-Hintergrundbild definiert ist, wird kein Hintergrundbild für die aktive Submap angezeigt.
  - Falls der Bereich auf **Global** gesetzt wird, wird kein Bild mehr als Standard-Hintergrundbild zugewiesen. Für Submaps, welche kein spezifisches Hintergrundbild zugewiesen wurde, wird kein Hintergrundbild angezeigt.

  In beiden Fällen wird das „Submap-Hintergrund-Manager“ Fenster geschlossen.
- Durch das Betätigen der Schaltfläche **Löschen** wird, wenn diese betätigt wird, das aktuell in der Hintergrund Bild Liste ausgewählte Bild aus der Liste gelöscht. Das gelöschte Bild wird nicht mehr als spezifisches oder Standard-Hintergrundbild angezeigt. Abgesehen von dem Löschen aus der Liste, bewirkt das Löschen eines Bildes dasselbe, wie das Betätigen der „Leeren“ Schaltfläche für beide Bereiche.
- Die **Abbrechen** Schaltfläche schließt das „Submap-Hintergrund-Manager“ Fenster und keine Aktion wird ausgeführt. Bereits geladenen oder gelöschte Bilder bleiben weiterhin geladen bzw. gelöscht.

5.9 Der Ereignis-Browser

Der Ereignis-Browser ist das zentrale Werkzeug im OpenScape FM, um Ereignisse anzuzeigen.

Wird der OpenScape FM geöffnet, so befindet sich der Ereignis-Browser im Anzeigebereich. Dieser zeigt alle Ereignisse an, für die der aktuelle Anwender Zugriffsrechte besitzt. Durch die Auswahl des Hauptmenüeintrages **Favoriten->Ereignisse** kann zu einem späteren Zeitpunkt diese Anzeige erneut aktiviert werden.

Der wesentliche Teil des Ereignis-Browsers besteht aus einer Tabelle, in der jede Zeile ein Ereignis repräsentiert. Die Farbe des Kreises innerhalb der Spalte **Status** in der jeweiligen Zeile zeigt dabei den Status an, der dem Ereignis zugewiesen ist.

Ein Doppelklick auf eine Zeile, die ein Ereignis repräsentiert, das einem Objekt zugeordnet ist, öffnet die Submap auf der sich das Objekt befindet. Ist kein Objekt zugeordnet, öffnet sich eine Ansicht, welche Informationen bezüglich des aktuellen Ereignisses bereitstellt. Diese Information kann alternativ für alle Ereignisse über den Menüeintrag **Ereignis->Ereignisdaten** aus dem Kontextmenü eines Ereignisses angezeigt werden.

Hinweis:
Ältere Versionen des OpenScape FM repräsentieren den Status über eine vollständige Einfärbung der einzelnen Zeilen. Dieses alte Verhalten kann global wiederhergestellt werden, indem die Zeile
`server.colored.events=true`
der Datei
`<OSFM-installationsverzeichnis>/startup/conf/OpenScapeFM.properties`
hinzugefügt wird.

Die verschiedenen Spalten zeigen die Information an, ob das Ereignis **Bestätigt** wurde, ob es **In Arbeit** genommen wurde, ob eine **Annotation** für das Ereignis existiert, den **Status** der dem Ereignis zugewiesen wurde (angezeigt in der entsprechenden Farbe), das **Datum** zu dem das Ereignis empfangen wurde, den **Ursprung** und die **Kategorie** des Ereignisses, und eine Kurz**Beschreibung** des Ereignisses. Die beiden letzten Spalten zeigen die Anzahl der bereits existierenden Ereignisse an, die mit dem Ereignis in Bezug stehen (**Korrelierte Ereignisse**), und die Anzahl der Ereignisse gleichen Typs (**Typ-Zähler**).

Durch Anklicken der Spalten-Überschriften kann der Inhalt der Tabelle entsprechend der angeklickten Spalte aufsteigend bzw. absteigend sortiert werden. Diese Sortierung wird für den Anwender abgespeichert und bei der nächsten Anmeldung automatisch verwendet.

Wurde einem Ereignis eine **Annotation** hinzugefügt, wird in der entsprechenden Spalte eine Sprechblase angezeigt. Der Tooltipp für diese Spalte zeigt dann den Inhalt der Annotation an, und der Tooltipp der Spalte **Bestätigt** den Zeitpunkt, an dem die Annotation zuletzt geändert wurde.

Ereignisse sind zu einem Ereignis korreliert, wenn sie als Kindereignis eingetragen wurden. Diese Ereignisse verwenden intern den gleichen Ereignisschlüssel für ein Objekt (z.B. verschiedene Statusereignisse für das gleiche Objekt). Die zu einem Ereignis korrelierten Ereignisse können über den Eintrag **Ereignis->Korrelierte Ereignisse** aus dem Kontextmenü des Ereignisses angezeigt werden.

Ob für ein bestimmtes Ereignis korrelierte Ereignisse existieren, oder ob es bestätigt ist, kann über das in der Spalte **Bestätigt** angezeigte Symbol identifiziert werden. Für individuelle Ereignisse ist dies ein einzelner **grüner Haken** (für bestätigte Ereignisse), oder ein einzelnes **rotes Quadrat** (für unbestätigte Ereignisse). Existieren korrelierte Ereignisse, verändern sich die Symbole entsprechend in **zwei grüne Haken**, oder **zwei rote Quadrate**.

Ereignisse sind gleichen Typs, wenn sie für das gleiche Objekt die gleiche Reaktion ausgelöst haben (z.B. zwei Major Alarm On Ereignisse für das gleiche Objekt). Die zu einem Ereignis typgleichen Ereignisse können über den Eintrag **Ereignis->Ereignisse gleichen Typs** aus dem Kontextmenü des Ereignisses angezeigt werden.

Die Schaltflächen unterhalb der Tabelle können dazu verwendet werden, um die aktuell ausgewählten Ereignisse zu **Bestätigen**, zu **Unbestätigen**, **In Arbeit** zu nehmen, **Nicht in Arbeit** zu nehmen, zu **Annotieren** oder zu **Löschen**, falls der aktuelle Anwender dazu die Rechte besitzt.

Da es eine Vielzahl von Ereignissen geben kann, können Filter aktiviert werden, um die Anzahl der angezeigten Ereignisse auf eine gewünschte Teilmenge zu beschränken.

Die oberhalb der Tabelle auswählbaren Seiten können verwendet werden, um eine Suche innerhalb der angezeigten Ereignisse durchzuführen. Jede Eingabe reduziert die Menge der angezeigten Ereignisse auf nur die, für die **alle** Eingaben auf **allen** Seiten zutreffen. Vier Seiten sind standardmäßig verfügbar. Durch das aktivieren von Plugins können weitere Seiten mit Plugin-spezifischen Suchkriterien hinzukommen.

Die Seite **Eigenschaften** erlaubt eine Suche nach dem **Bestätigt** Status, dem **In Arbeit** Attribut, der Ereignis-**Kategorie** (das Menü enthält nur die Kategorien, für die auch ein Ereignis vorliegt), der **Beschreibung** und des **Ursprungs** des Ereignisses. Einträge in den letzten beiden Feldern reduzieren die Suche auf Teilstring-Treffer in den entsprechenden Spalten.

Erfolgt eine Eingabe auf der Seite **Volltext**, so wird eine Teilstring-Suche in den Spalten **Beschreibung**, **Kategorie** und **Ursprung** durchgeführt. Eine dieser Suchen muss für die noch angezeigten Ereignisse zutreffen.

Die Seite **Status** kann verwendet werden, um die Suche auf ausgewählte Status-Werte einzugrenzen.

Auf der Seite **Zeit/Wartung** kann die Suche auf Ereignisse beschränkt werden, die in einem bestimmten Zeitrahmen eingetroffen sind. Es kann ein minimales Datum (**Start-Datum**), ein maximales Datum (**End-Datum**), ein **Zeitplan** und ein **Wartungs-Status** ausgewählt werden.

Um das einzelne Aufzählen korrelierter Ereignisse zu vermeiden, ist der Haken **Korreliert** auf der Seite **Eigenschaften** standardmäßig gesetzt. In diesem Fall wird nur das jeweils letzte der korrelierten Ereignisse angezeigt. Der Haken kann entfernt werden, um alle Ereignisse zu sehen. Die Voreinstellung kann jedoch nicht geändert werden. Wird ein neuer Ereignis-Browser geöffnet, ist der Haken wieder gesetzt.

Um die korrelierten Ereignisse für ein einzelnes Ereignis zu sehen, kann der Eintrag **Ereignis->Korrelierte Ereignisse** im Kontextmenü des Ereignisses gewählt werden. Dies öffnet einen neuen Ereignis-Browser, der die korrelierten Ereignisse anzeigt.

Werden Ereignisse in der Korreliert-Sicht **bestätigt**, werden alle korrelierten Ereignisse bestätigt. Werden sie **unbestätigt**, so wird nur das aktuellste korrelierte Ereignis auf nicht bestätigt gesetzt.

Schließlich kann die Menge der angezeigten Ereignisse auf nur die Ereignisse eingeschränkt werden, die sich auf Objekte beziehen, die sich im Unterbaum eines ausgewählten Objektes befinden. Dies kann z.B. verwendet werden, um nur die Ereignisse anzuzeigen, die sich auf Knoten eines bestimmten Netzwerkes beziehen. Dazu kann der Ereignis-Browser mit dem Menüeintrag **Ereignisse->Anzeigen** aus dem Kontext-Menü des Wurzel-Objektes des gewünschten Unterbaumes aufgerufen werden.

5.9.1 Ereignis-Übersicht

Ein schneller Gesamtüberblick über die aktuell nicht bestätigten Ereignisse erfolgt über die Anzeige im rechten unteren Eck des OpenScape FM Client (siehe *Bild 4*). Diese Anzeige ermöglicht es auf den ersten Blick zu erkennen, ob neue Ereignisse eingetroffen sind, und wie gravierend diese sind.

Bild 4 *Übersicht der unbestätigen Ereignisse*

Die Zahlen hinter den einzelnen Farbpunkten zeigen an, wieviele nicht bestätigte und nicht korrelierte Ereignisse der entsprechenden Priorität für den aktuellen Anwender im Ereignisbrowser zur Zeit angezeigt werden (im Beispeil 1 critical, 2 minor und 12 normal Ereignisse).

Durch das Anklicken einer der Farbpunkte wird eine Liste geöffnet, die alle unbestätigten Ereignisse der entsprechenden Priorität enthält.

5.9.2 Kommentare zu Ereignissen

Bei der Arbeit an den aktuell erkannten Problemen ist es oft hilfreich, wenn Sie für sich und Ihre Kollegen den Ereignissen Kommentare hinzufügen können. Verwenden Sie dazu den Kommentar-Browser. Zusätzlich kann der Kommentar-Browser dazu verwendet werden, um einen Überblick über die Bestätigungen und Unbestätigungen des betroffenen Ereignisses zu erhalten. Wählen Sie aus dem Kontextmenü des Ereignisses den Eintrag **Ereignis->Annotieren**, um den Kommentar-Browser (*Bild 5*) zu öffnen.

Der untere Teil des Browsers dient dazu, Kommentartexte zu erzeugen oder zu modifizieren.

Geben Sie den Text für Ihren Kommentar ein und klicken Sie auf **OK**. Der Kommentar wird registriert und in dem Textfeld unten im Kommentar-Browser angezeigt. Die Hintergrundfarbe der zugehörigen Bestätigungsschaltfläche im Ereignis-Browser wechselt zu Weiß, um anzuzeigen, dass für dieses Ereignis ein Kommentar vorliegt.

Um den Ereigniskommentar zu ändern, öffnen Sie den Kommentar-Browser erneut, geben Sie den neuen Text ein und klicken Sie auf **OK**. Der neue Text wird nun als Kommentar gespeichert.

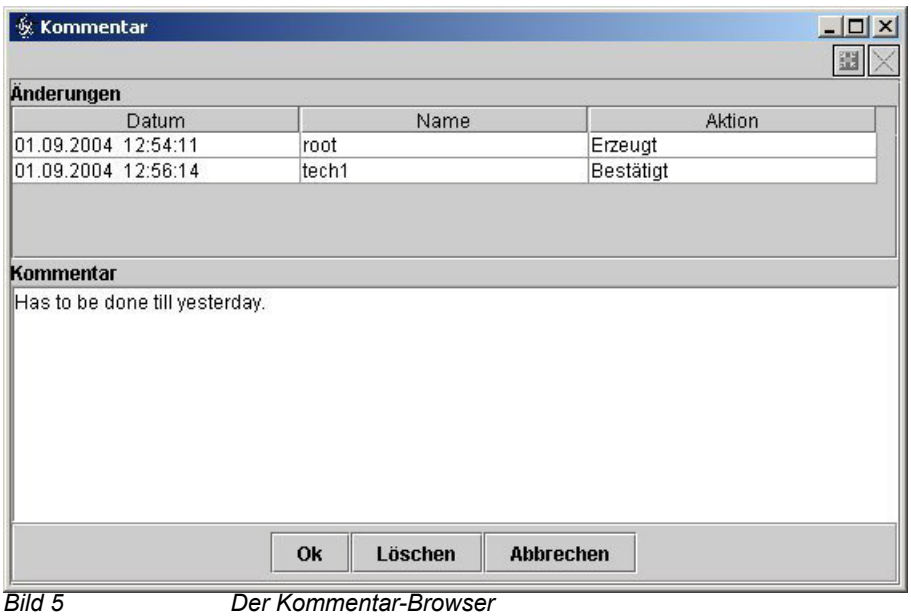


Bild 5 Der Kommentar-Browser

Um einen Kommentar zu löschen, klicken Sie auf **Löschen**. Die Hintergrundfarbe der zugehörigen Bestätigungsschaltfläche wird auf die Standardfarbe zurückgesetzt.

Der obere Teil des Browsers wird verwendet, um über alle Veränderungen des dem Ereignis zugeordneten Kommentars buchzuführen. Jede Veränderung führt zu einem Eintrag in der Änderungsliste. Jeder Eintrag besteht dabei aus drei Werten: der Zeitpunkt, zu dem die Veränderung stattfand, der Name des Anwenders, der die Veränderung ausgelöst hat, und aus dem Typ der Veränderung.

Veränderungstypen können z.B. die Erzeugung, Löschung oder Modifikation des Kommentars sein. Aber auch durch den Anwender ausgelöste Bestätigungen oder Unbestätigungen sind Veränderungstypen, die in die Liste des entsprechenden Ereignisses aufgenommen werden.

5.9.3 Rechte im Ereignis-Browser

Wie bei allen anderen Ansichten (Submap/Baum) unterliegt der Zugriff auf die im „Ereignis-Browser“ angezeigten Ereignisse den Rechten, die der einzelne Anwender hat. Für die Objekte, für die ein Anwender nur User- oder überhaupt keine Rechte hat, darf er die Ereignisse nicht einsehen. Ein Anwender ist befugt, Ereignisse einzusehen und Kommentare zu den Ereignissen abzugeben/zu ändern/zu löschen, die Objekte betreffen, für die er Operator-Rechte besitzt. Für die Objekte, für die er Administrator-Rechte besitzt, darf er sämtliche Funktionen des Ereignis-Browsers verwenden. Es können auch Ereignisse angezeigt werden, für die der Anwender unterschiedliche Rechte hat. So kann er beispielsweise befugt sein, die Ereignisse von Objekt „A“ zu löschen, nicht jedoch die Ereignisse von Objekt „B“.

5.10 Meldungsprotokoll

Im Meldungsprotokoll (*Bild 6*) werden alle Systemmeldungen aufgelistet, die sich auf den laufenden Client beziehen. Über den Eintrag **Meldungsprotokoll** des Quick Navigators im Submap/Info-Ansichtsbereich können Sie das Protokoll öffnen. Das Meldungsprotokoll zeigt in zwei Spalten die Tragweite und die Meldung selbst. Die erste Zeile des Meldungsprotokolls zeigt an, wo die Client-Protokolldatei vom Client gespeichert wurde.

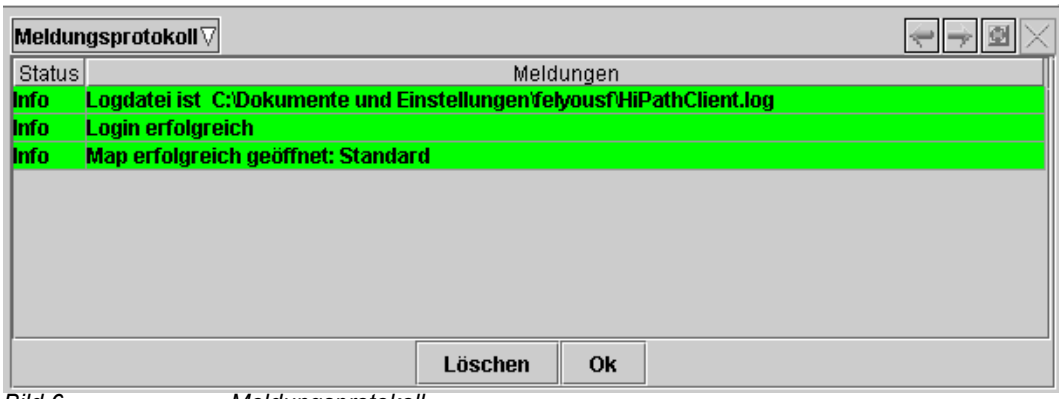


Bild 6 *Meldungsprotokoll*

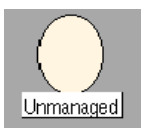
Bei Warnhinweisen am Client wird das Meldungsprotokoll automatisch geöffnet und die Warnmeldung wird gelb dargestellt.
Informationszeilen sind grün und bei Fehlern werden die Listeneinträge rot angezeigt.

Sie können die Meldungen einfach annehmen und das Meldungsprotokoll über die Schaltfläche **OK** schließen oder leeren Sie das Meldungsprotokoll über die Schaltfläche **Löschen**.

5.11 Topologien im Submap/Info-Ansichtsbereich

Über den Topologie-Viewer werden im Submap/Info-Ansichtsbereich Submaps mit Netzwerktopologien angezeigt. Dazu zählen Netzwerke, Teilnetzwerke und Geräte UND die Verbindungen zwischen Netzwerken und Geräten. Jedes Objekt der Netzwerktopologie wird als Symbol angezeigt. Das Erscheinungsbild eines Symbols hängt vom dargestellten Knotentyp sowie dem aktuellen Knotenstatus ab. Der Knotenstatus wird durch eine bestimmte Anzeigefarbe signalisiert.

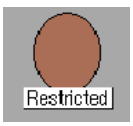
Es gibt elf verschiedene Zustände:



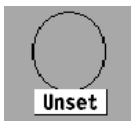
Nicht verwaltet→ hellbraun
Dieses Objekt ist zwar noch in der Datenbank registriert, wird jedoch nicht mehr überwacht.

Test → lachsrot
Die Statusangabe "Test" besagt, dass für das Objekt vorübergehende Diagnose- oder Wartungsmaßnahmen durchgeführt werden.

Deaktiviert → dunkelbraun
Der Status "Deaktiviert" gibt an, dass das Objekt inaktiv ist (obwohl es möglicherweise ordnungsgemäß funktioniert).



Eingeschränkt → (braun)
Die Statusangabe "Eingeschränkt" bedeutet, dass ein Objekt zwar normal funktioniert, jedoch möglicherweise nicht für alle Anwender verfügbar ist.



Nicht definiert → grau
Für dieses Objekt wurde kein Status vergeben.

Normal → grün
Das betreffende Objekt befindet sich im normalen Betriebszustand.

Hinweis → hellblau
An dem Objekt steht möglicherweise ein Problem bevor.

Geringfügig → gelb
An dem Objekt liegt ein geringfügiges Problem vor; dies sollte sich jedoch nicht auf die normale Nutzung des Objekts auswirken.

Schwerwiegend → orange
An dem Objekt bestehen ernsthafte Probleme; diese Probleme wirken sich gegebenenfalls auch negativ auf die normale Nutzung des Objekts aus.

Kritisch → rot
An dem Objekt liegt ein ernsthaftes Problem vor, so dass das Objekt nicht mehr ordnungsgemäß oder gar nicht mehr arbeitet.

	Unbekannt → blau Der Status eines Objekts ist nicht feststellbar.

Tabelle 2 Status von Objekten

Bei Eingang bestimmter Alarme beginnen die Symbole der zugehörigen Objekte zu blinken, um den Administrator von dem neuen Ereignis in Kenntnis zu setzen. Objekte können einen zusammengesetzten Status aufweisen, der die Zustände aller dem Objekt untergeordneten Objekte widerspiegelt (Status-Propagierung). Das Symbol eines solchen Objektes beginnt auch zu blinken, wenn ein Alarm für eines der untergeordneten Objekte ausgelöst wurde. Sind alle Ereignisse für dieses Objekt einschließlich aller untergeordneten Objekte bestätigt (über den Ereignis-Browser oder das Kontextmenü des Objekts), hört das Objektsymbol auf zu blinken. So wird deutlich, dass blinkende Objektsymbole Ereignisse anzeigen, die einen Eingriff erfordern.

Die angezeigten Symbole können mit der linken Maustaste ausgewählt und innerhalb der Submap verschoben werden. Sie können mehrere Symbole gleichzeitig auswählen, indem Sie sie bei gedrückt gehaltener Hochstelltaste der Reihe nach anklicken.

Der Topologie-Viewer zeigt alle Verbindungen zwischen den einzelnen Netzknoten an.

5.11.1 Anwenderdefinierte Verbindungen

Es kann vorkommen, dass Netzwerkobjekte keine Verbindungsinformationen über das Zielsystem liefern können. Über „Anwenderdefinierte Verbindungen“ können Sie solche bestehenden Verbindungen in die entsprechende Submap einbinden.
Wählen Sie ein Objekt und anschließend **Bearbeiten->Verknüpfen** aus dem Kontextmenü. Dieses Objekt wird dann als Quelle markiert. Wählen Sie das Ziel und anschließend **Bearbeiten->Zielsystem angeben** aus dem Kontextmenü und geben Sie das gewünschte Kennzeichen für die Verbindung ein. Klicken Sie dann auf **Herstellen**. Die neue Verbindung wird sofort angezeigt.

Wenn sich beide ausgewählten Objekte in der gleichen Ansicht befinden (d. h. Submap oder Liste), wird die Verbindung zwischen den beiden Objekten hergestellt. Wenn sich die beiden Objekte auf verschiedenen Submaps befinden, werden Sie gefragt, ob Sie die Verbindung auf der Ursprungs-Map (*Bild 7*) herstellen möchten und ob die Verbindung auf der Ziel-Submap hergestellt werden soll. Auf der von Ihnen gewählten Submap zeigt das Referenzsymbol die andere Seite der Verbindung an.

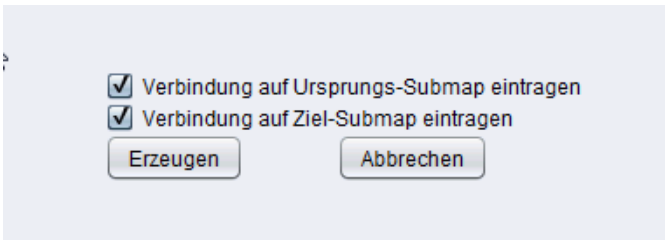


Bild 7 Menü für eine submap-übergreifende anwenderdefinierte Verbindung

Auf diese Weise können Sie logische Verknüpfungen zwischen Netzwerken, Teilnetzwerken oder Systemen und anderen Geräten herstellen (d. h. Verbindungssymbole erstellen).
Um eine anwenderspezifische Verbindung zu löschen, wählen Sie **Bearbeiten->Objekt Löschen** aus dem entsprechenden Kontextmenü.

Wir werden jetzt unsere Arbeit mit verschiedenen Maps und Submaps beginnen. Hierfür müssen dem System jedoch bekannte IP-Geräte vorliegen. Informationen zur Erfassung von IP-Geräten in Ihrem verwalteten Netzwerk finden Sie in der *IP Manager Plugin Bedienungsanleitung*.

5.12 Topologie-Navigation

Wie bereits zuvor in diesem Kapitel erwähnt, wird jede verwaltete Ressource als Objekt dargestellt. Diese Objekte werden in verschiedenen Ansichten (d. h. Submaps und Bäume) als ein oder mehrere Symbole grafisch dargestellt. Ein System wird beispielsweise intern als Einzelobjekt dargestellt; in unterschiedlichen Submaps und Bäume kann dieses System jedoch durch viele verschiedene Symbole angezeigt werden (*Bild 8*, siehe *Abschnitt 3.2, „Symbole“* und *Abschnitt 3.4, „Ansichten“*).

Sie können nie direkt auf die Objekte zugreifen. Der Zugriff erfolgt vielmehr über Symbole, d. h. die grafische Darstellung dieser Objekte. Ein Symbol ist eindeutig an ein einzelnes Objekt gekoppelt (aber auch hier gilt, dass ein Objekt mit mehreren Symbolen verknüpft sein kann). Wird nachfolgend der Begriff „Objekt“ verwendet, bezieht sich dieser auf ein Symbol, das in der grafischen Bedienoberfläche des Clients angezeigt wird.

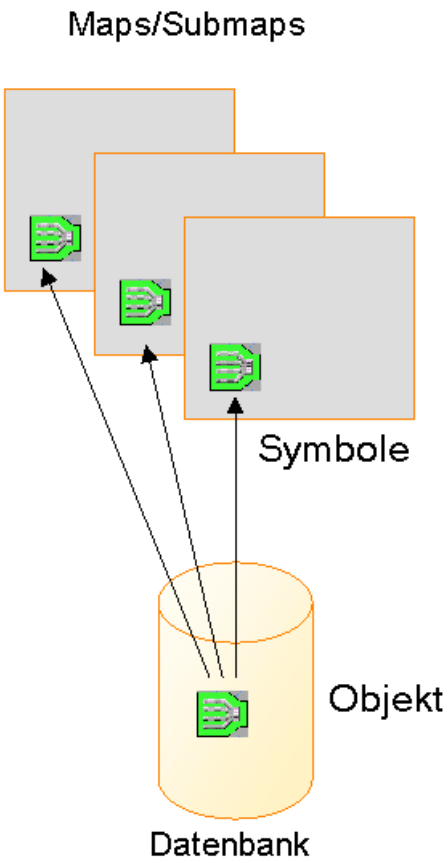


Bild 8 Darstellung von Objekten in Maps

Ein Objekt kann mit einer Ansicht verknüpft sein. Die Ansicht enthält alle zugehörigen Ressourcen des jeweiligen Objekts. Um von einem Objekt zur zugehörigen Submap zu gelangen, klicken Sie zweimal mit linken Maustaste auf das Symbol oder wählen Sie **Öffnen->Submap** aus dem Kontextmenü des Objekts. Im Submap/Info-Ansichtsbereich wird eine neue Karte geöffnet, die die Submap darstellt. Anschließend können Sie sich durch Doppelklicken auf die einzelnen Symbole oder über die jeweiligen Kontextmenüs in der Submap-Hierarchie nach unten bewegen. Um wieder nach oben zu gelangen, verwenden Sie den Menübefehl **Aufwärts** aus dem Kontextmenü der Submap. Um den zugehörigen Unterabschnitt auf einer neuen Karte im Anzeigebereich für Bäume anzuzeigen, wählen Sie **Öffnen->Baum**; *Abschnitt 5.13, „Systemnavigation mit Hilfe des Navigationsbaums“*.

Die Hierarchie der Submap spiegelt selbstverständlich die Objekthierarchie in der Datenbank wieder. *Bild 9* zeigt ein Beispiel für eine Hierarchie mit drei Submaps. Die oberste Ebene bildet die „Root-Submap“. Diese Submap enthält ein Symbol für das Anwenderverwaltungsobjekt. Die Submap des „Anwender Verwaltung“ Objekts enthält die Symbole für die Rechte-Verwaltung, die Gruppen-Verwaltung und die Anwender-Verwaltung (siehe zweites Fenster). Wie im dritten Fenster gezeigt, zeigt das Anwender Verwaltung Objekt alle Anwender-Objekte.

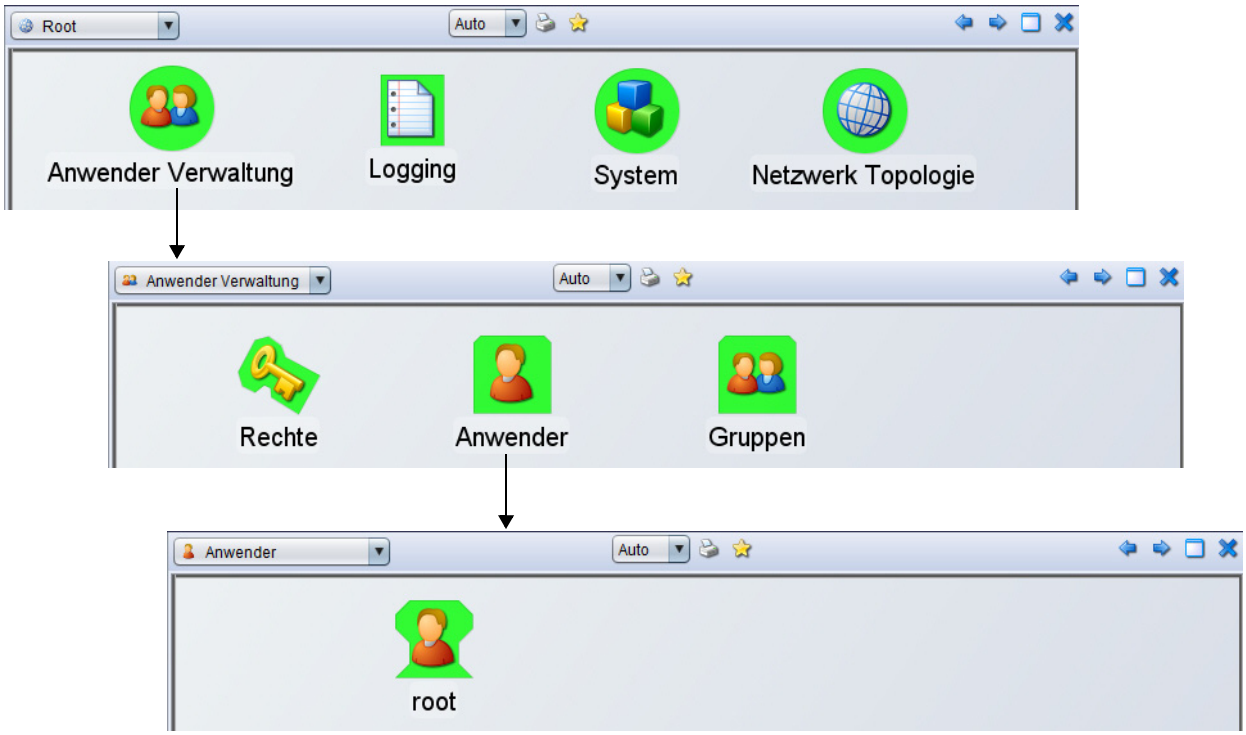


Bild 9 *Submap-Hierarchie: Anwender Verwaltung*

5.13 Systemnavigation mit Hilfe des Navigationsbaums

In sehr komplexen Netzen kann man bei der Arbeit mit vielen Submaps leicht den Überblick verlieren. Es besteht die Gefahr, dass die Beziehung zwischen den einzelnen Submaps nicht mehr klar ist. Der Navigationsbaum (*Bild 10*) hilft Ihnen in diesem Fall, sich zurecht zu finden. Der Navigationsbaum befindet sich im linken Abschnitt des Hauptfensters, dem Baum-Ansichtsbereich. Jedes Objekt wird durch ein bestimmtes Symbol dargestellt und bildet einen Unterabschnitt des Baums mit den untergeordneten Objekten als Zweige. Sie kennen dieses Prinzip möglicherweise bereits von anderen gängigen Dateiverwaltungssystemen (wie dem Windows Explorer). Symboltyp und Kennzeichen sind außerdem abhängig vom Ort. Wenn Sie die Form und/oder das Bitmap eines Objektsymbols an einem Ort verändert haben, gilt diese Erscheinung nur an diesem bestimmten Ort in der Hierarchie. An Orten, an denen die Erscheinung nicht verändert wurde, wird das Objektsymbol mit der ursprünglichen Form und dem Original-Bitmap dargestellt. Die Steuerelemente für die Baum-Ansicht (*Bild 10*) umfassen die aus dem Submap/Info-Ansichtsbereich bekannten Elemente **Quick Navigator** sowie die Schaltflächen **Vor**, **Zurück**, **Lösen** und **Schließen**. Für die Navigation im Baum-Ansichtsbereich gelten die gleichen Prinzipien wie im Anzeigebereich: Sie können sich in allen geöffneten Bäumen bewegen (Schaltflächen **Vor** und **Zurück**) und Sie können Bäume lösen (Schaltfläche **Lösen**), um sie in einem separaten Fenster anzeigen zu lassen. Sie können neue Bäume in neuen Karten öffnen, die anschließend über den **Quick Navigator** verfügbar sind, wobei die Namen der gelösten Baum-Karten in Klammern ausgeführt sind.

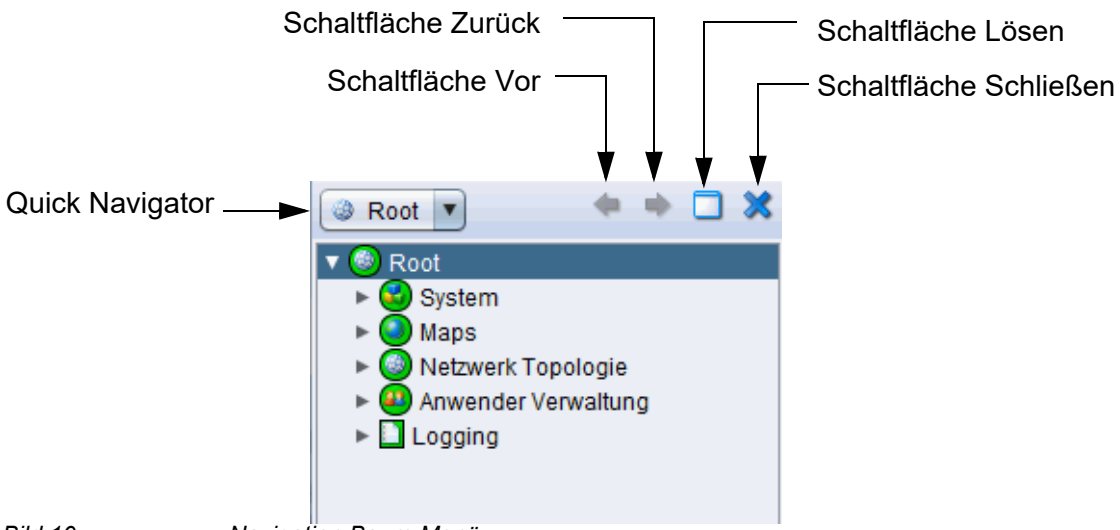


Bild 10 *Navigation Baum-Menü*

Sie können alle Unterzweige eines Symbols (d. h. alle untergeordneten Objekte) mit einem Doppelklick aufrufen und einsehen. Mit Ausnahme der Root-Submap kann jedes Objekt außerdem über einen speziellen Umschalter am Abzweigungspunkt eines Unterzweiges geöffnet bzw. geschlossen werden.

Ein horizontaler Umschalter (*Bild 11*) zeigt an, dass die Abzweigung geschlossen ist. Sie können die Abzweigung durch einen einfachen Mausklick auf den Umschalter öffnen; dieser wechselt dann in die vertikale Position. Existieren in dem Objekt weitere untergeordnete Objekte, werden diese als Unterzweige angezeigt.

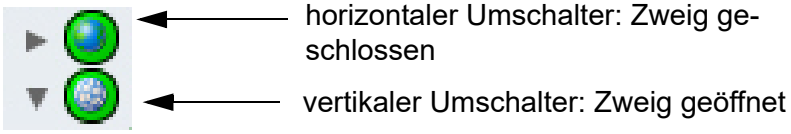


Bild 11 *Umschalter im Navigationsbaum*

Ein Zweig kann durch ein Doppelklick auf das entsprechende Symbol oder durch einen einfachen Klick auf den Umschalter vor dem Symbol geöffnet werden.

Wenn Sie eine Submap im Submap/Info-Ansichtsbereich anzeigen/öffnen möchten, sollten Sie hierfür das Kontextmenü des Objektsymbols im Navigationsbaum verwenden: wählen Sie **Öffnen->Submap**. Sie können auch ein bestimmtes Objekt/einen bestimmten Unterabschnitt anzeigen lassen. Verwenden Sie dazu das zugehörige Kontextmenü und wählen Sie **Öffnen->Baum**. Das ausgewählte Objekt dient dann als Root des neuen Baums. So können Sie alle anderen Objekte von Ihrem Unterabschnitt ausschließen. Des Weiteren erscheint der Name des neuen Unterabschnitts als Eintrag im Quick Navigator, so dass Sie zwischen allen geöffneten Bäumen hin- und herschalten können. Der aktuell angezeigte Baum wird selektiert dargestellt..

Wird ein Objekt im Navigationsbaum geöffnet, in dessen Unterabschnitt das Objekt selbst enthalten ist, d. h. es innerhalb der Abfolge der Baum-Objekte zu einer Rekursion kommt, wird das Symbol des bereits geöffneten Objekts mit einem „R“ (Rekursion) vor seinem Kennzeichen markiert. Es ist nicht möglich, dieses Objekt nochmals zu öffnen, d. h., den Baum an diesem Punkt zu öffnen.

Wie Sie wahrscheinlich bemerkt haben, bieten die Symbole im Anzeigebereich für Baum-Ansichten die gleichen Funktionen über die Kontextmenüs an wie die Symbole der Submaps im Anzeigebereich für Submaps und Informationen. Sie können also die Darstellung Ihres Netzwerks entweder mit Hilfe des Navigationsbaums oder der Submaps analysieren und konfigurieren.

5.14 Drag & Drop

Wie aus vielen Betriebssystemen bekannt, wird Drag & Drop unterstützt, um Objekte innerhalb der Oberfläche zu verschieben oder zu kopieren.

Um ein Objekt zu kopieren, muss die Strg-Taste gedrückt sein während das Objekt positioniert wird.

Dies kann sowohl im Baum wie auch im Submap-Bereich durchgeführt werden. So kann z.B. ein Objekt in eine Submap kopiert werden, indem die Submap geöffnet wird, das Objekt im Baum selektiert wird, und es auf die Submap gezogen wird, während die Strg-Taste gedrückt ist.

Ob Objekte verschoben oder kopiert werden dürfen, richtet sich nach dem Kontext.

5.15 Favoriten

Einige Submaps, Bäume oder Ereignis-Browser-Suchen werden häufig verwendet. Um einen schnellen Zugriff auf diese zu ermöglichen, können Submaps oder konfigurierte Suchen unter dem Hauptmenü **Favoriten** abgelegt werden.

Sie werden generiert und gespeichert, indem im Bereich für Zusätzliche Steuerelemente die Schaltfläche  betätigt wird, und ein Name für den Favoriten ausgewählt wird. Dies fügt dem Menü **Favoriten** einen Eintrag mit dem gewählten Namen hinzu.

Drei Einträge sind immer vorhanden:

- **Submap:** Dies navigiert zur Home-Submap.
- **Navigationsbaum:** Dies navigiert zum Home-Baum.
- **Ereignisse:** Dies öffnet den Ereignisbrowser.

Favoriten können gelöscht werden, indem das entsprechende Objekt innerhalb der Anwenderverwaltung auf der Submap **Favoriten** gelöscht wird. Die drei voreingestellten Einträge können nicht gelöscht werden.

Ein Submap- oder Baum-Favorit kann rekonfiguriert werden, indem ein Objekt auf das entsprechende Favoriten-Symbol gezogen wird. Die Submap des gezogenen Objektes wird dann für den verwendeten Favoriten benutzt. Dies kann auch für die voreingestellten Favoriten *Submap* und *Navigationsbaum* durchgeführt werden.

Innerhalb der Submap-Sicht kann die Submap eines Objektes oder die Submap selbst zur Home-Submap gemacht werden, indem aus dem Kontextmenü eines Objektes oder der Submap der Eintrag **Submap->Start-Submap setzen** ausgewählt wird.

Die Favoriten werden entweder individuell dem aktuellen Anwender oder einer ihm zugewiesenen Startsicht-Gruppe (siehe *Abschnitt 14.1.1*) zugeordnet.

5.15.1 Autostart

Während Favoriten einen schnellen Zugriff auf häufig benötigte Sichten erlauben, ermöglicht es die Autostart-Funktion Sichten festzulegen, die beim Starten eines Clients automatisch angelegt werden.

Die Definition von Autostart-Sichten ist an die Definition von Favoriten angelehnt. Alle Favoriten, die in der Anwenderverwaltung in die Submap **Autostart** kopiert werden, werden beim Start eines Clients automatisch geöffnet. Dies geschieht in der Reihenfolge, in der sie im Navigationsbaum angezeigt werden.

Die Reihenfolge im Baum kann durch Selektion und Verwendung der Tastenkombination Shift + Pfeil nach oben/ unten angepasst werden.

Für Anwender deren Startsicht (siehe *Abschnitt 14.1.1*) und deren Autostart mit einer Gruppe verbunden wurde, erfolgt die Definition über die entsprechende Gruppe.

5.15.2 Toolbar-Favoriten

Ausgewählte Favoriten können in die Toolbarleiste (oberhalb der Hauptmenüleiste) aufgenommen werden, um einen direkten Zugriff zu ermöglichen.

Die Definition von Toolbar-Favoriten ist an die Definition von Favoriten angelehnt. Alle Favoriten, die in der Anwenderverwaltung in die Submap **Toolbar** kopiert werden, werden in der Toolbar angezeigt.

Für Anwender deren Startsicht (siehe *Abschnitt 14.1.1*) und deren Toolbar mit einer Gruppe verbunden wurde, erfolgt die Definition über die entsprechende Gruppe.

5.16 Objekt-Kommentare

Den Objekten im OpenScape FM können individuelle Kommentare zugewiesen werden.

Diese werden an allen Symbolen, die das entsprechende Objekt repräsentieren, als Tooltipp angezeigt.

Kommentare können eingerichtet bzw. modifiziert werden, indem aus dem Kontextmenü eines Symbols des gewünschten Objektes der Eintrag **Eigenschaften** ausgewählt wird. Die Konfiguration erfolgt dann auf dem Reiter **Kommentare**.

5.17 Statuserklärung

Warum ein Objekt seinen aktuellen Status besitzt kann über den Menüeintrag **Statuserklärung** aus dem Kontextmenü des entsprechenden Objektes angezeigt werden.

Das sich öffnende Fenster enthalt die Begründung bzw. die Berechnungsgrundlage für den aktuellen Status (siehe dazu auch *Abschnitt 13.3*).

Wird der Status durch andere Objekte (zusammengesetzter Status) und zugehörige Ereignisse hervorgerufen, enthält das Fenster zusätzlich eine Liste der Objekte und Ereignisse, die den aktuellen Status ausgelöst haben.

In der Regel handelt es sich bei den anderen relevanten Objekten um Sub-Komponenten des aktuellen Objektes oder um Objekte, die vom aktuellen Objekt überwacht werden. Handelt es sich um IP-Knoten und sind diese nicht erreichbar, so werden auch die IP-Knoten-Ereignis-Objekte dieser Knoten als relevant betrachtet.

Relevante Ereignisse in diesem Zusammenhang sind alle Ereignisse der relevanten Objekte, deren Status nicht ‚*Normal*' ist.

6 Server-Konfiguration

Dieses Kapitel beschreibt die grundlegenden Funktionen, um den OpenScape FM Server zu konfigurieren.

Diese Funktionen werden aus der Hauptmenüleiste des Clients über den Eintrag **Server->Administration->Server-Eigenschaften** aufgerufen. Dieser öffnet das Konfigurationsfenster, das die verschiedenen Konfigurationsmöglichkeiten auf den in den folgenden Abschnitten beschriebenen Seiten anbietet.

6.1 Mail-Konfiguration

Auf der Seite **Mail-Konfiguration** kann die Vorbindung zum Mail-Server festgelegt werden, über welchen das OpenScape FM seine Mail-Nachrichten versendet, die z.B. von der Event Correlation Engine oder dem Reporting versendet werden.

Es kann das zu verwendende Mail **Protokoll**, der **Server** und der gewünschte **Port** angegeben werden.

Außerdem kann unter **Default Absenderadresse** eine Mail-Adresse angegeben werden, die immer dann als Versender benutzt wird, wenn für den Einzelfall kein gesonderter Absender angegeben wurde.

Über die Felder **Postfach/Benutzer** und **Passwort** wird der Account und dessen Autorisierung angegeben, über den das OpenScape FM seine Mails versenden soll.

6.2 Startargumente des Server Prozesses

Auf der Seite **Startargumente des Server Prozesses** können die Ressourcen begrenzt werden, die vom OpenScape FM Server belegt werden.

- **Maximaler Speicher**:
  Der hier angegebene Wert beschränkt die Größe des Hauptspeichers, der vom OpenScape FM Server belegt wird. Wird der Wert überschritten, wird entsprechend in die Auslagerungsdatei ausgelagert.
- **Maximale Logfile-Größe**:
  Dieser Wert beschränkt die Größe der Logdateien.
  Wird der Wert überschritten wird eine neue Logdatei begonnen, die alte wird nach `name_old` verschoben, eine bereits existierende `name_old` Datei wird nach `name_older` verschoben, und eine bereits existierende `name_older` Datei wird gelöscht.
- **Alte Protokolle TLSv1 und TLSv1.1 aktivieren**
  Ist dieser Haken gesetzt, werden die eigentlich veralteten Transport Layer Security Protokolle verwendet. Dies ist nicht empfohlen, kann aber beim Einsatz bestimmter Kombinationen von Java-Versionen notwendig sein.
  Ist der Haken nicht gesetzt, kommt TLSv2 zum Einsatz.

6.3 Active Directory Konfiguration

Das OpenScape FM erlaubt automatisches Anmelden von Anwendern mittels Active Directory.

Auf der Seite **Active Directory Konfiguration** kann diese Funktion aktiviert und der zu verwendende Active Directory Server ausgewählt werden.

Mehr dazu findet sich in *Abschnitt 14.1.9*.

6.4 Ereignis-Browser

Auf der Seite **Ereignis-Browser** wird konfiguriert, welche Ereignisse automatisch aus den Ereignis-Browser gelöscht werden sollen.

Ein Ereignis wird immer dann automatisch gelöscht, wenn die Anzahl der vorhandenen Ereignisse die im Feld **Maximale Ereignisanzahl** angegebene Maximalgrenze überschreitet.

Das Auswahlmenü **Regel zum Löschen von Ereignissen** legt dann fest, welches Ereignis gelöscht wird.

- **Älteste**
  Das älteste vorliegende Ereignis wird gelöscht.
- **Älteste Bestätigte**
  Das älteste bestätigte Ereignis wird gelöscht. Sind alle Ereignisse bestätigt, wird das älteste vorliegende Ereignis gelöscht.
- **Älteste Bestätigte nach Status**
  Das älteste Ereignis unter den bestätigten Ereignissen mit dem niedrigsten Status wird gelöscht. Gibt es auch keine bestätigten *Critical* Ereignisse mehr, wird das älteste unbestätigte Ereignis des niedrigsten Status gelöscht.

Außerdem kann auf der Seite festgelegt werden, ob das Bestätigen eines Ereignisses automatisch auch das Attribut *In Arbeit* von diesem Ereignis entfernt.

6.5 Proxies

Die Seite **Proxies** dient dazu, Verbindungen zu IP-Adressen einzurichten, die nicht in intern überwachten Netzwerken liegen.

Die Seite besteht aus einer Auflistung von Adressen und Adressbereichen, denen jeweils ein Proxy zugewiesen werden kann. Dieser ist dann für die Anbindung der entsprechenden IP-Adressen zuständig.

Die Liste wird vor einem Kontakt mit einer IP-Adresse in der Reihenfolge der **Index**-Nummer ausgewertet, und der erste Eintrag, der zu der gewünschten IP-Adresse passt kommt zur Ausführung.

Dabei versucht OpenScape FM in der Regel zuerst eine HTTP (HTTPS) Verbindung herzustellen. Gelingt dies nicht wird eine SOCKS Verbindung versucht.

Über die unten platzierten Schaltflächen können Einträge erzeugt, bzw. selektiert Einträge gelöscht oder innerhalb der Liste verschoben werden.

Dabei enthalten die Felder:

- **Index**
  Das Reihenfolgekriterium der Auswertung.
- **Netzwerk**, **Adresse** und **Maske**
  Diese Felder definieren den IP-Adressbereich, für den der jeweilige Eintrag zuständig ist.
  Dabei kann in das Feld **Netzwerk** oder **Adresse** der Hostname oder die IP-Adresse des entsprechenden IP-Knotens oder Netzwerkes und in das Feld **Maske** die Netzmaske (z.B. eingetragen `255.255.240.0`) eingetragen.
  Das OpenScape FM ermittelt zu eingegebenen Namen oder IP-Adressen das passende Gegenstück und überträgt diese automatisch in die Felder **Netzwerk** und **Adresse**.
- **Host** und **Port**
  Diese beiden Felder definieren den Proxy, der für die Verbindung zu den passenden IP-Adressen verwendet werden soll.
- **Typ**
  Legt die Art der Verbindung fest. Diese kann per *SOCKS* oder *HTTP* erfolgen.
  Wird *Direct* ausgewählt, erfolgt eine unmittelbare Verbindung ohne einen zwischengeschalteten Proxy. Dies kann z.B. verwendet werden, um einen einzelnen Knoten eines definierten Netzwerkes aus der Proxy-Verwendung auszuschließen, indem der *Direct* Eintrag vor der Definition des Netzwerkes in die Proxy-Liste aufgenommen wird.

6.6 Datenbankverbindung

Die Seite **Datenbankverbindung** kann verwendet werden, um eine Standard-Datenbank auszuwählen, sie zu konfigurieren oder eine neue Standard-Datenbank einzurichten.

Im Menü **Datenbankverbindung** kann eine der aktuell definierten Datanbanken als Standard-Datenbank ausgewählt werden. Mit dem daneben befindlichen **Schaltfläche** kann der Zugriffsaccount für die ausgewählte Datenbank konfiguriert werden.

Über die Schaltfläche **Neue Verbindung** wird eine neue Datenbank im OpenScape FM eingeführt.

Neben einem **Objektnamen** zur Identifikation der Datenbank-Definition kann unter **Treiber** einer der Datenbank-Treiber ausgewählt werden, die sich im Verzeichnis
`<OpenScape FM_installationverzeichnis>/server/lib/external` oder
`<OpenScape FM_installationverzeichnis>/server/lib/external`
befinden. Mit Auswahl der Treibers wird der Typ der Datenbank ausgewählt, über die Schaltfläche **Erzeugen** wird dann ein Fenster geöffnet, in dem die Zugriffsparameter festgelegt werden können.

6.7 Daten Export

Auf der Seite **Daten Export** wird festgelegt, wann alte Daten automatisch aus der OpenScape FM Datenbank gelöscht werden sollen.

Über drei Seiten verteilt kann getrennt für **Ereignis**se, **Status**wechsel und System Management **Parameter** Werte festgelegt werden, wie alt zu löschende Daten mindestens sein müssen (**Löschintervall**) und wie häufig überprüft werden soll, ob zu löschende Daten vorliegen (**Löschprüfintervall**).

Für System Management Parameter kann zusätzlich ausgewählt werden, die Daten welcher externen Agenten überhaupt exportiert werden sollen (**Exportiere Parameter-Daten für Agent**).

6.8 Update

Die automatische Software-Update-Funktion kann auf der Seite **Update** konfiguriert werden. Mehr dazu findet sich unter *Abschnitt G.1*.

6.9 SSL-Zertifikat

Auf der Seite SSL-Zertifikat kann festgelegt werden, ob der Server HTTPS verwenden soll, und welche Parameter für die Erstellung der selbstsignierten Zertifikate verwendet werden. Mehr dazu findet sich in *Abschnitt 26.2*.

6.10 Info

Die Seite **Info** zeigt allgemeine Informationen über den Server an.

Sie zeigt z.B. den freien und verwendeten Speicher auf dem Server-Host, das Datum der Server- und Datenbankerstellung, die installierte Version und die Installationstermine der bisher installierten Versionen an.

7 Objekt- und Ereignis-Suche

Das OpenScape FM stellt Funktionen bereit, um Objekte oder Ereignisse zu suchen. Diese werden in den folgenden Abschnitten vorgestellt.

Die einfache Schnellsuche (siehe *Abschnitt 7.1*) erlaubt lediglich einen schnellen Zugriff auf Objekte, deren Eigenschaften den gesuchten Teilstring enthalten.

Dagegen erlauben die Objekt-Suche (siehe *Abschnitt 7.2*) und die Ereignis-Suche (siehe *Abschnitt 7.3*) komplexe Suchanfragen, in denen alle erdenklichen Objekt- bzw. Ereigniseigenschaften zur Filterbedingung gemacht werden können.

7.1 Objekt-Schnellsuche

Die Schnellsuche ist ein Suchfilter, der nach OpenScape FM Objekten sucht, welche spezifische Teilstrings in ihren relevanten Eigenschaften enthalten. Unter den relevanten Eigenschaften befinden sich der Objektbezeichner, der eindeutige Objektname und Kommentare für das Objekt bzw. Annotationen für ein Ereignis.

Das Eingabefeld für die Schnellsuche befindet sich in der rechten Hälfte der Hauptmenüleiste und die Suche wird durch das Eingeben eines Suchtextes in das Eingabefeld und Betätigung der *Return*-Taste gestartet.

Um z.B. eine Schnellsuche durchzuführen, die einen spezifischen Host oder Objekte mit einem spezifischen Kommentar finden soll, müssen lediglich Teile des Host-Namens oder des Kommentars in das Feld eingegeben und *Return* gedrückt werden.

Es können mehrere Einträge, durch Leerzeichen getrennt, in das Eingabefeld eingegeben werden.

Einträge, die aus einem einzelnen Zeichen bestehen werden von der Suche ignoriert, um nutzlose Suchergebnisse zu vermeiden.

Ein Objekt passt zu einer Suche, wenn wenigstens eine seiner relevanten Objekt-Eigenschaften alle Sucheinträge als Teilstring enthält.

Die Suche ist unabhängig von der Groß-/Kleinschreibung und Platzhalter werden nicht unterstützt. Mit Ausnahme der Groß-/Kleinschreibung wird alles genauso ausgewertet, wie es eingegeben wird.

Alle Objekte, die auf eine Suche passen, werden in einer Ergebnistabelle dargestellt. Diese Tabelle zeigt den **Objekt**-Bezeichner, den Objekt-**Typ**, den eindeutigen **Internen Objektnamen** und in wievielen Submaps das entsprechende Objekt aktuell **Versteckt** ist. Die üblichen Kontext-Menüs für die Tabellen-Einträge können verwendet werden, um auf die einzelnen Objekte und ihre Funktionen zuzugreifen.

Standardmäßig werden die Objekte nach der Relevanz ihres Objekttyps sortiert. Dabei stehen die relevanten Typen wie IP-Knoten und IP-Netzwerke an der Spitze der Tabelle.

7.2 Objekt-Suche

Das OpenScape FM Desktop stellt einen Dialog zu Verfügung um Objekte, die gemeinsame Eigenschaften besitzen, zu suchen. So ist es möglich:

- Objekte zu finden, die sich entweder in der offenen Map befinden, oder (falls die zugehörige Submap noch nicht geöffnet ist) in der Objekt-Datenbasis, welche die Suchobjekte enthält.
- Suchanfragen nach bestimmten Objekt- und Symboleigenschaften zu generieren. Dies könnten z.B. alle Anwender, alle Ip-Knoten oder alle Objekte mit einem spezifischen Bezeichner sein.
- Die Submap für die gefundenen Objekte direkt aus der Ergebnisliste heraus zu öffnen.

Die Auswahl des Menüeintrages **Client->Objektsuche...** öffnet das 'Objektsuche' Fenster, um eine globale Suche durchzuführen. Soll die Suche auf einen Teilbaum der Objekt-Hierarchie beschränkt werden, kann der Menüeintrag **Öffnen->Objektsuche...** im Kontextmenü des Wurzelobjektes des gewünschten Teilbaumes ausgewählt werden. Dies öffnet das gleiche Fenster. Wurde für einen Teilbaum bereits eine Objektsuche durchgeführt, kann die gleiche Suche über das Kontextmenü des Wurzelobjektes und den Eintrag **Öffnen->Letzte Suche** erneut ausgeführt werden.

Die Karteikarte **Objekt** dieses Fensters wird verwendet, um Objektsuchen durchzuführen. Diese Karteikarte muss aktiv sein, wenn die Schaltfläche **Suchen** betätigt wird, damit eine Objektsuche ausgeführt wird. Der Name der aktuellen Seite lautet in diesem Fall ebenfalls **Objektsuche**.

Es gibt unterschiedliche Objekt- bzw. Symbol-Charakteristiken, die ausgewählt werden können, um Objekte aus der OpenScape FM-Datenbasis zu suchen:

- **Kennzeichen:** Der Map-spezifische Bezeichner, der auf der Submap oder im Baum dargestellt wird. In das Feld kann ein Suchmuster eingegeben werden. Dieses Suchmuster ist entweder ein einfacher Teilstring oder ein Regulärer Ausdruck. Nähere Details zu Regulären Ausdrücken finden sich in *Abschnitt 18.2.1, „Einrichtung von Filtern“*.
- **Objektname:** Der eindeutige Name des Objektes in der Datenbasis des OpenScape FM Servers. Dieses Feld kann ebenfalls einen Teilstring oder einen Regulären Ausdruck enthalten. Nähere Details zu Regulären Ausdrücken finden sich in *Abschnitt 18.2.1, „Einrichtung von Filtern“*.
- **Technologie/Objektyp:** Die Objekttechnologie und der Objekttyp für wesentliche Objekte. Bestimmte Wesentliche Objekte werden durch eine Technologie und einen Objekttyp klassifiziert. In anderen Worten: wesentliche Objekte sind einer Technologie zugeordnet. Ein gebräuchliches Beispiel für eine Technologie ist “IP”, der z.B. die Objekttypen “Netzknoten” (Suche nach allen IP Netzknoten), “Snmp” (Suche nach allen bekannten Snmp Agenten), “HTTP” (Suche nach allen Bekannten Web Browsern) zugeordnet sind. Es kann nach allen Objekten einer Technologie gesucht werden, oder nur nach den Objekten eines Objekttyps einer Technologie. Wird im Auswahlmenü eine Technologie ausgewählt, so erscheinen im zugehörigen **Objekttyp** Auswahlmenü alle dieser Technologie bekannten Objekttypen.
- **Status:** Der Anwender kann nach Objekten suchen, die durch ein Symbol mit den ausgewählten Status, wie z.B. 'Normal” oder “Minor” repräsentiert werden.
- **Form:** Die Form des Symbols, dass das Objekt auf Submaps oder im Baum repräsentiert.
- **Bitmap:** Die Bitmap des Symbols, dass das Objekt auf Submaps oder im Baum repräsentiert.

- **Groß-/Kleinschreibung:** Mit Hilfe dieses Schalters kann festgelegt werden, ob bei der Suche nach Kennzeichen oder Objektnamen die Groß-/Kleinschreibung berücksichtigt werden soll oder nicht.
- **Objektnamen anzeigen:** Ist der Schalter angeschaltet, so werden in der Suchergebnisliste die Objektnamen der gefundenen Objekte angezeigt. Zusätzlich werden, in eckige Klammern eingeschlossen, die Kennzeichen angezeigt. Ist der Schalter ausgeschaltet, werden ausschließlich die Kennzeichen angezeigt.
- **Status Propagation berücksichtigen:** Ist dieser Schalter eingeschaltet, werden nur Objekte von der Suche berücksichtigt, die ihren Status bis zu dem Objekt propagieren können, für das die Suche gestartet wurde (oder das Root-Objekt für eine globale Suche). Dies kann verwendet werden, um nur die Objekte zu finden, die unmittelbaren Einfluss auf den Status des Basis-Objektes der Suche nehmen können.
- **Objekteigenschaften**, **Werte:** Unter **Objekteigenschaften** kann eine Objekteigenschaft (siehe *Abschnitt 5.7, „Standard-Info-Browser“*) ausgewählt werden. Es werden dann nur die Objekte gefunden, welche die entsprechende Objekteigenschaft besitzen, und deren Eigenschaftswert dem Eintrag im Feld **Werte** entspricht.

Wird mehr als eine Objekt-/Symbol-Charakteristik angegeben, so verbinden die Suchmaschine diese mit einer UND-Relation. Das heißt, alle ausgewählten Charakteristiken müssen gleichzeitig zutreffen. Um eine Objektsuche zu starten, muss die Schaltfläche **Suchen** im unteren Bereich des “Objektsuche” Fensters betätigt werden während die Karteikarte **Objekt** geöffnet ist. Die Liste **Suchergebnisse** zeigt daraufhin alle gefundenen passenden Objekte sofort an. Um eine Objektsuche abzubrechen, kann die Schaltfläche **Stopp** aktiviert werden. Ein Doppelklick auf einen Eintrag innerhalb der Suchergebnis Liste öffnet die Submap (des ersten gefundenen Vaterobjektes) auf dem das entsprechende Objekt dargestellt ist.

Die Schaltflächen **Verwalten**, **Nicht verwalten** und **Löschen** lösen für alle in der Liste selektierten Objekte die gleichnamigen Funktionen aus. D.h. die selektierten Objekte werden, falls möglich, verwaltet, nicht verwaltet, oder nach Rückfrage gelöscht.

Die Schaltfläche **Ereignisse** öffnet ein Fenster, das alle Ereignisse der aktuell in der Objektliste befindlichen Objekte enthält.

Mit der Schaltfläche **Verstecken** können alle selektierten Objekte versteckt bzw. mit der Schaltfläche **Anzeigen** wieder sichtbar gemacht werden. Dies entspricht den in *Abschnitt 12.1, „Versteckte Objekte“* beschriebenen gleichnamigen Funktionen für Symbole. In diesem Fall wird die Funktion jedoch nicht für jeweils ein einzelnes Symbol, sondern für alle Symbole ausgeführt, welche die selektierten Objekte darstellen.

Die Schaltfläche **Suche Zurücksetzen** leert alle Eingabefelder der Karteikarten **Objekt** *und* **Ereignis**, entfernt alle Auswahlhaken und setzt alle Auswahlmenüs auf die jeweilige Voreinstellung zurück. Diese Funktion ermöglicht die schnelle Einleitung einer neuen Suche.

7.3 Ereignis-Suche

Die Ereignis-Suche verwendet das gleiche Fenster wie die oben beschriebene Objekt-Suche (siehe *Abschnitt 7.2, „Objekt-Suche“*). Ähnlich der Objekt-Suche können Ereignisse für alle Objekte gesucht werden (über den Hauptmenü-Eintrag **Client->Objektsuche...**), oder für alle Objekte, die sich in einer untergeordneten Hierarchie befinden (über den Kontextmenü-Eintrag **Öffnen->Objektsuche...** des übergeordneten Objektes).

Falls Ereignisse gesucht werden sollen, muss die Karteikarte **Ereignis** aktiv sein, wenn die Schaltfläche **Suchen** betätigt wird. Der Name der aktuellen Seite lautet in diesem Fall ebenfalls **Ereignissuche**.

Die Suche zeigt dann alle Ereignisse an, welche den unten beschriebenen Ereignis-Kriterien entsprechen **UND** die für ein Objekt empfangen wurden, das den auf der Karte **Objekt** gewählten Kriterien entspricht. Sollen *alle* Ereignisse berücksichtig werden, kann für die Objekt-Suchfelder **Kennzeichen** und **Objektname** der allgemeine Platzhalter `.*` verwendet werden.

Die folgenden Ereignis-Kriterien können konfiguriert werden, um die gefundenen Ereignisse einzuschränken:

Kategorie, **Ursprung**, **Beschreibung**, **Bestätigt**, **Korreliert**: Diese korrespondieren mit den entsprechenden Feldern des Ereignis-Browsers (siehe *Abschnitt 5.9, „Der Ereignis-Browser“*). Für die Felder **Ursprung** und **Beschreibung** können reguläre Ausdrücke verwendet werden (siehe *Abschnitt 18.2.1, „Einrichtung von Filtern“*).

Status Minimum, **Status Maximum**: Diese definieren den minimalen und maximalen Status der zutreffenden Ereignisse.

Zeitplan: Hier kann ein Zeitplan oder Wartungsfilter ausgewählt werden, in dem die zutreffenden Ereignisse empfangen worden sein müssen.

Startdatum, **Endedatum**: Diese definieren das Zeitintervall in dem die zutreffenden Ereignisse empfangen worden sein müssen.

8 Ereignisaktionen

Ereignisaktionen sind im OpenScape FM dafür verantwortlich, die Ereignisse zu erzeugen, die im Ereignis Browser (siehe *Abschnitt 5.9*) angezeigt werden.

Im OpenScape FM existieren drei verschiedene Quelltypen, deren Ereignisse Ereignisaktionen auslösen können:

- **Externe Ereignisse** werden von externen Quellen über allgemeine SNMP-Traps ausgelöst. Die entsprechende MIB muss in das OpenScape FM geladen worden sein.

  Zum Beispiel: Ist ein SNMP-Trap aufgetreten, der von einem Drucker abgesendet wurde und ein Problem meldet, wird im OpenScape FM eine Externe Ereignisaktion erstellt, falls dies entsprechend konfiguriert wurde.

- **Integrierte Ereignisse** werden durch spezifische SNMP-Traps ausgelöst, die Technologie spezifischen OpenScape FM Plugins bekannt sind, und von diesen behandelt werden.

  Zum Beispiel: Link-Down-Traps werden durch das IP Manager Plugin erkannt und bearbeitet. Wurde das IP Manager Plugin initialisiert, werden Integrierte Ereignisaktionen erzeugt. Auch dann, wenn die entsprechende MIB nicht in das OpenScape FM geladen wurde.

- **Interne Ereignisse** werden durch das OpenScape FM selbst ausgelöst, und werden verwendet, um den Anwender über Fakten zu informieren, die durch das OpenScape FM festgestellt wurden.

  Zum Beispiel: Wird ein Lizenzverstoß durch das OpenScape FM festgestellt, oder kann ein IP-Knoten nicht mehr erreicht werden, wird eine Interne Ereignisaktion erzeugt.

Für alle drei Auslösungstypen können im OpenScape FM **Ereignisse** (siehe *Abschnitt 8.1*) und **Automatisierte Aktionen** auf diese Ereignisse (siehe *Abschnitt 8.2*) konfiguriert werden.

In einigen Fällen sind manuell angestoßene Aktionen für bereits aufgelistete Ereignisse erwünscht. Wie diese behandelt und konfiguriert werden, ist in *Abschnitt 8.3* beschrieben.

Sollen bestimmte Ereignisse für vordefinierte oder alle Objekte unterdrückt werde, kann das gewünschte Ignorieren über ein vereinfachtes Verfahren konfiguriert werden (siehe *Abschnitt 8.4*).

8.1 Ereignisse Anpassen

Die Ereignisanpassung legt fest, welche eingehenden Ereignisse durch das OpenScape FM bearbeitet werden sollen, und wie diese Ereignisse strukturiert und im Ereignis-Browser angezeigt werden sollen.

Die erzeugten OpenScape FM Ereignisse werden zusätzlich dem Objekt zugeordnet, zu dem sie am besten passen. In der Regel ist dies ein Kind-Objekt des IP-Knotens, dessen IP dem Ereignis zugeordnet werden kann. Ein Interface-Ereignis wird also in der Regel z.B. dem passenden Interface-Objekt des IP-Knotens zugewiesen, zu dem das Interface gehört.

Hinweis:
In einigen Fällen können Ereignisse auch mehreren Objekte zugewiesen werden. Für einige Technologien werden z.B spezielle Ereignisse einer Komponente und dem übergeordneteten IP-Knoten zugewiesen.
Wird ein derartiges Ereignis bestätigt, wirkt sich eine Bestätigung entsprechend auf alle Objekte aus, denen das Ereignis zugewiesen wurde.

Kann ein Ereignis keinem konkreten Kind-Objekt eines IP-Knotens zugewiesen werden, wird als Default das Kind-Objekt **Ereignisse** verwendet.

Die Ereignisanpassung zeigt eine Liste mit allen möglichen eingehenden Ereignissen an, und bietet die Möglichkeit, basierend auf den Werten dieser Ereignisse OpenScape FM Ereignisse zu generieren.

Standardmäßig stellt des OpenScape FM vordefinierte Ereigniskonfigurationen für zahlreiche interne und integrierte Ereignisse bereit.

Die Anpassung findet auf zwei Seiten statt. Zunächst wird die Ereignisanpassung verwendet, um eine Ereignisquelle auszuwählen (siehe *Abschnitt 8.1.1*). Danach kann der Ereignis-Konfigurationsbrowser verwendet werden, um individuelle Ereignisse für die ausgewählte Quelle zu definieren (siehe *Abschnitt 8.1.2*).

8.1.1 Anpassung der Ereignisquellen

In der Ereignisanpassung wird zunächst eine Ereignisquelle ausgewählt. Die Ereignisanpassung kann über den Eintrag **Ereignistypen** aus dem Hauptmenü **Server** gestartet werden.

Das Konfigurationsfenster enthält eine Auflistung aller möglichen Ereignisquellen. Jede Quelle für interne oder integrierte Ereignisse wird im Allgemeinen durch den Namen des Plugins repräsentiert, das die Ereignisse generiert. Für externe Quellen (SNMP-Traps) wird ein Eintrag für jede Enterprise MIB Definitionsdatei, die in das OpenScape FM geladen wurde, angezeigt.

Ein Doppelklick auf eine Quelle in der Liste, oder die Auswahl einer Quelle und ein Betätigen der Schaltfläche **Konfigurieren** öffnet den **Ereignis-Konfigurationsbrowser** für die ausgewählte Quelle.

8.1.2 Ereignis-Konfigurationbrowser

Der Ereignis-Konfigurationsbrowser dient dazu, festzulegen wie eingehende Ereignisse, abhängig von ihrem Typ, durch das OpenScape FM behandelt und im Ereignis-Browser angezeigt werden sollen. Jeder Ereignis-Konfigurationsbrowser wird, wie oben beschrieben, für eine ausgewählte Ereignisquelle geöffnet.

Das Browser-Fenster enthält eine Tabelle in der jede Zeile ein durch die Quelle definiertes Ereignis repräsentiert. Im Falle externer Ereignisse werden diese Ereignisse durch die entsprechende Definitionsdatei festgelegt

Die Spalte **Trap** enthält die Namen der unterschiedlichen eingehenden Ereignisse. Alle anderen Einträge können mit Hilfe der entsprechenden Felder, Schalter und Menüs auf der rechten Seite des Fensters konfiguriert werden.

Alle Textfelder können Makros beinhalten, die durch entsprechende Inhalte ersetzt werden, wenn ein Ereignis empfangen wird. Makros beginnen mit einem Dollar-Symbol (’$’) gefolgt von einem Bezeichner, der den Inhalt des Makros festlegt. Die möglichen Makros werden in der folgenden Tabelle aufgeführt.

`$1` - `$99`	Wert der entsprechenden Trap- oder Ereignis-Variablen
$#	Anzahl der Variablen
`$*`	Alle Trap- oder Ereignis-Variablen
`$@`	Die Zeit in Sekunden zu der das Ereignis generiert wurde
`$T`	Die Systemzeit des SNMP-Agenten-Systems als der Trap versendet wurde (für externe Ereignisse)
`$x`	Der Zeitpunkt als formatierte Zeichenkette, zu dem das Ereignis generiert wurde
`$R` oder `$r`	Die Absender IP
`$e`	Die Enterprise-OID des Ereignisses
`$h`, `$H`	Der Hostname bzw. FullyQualified Hostname, oder, falls dieser nicht ermittelt werden kann, die IP-Adresse der Ereignisquelle

Tabelle 3 Makros

Das Feld **Meldung** konfiguriert die Zeichenkette, die in der Spalte *Beschreibung* des Ereignis-Browsers angezeigt wird. Die Spalte **Kategorie** definiert den Inhalt der Ereignis-Browser-Spalte gleichen Namens.

Das Feld **Statusformat** konfiguriert den Status, der mit dem Ereignis verbunden wird, und der im Ereignis-Browser in der Spalte *Status* angezeigt wird. Hier kann einer der konstanten Werte aus dem Auswahlmenü (z.B. ’*Normal*’, ’*Critical*’) gewählt werden. Wurde im MIB-Editor ein Ressource-Schlüssel definiert, so wird dieser angezeigt.

Der Schalter **Verwaltet** legt fest, ob entsprechende Ereignisse ausgewertet werden sollen, oder nicht.

Der Schalter **Blinken** legt fest, ob das betroffene Objekt im OpenScape FM blinken soll, wenn ein entsprechendes unbestätigtes Ereignis im Ereignis-Browser existiert.

Der Schalter **Client-Meldung** legt fest, ob eine Client-Meldung erzeugt werden soll, wenn ein entsprechendes Ereignis erstellt wird.

Ereignisse: Automatisch bestätigen

Das OpenScape FM besitzt einen Mechanismus, der es ermöglicht, dass neu eingehende Ereignisse automatisch alle bereits vorhandenen ‚passenden‘ Ereignisse bestätigen. Dies soll z.B. dafür sorgen, dass gutmeldende Traps automatisch die zugehörigen Problem-Traps bestätigen.

Um dies zu ermöglichen, wird intern jedem eingehenden Ereignis automatisch mindestens ein Schlüssel zugewiesen. Bereits vorhandene Ereignisse, mit einem dieser Schlüssel, werden in diesem Augenblick automatisch bestätigt. Dabei spielt der Typ der Ereignisse keine Rolle.

Die Felder **Ereignistypformat** und **Ereignistyptrenner** legen fest, wie für den ausgewählten Ereignistyp diese Schlüssel generiert werden.

Das Feld **Ereignistypformat** definiert dabei die Formatvorlage, welche zur Generierung des Schlüssels verwendet wird. In diese können die oben aufgeführten Makros eingebunden sein.

Soll mehr als ein Schlüssel für ein Ereignis erzeugt werden, so kann im Feld **Ereignistyptrenner** ein Symbol festgelegt werden, mit dem die Zeichenkette aus dem Ereignistypformat-Feld unterteilt wird. Alle so generierten Schlüssel werden mit dem entsprechenden Ereignis im Ereignisbrowser verbunden.

Beispiel:

Ein Trap wurde empfangen und die Trap-Variablen $3, $4 und $5 enthalten die Werte ’100’, ’15’ und ’36’.

Wurde das Ereignistypformat mit ’XTrap $3 $4’ definiert und wurde kein Trenner festgelegt, so wird als Schlüssel für das Ereignis ’XTrap 100 15’ abgelegt.

Wurde das Ereignistypformat mit ’`XTrap $3 $4&XTrap $3 $5`’ definiert und wurde als Trenner ’`&`’ festgelegt, so sind die Schlüssel für das Ereignis: ’`XTrap 100 15`’ und ’`XTrap 100 36`’.

Soll zusätzlich zu den bereits vorhandenen Ereignissen mit gleichem Schlüssel auch das aktuelle neue Ereignis bestätigt werden, können stattdessen die Felder **Rücksetztypformat** und **Rücksetztyptrenner** verwendet werden. Die Felder für das Ereignistypformat müssen in diesem Fall leer bleiben.

Beispiel:

Für den Trap `Link-Down` wurde das **Ereignistypformat** `$r:Down:$1` festgelegt.

Für den Trap `Link-Up` wurde das **Rücksetztypformat** `$r:Down:$1` festgelegt.

Wird nun ein `Link-Down` Trap empfangen, für den $r durch `192.168.1.1` und `$1` durch `4` substituiert werden, so wird der Schlüssel `192.168.1.1:Down:4` für das dem Trap zugehörige Ereignis abgelegt.

Wird später ein `Link-Up` Trap empfangen, für den `$r` ebenfalls durch `192.168.1.1` und `$1` ebenfalls durch `4` substituiert werden, so wird durch das gewählte Rücksetztypformat ein identischer Schlüssel generiert, und damit durch den Trap das ursprüngliche `Link-Down` Ereignis und das neue passende ‚positive‘ `Link-Up` Ereignis bestätigt.

Wird für einen Ereignistyp weder ein Ereignistypformat noch ein Rücksetztypformat vergeben, wird ein Default-Format verwendet. Dieses setzt den Schlüssel aus der Quelle des Ereignisses und dem Namen des Ereignistyps zusammen. Dies sorgt dafür, dass Ereignisse vorhandene gleichartige Ereignisse für das gleiche Objekt automatisch bestätigen.

Für viele Ereignistypen werden bei der Installation des OpenScape FM bereits automatisch sinnvolle Konfigurationen eingetragen.

Diese Voreinstellungen sorgen in aller Regel dafür, dass Ereignisse mit Status ‚*Normal*‘ alle inhaltlich passenden Ereignisse der gleichen Quelle mit anderem Status bestätigen.

Ereignisse: Duplikate unterdrücken

Die Felder **Duplikat-Format** und **Duplikat-Zeit** können verwendet werden, um die Auswertung von duplizierten eingehenden Ereignissen zu vermeiden (z.B. die Verhinderung einer doppelten Auswertung eines Ereignisses, dass von zwei überwachenden Quellen gesendet wird).

Das *Duplikat-Format* wird wie die oben beschriebenen Schlüssel verwendet. Basierend auf dem Format, wird für jedes eingehende Ereignis, für das ein *Duplikat-Format* definiert wurde, ein *Duplikat-Schlüssel* erstellt. Anschließend wird überprüft, ob innerhalb des durch die *Duplikat-Zeit* definierten Zeitintervalls ein anderes Ereignis des gleichen Typs und mit dem gleichen *Duplikat-Schlüssel* empfangen wurde. Ist dies der Fall, wird das Ereignis als Duplikat markiert und standardmäßig ignoriert.

Hinweis:
Eingehende Ereignisse werden durch das Event Correlation Engine Plugin bearbeitet. Im ECE kann die Bearbeitung von Ereignissen, die als Duplikate markiert sind, modifiziert werden (siehe separate *Event Correlation Plugin Bedienungsanleitung*).

Die Schaltflächen unterhalb der Tabelle **Aktualisieren** den Tabelleninhalt, **Schließen** das Fenster oder öffnen die Konfiguration für die Ereignisaktion des aktuellen Ereignisses (siehe *Abschnitt 8.2*).

8.2 Automatisierte Reaktionen für Ereignisse

Eine Automatisierte Reaktion für ein eingehendes Ereignis ist eine vordefinierte Aktion, die immer dann ausgeführt wird, wenn ein Ereignis eines spezifischen Typs für ein spezifisches Objekt innerhalb eines definierten Zeitintervalls empfangen wird.

Allen Ereignissen, die vom OpenScape FM behandelt werden, können vollständig konfigurierbare Automatisierte Reaktionen zugewiesen werden. Automatisierte Reaktionen sind daher ein Mechanismus, der es dem OpenScape FM erlaubt, sofort auf einkommende Ereignisse zu reagieren. Und zwar derartig, dass dies unter vollständiger Kontrolle der OpenScape FM Administratoren geschieht.

Die folgenden Unterabschnitte beschreiben, wie Aktionen mit einer Kombination aus Ereignissen, Objekten und Zeitintervallen verbunden werden können, um eine Automatisierte Reaktion zu definieren (siehe *Abschnitt 8.2.1*), und wie die Objektfilter (siehe *Abschnitt 8.2.2*), Zeitfilter (siehe *Abschnitt 8.2.3*) und Aktionen (siehe *Abschnitt 8.2.4*), die kombiniert werden sollen, konfiguriert werden.

Für den Sonderfall, dass bestimmte Ereignisse lediglich ignoriert werden sollen, wird in *Abschnitt 8.4* ein vereinfachtes Konfigurationsverfahren beschrieben.

8.2.1 Automatisierte Reaktionen definieren

Entsprechend der Konfiguration wird eine Automatisierte Reaktion dann ausgeführt, wenn ein Ereignis eines spezifischen Ereignistyps für ein definiertes Objekt innerhalb eines definierten Zeitintervalls eintrifft.

Wichtiger Hinweis:
Für diese Funktionalität wird das Event Correlation Engine Plugin benötigt.

Die Konfiguration der Automatisierten Reaktionen für Ereignisse wird über den Eintrag **Ereignisfilter** aus dem Hauptmenü **Server** aufgerufen.

Für einzelne Ereignistypen kann ein ähnliches Konfigurationsfenster geöffnet werden, indem der Eintrag **Konfigurieren** aus dem Kontextmenü eines Symbols ausgewählt wird, das den Ereignistyp repräsentiert. Derartige Symbole sind z.B. bei der Konfiguration von Ereignistypen verfügbar (siehe *Abschnitt 8.1*).

Hinweis:
Mit Ausnahme des fehlenden Auswahlbereichs für Ereignistypen sind die Konfigurationsfenster funktional identisch.

Die auf einen einzelnen Ereignistyp beschränkte Konfiguration kann ebenfalls aus dem Kontextmenü eines Ereignisses geöffnet werden. Hier öffnet der Eintrag **Ereignis->Ereignisfilter** die Konfiguration für den Typ des Ereignisses.

Auf der Seite **Ereignisfilter**, können den Aktionen Kombinationen von Ereignistypen, Objektfiltern und Zeitfiltern zugewiesen werden.

Die Seite enthält eine Liste, die pro Zeile eine konfigurierte Automatisierte Reaktion anzeigt. Jede dieser Zeilen zeigt den **Ereignistyp** und die Zuweisungen zu diesem Ereignistyp an: das *Objekt*, der *Zeitplan* und die *Aktion*.

Neue Einträge können mit der Schaltfläche **+** erzeugt und ausgewählte Einträge mit der Schaltfläche **-** gelöscht werden.

Ausgewählte Einträge können modifiziert werden, indem die Konfigurationsparameter mit Hilfe der rechts befindlichen Auswahlelemente modifiziert werden:

- Der Bereich **Ereignistypen** zeigt einen Baum mit den internen, integrierten und externen Ereignistypen an, die dem OpenScape FM bekannt sind (siehe *Abschnitt 8.1*). Sie sind nach ihrer Quelle geordnet. Ereignistypen, die aktuell nicht überwacht werden, werden im Status *Nicht verwaltet* dargestellt.
- Das Menü **Filter** wird verwendet, um die Objekte auszuwählen, die mit der Automatisierten Reaktion verbunden werden sollen. Es enthält zwei Einträge für jeden definierten Objektfilter (siehe *Abschnitt 8.2.2*). Die entsprechenden Einträge besitzen entweder einen grünen Haken oder ein rotes X vor dem Namen des Filters. Der Haken-Eintrag repräsentiert die Objekte, für die der Filter zutrifft. Der X-Eintrag alle Objekte, für die der Filter nicht zutrifft.
- Das Menü **Zeitplaner** wird verwendet, um die Zeitintervalle auszuwählen, während denen die Automatisierte Reaktion durchgeführt werden soll. Es enthält zwei Einträge für jeden definierten Zeitfilter (siehe *Abschnitt 8.2.3*). Die entsprechenden Einträge besitzen entweder einen grünen Haken oder ein rotes X vor dem Namen des Filters. Der Haken-Eintrag repräsentiert Zeitpunkte, auf die der Filter zutrifft, der X-Eintrag alle anderen Zeitpunkte.
- Das Menü **Aktionen** wird verwendet, um eine Aktion auszuwählen, die von der Automatisierten Reaktion ausgelöst werden soll. Es enthält Einträge für alle vordefinierten Aktionen, die als Reaktion durchgeführt werden können (siehe *Abschnitt 8.2.4*). Die ausgewählte Aktion wird immer dann ausgeführt, wenn ein Ereignis des ausgewählten Typs empfangen wird, und die ausgewählten Filter zutreffen.

8.2.2 Objektfilter für Reaktionen definieren

Objektfilter werden verwendet, um die Objektmenge festzulegen, für die eine Automatisierte Reaktion ausgeführt werden soll.

Objektfilter werden automatisch erstellt und durch Event Correlation Engine (ECE) Knoten repräsentiert. Abhängig vom Filtertyp sind die Knoten vom Typ *IP-Muster-Filter* oder *Objekt-Filter* (siehe *Event Correlation Engine Plugin Bedienungsanleitung*).

Beide Knotentypen besitzen zwei Ausgänge. Einen für passende und einen für nicht passende Objekte. Beide Ausgänge können einer Automatisierten Reaktion zugewiesen werden. Es ist daher möglich, ‚invertierte' Filter zu erstellen.

Die Konfiguration der Automatisierten Reaktionen für Ereignisse wird in einem Fenster behandelt, dass sich öffnet, wenn der Eintrag **Ereignisfilter-Konfigurieren** aus dem Hauptmenü **Server** ausgewählt wird. Die Seite **Filter** innerhalb des Fensters kann verwendet werden, um diese Filter zu konfigurieren.

Die Seite enthält eine Auflistung der aktuell definierten Objektfilter. Jeder Filter wird durch eine eigene Zeile repräsentiert.

Die Schaltfläche **Erzeuge Filter** (**+**) kann verwendet werden, um einen neuen Filter zu erstellen. Der Typ des Filters kann aus dem sich öffnenden Fenster ausgewählt werden:

- **Objekt-Filter** kann verwendet werden, um einen neuen Filter zu erstellen, der nach manuell definierten Objekten filtert. Der Filter schaut nach Objekten aus, die aus dem Navigationsbaum ausgewählt wurden, oder die spezifische Eigenschaften besitzen, und wird durch einen ECE-Knoten des Typs *Objekt-Filter* repräsentiert.
- **IP-Muster-Filter** kann verwendet werden, um einen neuen Filter zu erstellen, der überprüft, ob sich IP-Knoten innerhalb der ausgewählten Teilnetzwerke befinden. Er wird durch einen ECE-Knoten des Typs *IP-Muster-Filter* repräsentiert.

Abhängig vom Filtertyp. kann die Schaltfläche **Konfigurieren** verwendet werden, um die Objekte und Objekteigenschaften oder die Teilnetzwerke zu verändern, die dem ausgewählten Filter zugewiesen wurden.

Die Schaltflächen **Ändert das Kennzeichen des Objektes** und **Objekt löschen** können verwendet werden, um den ausgewählten Filter umzubennen oder zu löschen. Der Name des Filters wird verwendet, um ihn in den Filter-Auswahlmenüs zu selektieren.

8.2.3 Zeitfilter für Reaktionen definieren

Zeitfilter werden verwendet, um die Zeitintervalle festzulegen, in denen Automatisierte Reaktionen ausgeführt werden sollen.

Zeitfilter werden automatisch erstellt und durch Event Correlation Engine (ECE) Knoten des Typs *Zeitplan*. repräsentiert (siehe *Event Correlation Engine Plugin Bedienungsanleitung*).

Der Knotentyp stellt zwei Ausgänge bereit, die für die Zeitfilter relevant sind. Einer für Ereignisse, die während des definierten Zeitintervalls auftreten, und einen für die sonstigen Ereignisse. Beide Ausgänge können einer Automatisierten Reaktion zugewiesen werden. Wurde z.B. ein Zeitfilter definiert, der während der Supportzeiten greift, so kann dieser auch für eine spezifische Reaktion verwendet werden, die immer dann ausgeführt werden soll, wenn kein unmittelbarer Support zu Verfügung steht (wie das Informieren eines Technikers über Telefon, falls ein sehr wichtiges Ereignis eintritt).

Die Konfiguration der Automatisierten Reaktionen für Ereignisse wird in einem Fenster behandelt, dass sich öffnet, wenn der Eintrag **Ereignisfilter-Konfigurieren** aus dem Hauptmenü **Server** ausgewählt wird. Die Seite **Zeitplan** innerhalb des Fensters kann verwendet werden, um diese Filter zu konfigurieren.

Die Seite enthält eine Auflistung der aktuell definierten Zeitfilter. Jeder Filter wird durch eine eigene Zeile repräsentiert.

Die Schaltfläche **Erzeuge Zeitplan** (**+**) kann verwendet werden, um einen neuen Filter zu erstellen, der nach einer Menge von manuell definierten Zeitintervallen filtert. Der Filter schaut danach, ob Zeitpunkte innerhalb der definierten Zeitintervalle liegen. Er wird durch einen ECE-Knoten des Typs *Zeitplan-Filter* repräsentiert.

Die Zeitpläne werden durch Objekte im Container **Root->System->Server->Filter Manager** repräsentiert. Wird ein Filterobjekt als Disabled (dunkelbraun) dargestellt, so trifft der Filter zum aktuellen Zeitpunkt nicht zu.

Die Schaltfläche **Konfigurieren** kann verwendet werden, um die Zeitintervalle zu verändern, die dem ausgewählten Filter zugewiesen sind.

Die Schaltflächen **Ändert das Kennzeichen des Objektes** und **Objekt löschen** können verwendet werden, um den ausgewählten Filter umzubennen oder zu löschen. Der Name des Filters wird verwendet, um ihn in den Filter-Auswahlmenüs zu selektieren.

8.2.4 Aktionen für Reaktionen definieren

Aktionen werden ausgeführt, wenn Automatisierte Reaktionen durch eingehende Ereignisse ausgelöst werden.

Die Aktionen, die in der Konfiguration der Automatisierten Reaktionen (siehe *Abschnitt 8.2.1*) verfügbar sein sollen, können in der Event Correlation Engine definiert und konfiguriert werden (siehe separate *Event Correlation Engine Plugin Bedienungsanleitung*).

Im ECE können existierende Aktionen modifiziert, oder neue Aktionen erstellt werden.

Das ECE-Modul, das für die Verarbeitung der Aktionen für Automatisierte Reaktionen zuständig ist, befindet sich im Ebenen-Filter-Knoten mit der Bezeichnung *Ereignisreaktionen*. Dieser findet sich im Container *Ereignisquelle* auf der zentralen ECE Submap.

Der Knoten *Ereignisreaktionen* enthält den Container *Aktionen*, in dem jedes Ausgangsobjekt eine mögliche Aktion repräsentiert. Die Bezeichner dieser Ausgangsobjekte dienen als Namen der Aktionen. ECE-Knoten, welche die gewünschten Aktionen durchführen, können an das jeweilige Ausgangsobjekt angebunden werden.

Neue Ausgangsobjekte und somit neue Aktionen können über den Eintrag **Neu->Aktion** aus dem Kontextmenü des Knotens *Ereignisreaktionen* erzeugt werden.

Die Konfiguration von Aktionen kann auch über ein Fenster durchgeführt werden, das sich über den Eintrag **Ereignisfilter-Konfigurieren** aus dem Hauptmenü **Server** öffnen lässt. Die Seite **Aktionen** innerhalb des Fensters wird für die Konfiguration dieser Aktionen verwendet.

Die Seite enthält eine Auflistung der aktuell definierten Aktionen. Jeder Aktion wird durch eine eigene Zeile repräsentiert.

Die Schaltfläche **Erzeuge Aktion** (**+**) kann verwendet werden, um eine neue Aktion zu erstellen. Während die oben beschriebene Methode die Erstellung eines beliebigen Aktionstyps ermöglicht, kann das durch die Schaltfläche geöffnete Fenster verwendet werden, um einige häufig benötigte generische Aktionen zu erzeugen:

- **Debugger** kann verwendet werden, um neue Aktionen zu erzeugen, die auf ECE Knoten des Typs *Debugger* basieren. Dieser Knotentyp sammelt eingehende Ereignisse und wird hauptsächlich für Debugging-Zwecke eingesetzt.
- **Externe Aktion** kann verwendet werden, um neue Aktionen zu erzeugen, die auf ECE Knoten des Typs *Externe Aktion* basieren. Dieser Knotentyp generiert Email, erzeugt SMS-Meldungen oder startet externe ausführbare Programme wenn er ein Ereignis empfängt.

- **Modifizierer** kann verwendet werden, um neue Aktionen zu erzeugen, die auf ECE Knoten des Typs *Modifizierer* basieren. Mit diesem Knotentyp können eingehende Ereignisse modifiziert werden. Beispielsweise kann ihr Status verändert werden, oder sie können bestätigt werden.

Die Schaltfläche **Konfigurieren** kann verwendet werden. um die Konfiguration des Knotens zu modifizieren, welcher die entsprechende Aktion repräsentiert

Die Schaltflächen **Ändert das Kennzeichen des Objektes** und **Objekt lösschen** können verwendet werden, um die ausgewählte Aktion umzubennen oder zu löschen. Der Name der Aktion wird verwendet, um sie in den Aktions-Auswahlmenüs zu selektieren.

8.3 Manuell angestoßene Reaktionen für Ereignisse

Neben den oben beschriebenen automatisierten Reaktionen (siehe *Abschnitt 8.2*) ist es manchmal erwünscht, bestimmte sich wiederholende Reaktionen für bereits im Ereignis-Browser (siehe *Abschnitt 5.9*) vorhandene Ereignisse durchzuführen.

So kann es z.B. erwünscht sein, dass ein Techniker für einzelne Ereignisse manuell kontaktiert werden soll, oder dass einzelne Ereignisse besonders behandelt werden sollen.

Für derartige Fälle bietet die Event Correlation Engine mit dem extra für diese Aufgabe bereitgestellten Ereignismenüeintrag-Knoten sehr umfangreiche Möglichkeiten an (siehe separate *Event Correlation Engine Plugin Bedienungsanleitung*).

Jeder dieser Knoten erweitert die Kontextmenüs aller Ereignis-Objekte um einen zusätzlichen Menüeintrag. Wird einer dieser Einträge ausgewählt, so wird der mit dem jeweiligen Knoten verbundene frei erstellbare Workflow ausgelöst und mit den Daten des zugehörigen Ereignisses befüllt. Jede beliebige in der Event Correlation Engine mögliche Aktion kann somit mit einem Menüeintrag der Ereignisse verbunden und mit dessen spezifischen Werten ausgeführt werden.

8.4 Ereignisse ignorieren (vereinfachtes Verfahren)

In *Abschnitt 8.2 ff.* wird beschrieben, wie eingehende Ereignisse automatisch durch das OpenScape FM behandelt werden können.

Dieses Verfahren ist höchst flexibel, aber auch mit einer relativ aufwendigen Konfiguration verbunden.

Für den speziellen Fall, dass bestimmte Ereignisse zukünftig grundsätzlich ignoriert werden sollen, bietet OpenScape FM ein deutlich vereinfachtes Verfahren an, das aus dem Kontextmenü eines passenden Ereignisses angestoßen werden kann:

- Der Eintrag **Ereignis->Ignoriere** aktiviert oder deaktiviert das Ignorieren des Ereignistyps des gewählten Ereignisses für das Objekt, dem das Ereignis zugewiesen ist.
- Der Eintrag **Ereignis->Ignoriere Global** aktiviert oder deaktiviert das Ignorieren des Ereignistyps entsprechend für alle Objekte.

In beiden Fällen zeigt ein Haken hinter dem Eintrag an, dass eine allgemeiner bzw. eine objekt-spezifischer Filter für den gewählten Ereignistyp vorliegt.

Hinweis:
Wurde das Objekt, dem das Ereignis zugewiesen ist, aus dem OpenScape FM entfernt, wird der Haken hinter **Ignoriere** immer angezeigt, da für dieses ehemalige Objekt alle Ereignisse ignoriert werden.

Am einfachsten kann auf vorliegende Ereignisse über den Ereignis-Browser (siehe *Abschnitt 5.9*) zugegriffen werden.

Soll das konfigurierte Ignorieren für ein Objekt oder alle Objekte zurückgenommen oder eine durch eine andere Aktion ersetzt werden, kann dies wie gewohnt mit der in *Abschnitt 8.2.1* beschriebenen Methodik erreicht werden.

Wird aus dem Kontextmenü eines Ereignisses der Eintrag **Ereignis->Ereignisfilter** ausgewählt, öffnet sich ebenfalls das in *Abschnitt 8.2.1* beschriebene Fenster. In diesem Fall ist der Inhalt aber auf den passenden Ereignistyp beschränkt.

9 Anzeige von Tray Bar Symbolen

Die Windows Plattform stellt einen System Tray Bar zu Verfügung, der verwendet werden kann, um das Verhalten von Systemprogrammen mit Hilfe von Symbolen zu überwachen. Außerdem kann er für den schnellen Zugriff auf Funktionen der Systemprogramme benutzt werden.

Der OpenScape FM Desktop enthält eine eigene Tray Bar Überwachung, welche die folgenden Funktionalitäten enthält:

- Status-Überwachung *eines* beliebigen Objektes aus der OpenScape FM Datenbasis pro Anwender.
- Benachrichtung (durch Abspielen einer Sounddatei bzw. durch Blinken) bei Statusveränderung des zu überwachenden Objektes.
- Direkter Start des OpenScape FM Clients mit automatischem Login.

Die Tray Bar Überwachung stellt den Zustand eines für den aktuellen Anwender des Desktop Clients definierten OpenScape FM Objektes (dem Überwachungsobjekt) mit Hilfe eines Tray Bar Symbols dar.

Das Tray Bar Symbol wird für das konfigurierte Überwachungsobjekt angezeigt sobald der Desktop Client gestartet wird. Dabei können die folgenden Symbole abhängig vom Status des Überwachungsobjektes angezeigt werden:

Erscheinungsbild	Kategorie	Status
	Alarm	Critical → rot
	Alarm	Major → orange
	Warnung	Minor → gelb
	Warnung	Warning → hellblau
	Ok	Normal → grün
	Ok	Disabled → dunkelbraun
	Ok	Restricted → braun
	Ok	Testing → lachsfarben
	Ok	Unknown → blau
	Ok	Unmanaged → hellbraun
	Ok	Unset → hellgrau

Ein beliebiges OpenScape FMObjekt wird für die Überwachung durch das Tray Bar Symbol festgelegt, indem aus seinem Kontextmenü der Eintrag **Bearbeiten->Überwachungsobjekt zuweisen** ausgewählt wird. Dies beendet die Überwachung des bisher ausgewählten Objektes und started die Überwachung des aktuellen Objektes durch das Tray Bar Symbol.

Wird vom Anwender kein Objekt zugewiesen, wird standardmäßig der Container *Persönliche Sicht* des Anwenders überwacht.

Das Tray Bar Symbol wird automatisch angelegt, wenn ein Desktop Client geöffnet wird, und standardmäßig geschlossen, wenn der Client beendet wird.

Wird in den allgemeinen Einstellungen (Eintrag **Client->Einstellungen** der Hauptmenüleiste) der Haken vor **Schließen minimiert in den System Tray** aktiviert, so beendet ein Schließen des Clients diesen nicht, sondern macht ihn lediglich unsichtbar während das System Tray Symbol erhalten bleibt.

Über das Eingabefeld **Alarmton für Überwachungsobjekt** und die zugehörige Schaltfläche **Auswählen** kann über einen Datei-Browser eine Sound-Datei ausgewählt werden. Diese wird immer dann abgespielt, wenn sich der Status des vom Tray Bar überwachten Objektes verschlechtert, also sich beispielsweise von *Normal* nach *Minor*, oder von *Warning* nach *Critical* ändert.

Das Tray Bar Symbol selbst bietet drei Funktionen über Menüeinträge an:

- **OpenScape FM Fault Management Client** öffnet den zu dem Symbol gehörenden Desktop Client.
- **Details** zeigt ein Übersichtfenster mit der aktuellen Konfiguration an.
- **Beenden** schließt das Symbol und beendet den zugehörenden Desktop Client.

10 Drucken

Der Desktop bietet Ihnen zwei verschiedene Druckoptionen. Sie können die aktuell angezeigte Submap drucken oder Sie können die Druckoption des Listen-Browsers verwenden. Beide Funktionen werden über die Schaltfläche **Drucken** aktiviert, die sich unter den zusätzlichen Steuerelementen des Submap/Info-Ansichtsbereichs befindet.

Bild 12 Die Schaltfläche „Drucken“

10.1 Drucken aus einer Submap heraus

Wenn Sie die Druckoption aus einer Submap heraus starten, wird über die entsprechende Schaltfläche der Standard-Druckdialog Ihres Betriebssystems geöffnet, in dem Sie die Druckparameter festlegen können.

10.2 Drucken aus dem Info-Browser heraus

Wenn Sie die Druckfunktion eines Info-Browsers nutzen, stehen Ihnen zusätzliche speziellere Optionen zur Verfügung.

Verwenden Sie zum Ausdrucken von Daten aus Info-Browsern (z. B. Alarm-Browser oder Discovery-Browser) die Schaltfläche Drucken im oberen Teil des Info-Browsers. Im dem sich daraufhin öffnenden Druckmenü (Bild 13) stehen Ihnen etliche Konfigurationsparameter zur Verfügung.

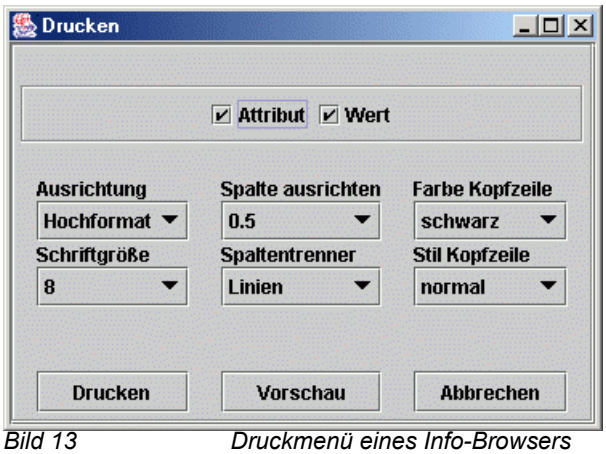


Bild 13 Druckmenü eines Info-Browsers

In der obersten Zeile können Sie festlegen, welche Spalten ausgedruckt werden sollen. Im mittleren Teil des Druckmenüs können Sie das Erscheinungsbild Ihres Ausdrucks bestimmen, wie beispielsweise den Spaltenabstand oder die Farbe der Spaltentitel. Sie können sich vor dem Drucken eine Vorschau anzeigen lassen. Dies erreichen Sie über die Schaltfläche **Vorschau**. *Bild 14* zeigt den Druckvorschau-Dialog für die „Objekt Eigenschaften“. Da ihr Ausdruck mehrere Seiten umfassen kann, wird in der rechten Ecke der Vorschau die

aktuelle Seite und die Seitenanzahl angezeigt. Zusätzlich können Sie durch die einzelnen Seiten blättern. Dazu benutzen Sie die Pfeile in der Mitte der Dialog-Toolbar. Über die Zoom-Auswahl im Vorschau-Dialog können Sie die Anzeigegröße Ihres Dokuments festlegen. Dazu stehen die Zoom-Faktoren **10%**, **25%**, **50%**, **75%** oder **100%** zur Verfügung.

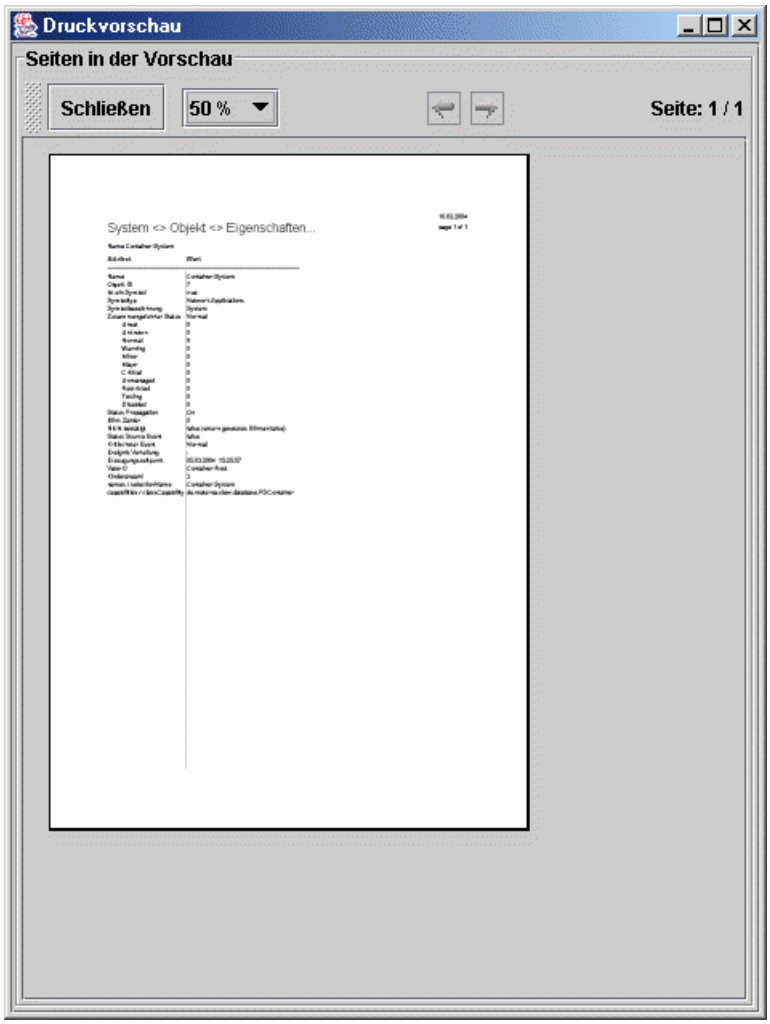


Bild 14 *Druckvorschau, hier Objekt Eigenschaften*

Wenn Sie die Daten so drucken möchten wie sie in der Vorschau dargestellt sind, klicken Sie auf **Drucken** im **Druckmenü** (*Bild 13*). Um die Druckfunktion nutzen zu können, muss an Ihrem Computer zunächst ein Drucker eingerichtet werden.

11 Anwendersitzungen

Mit Hilfe von Anwendersitzungen kann überwacht werden, welche Anwender gerade aktiv sind. Dies ist ein interner Prozess. Anwendersitzungen ermöglichen eine Kontrolle der Zugriffsrechte (*Kapitel 15, „Zugriffsrechte“*) und der Anwendersprache sowie die Funktionsüberwachung der Client-Verbindung.

11.1 Grundlagen: Anwendersitzungen

Wenn ein Anwender den Client startet, wird eine Sitzung zwischen dem Client und dem Server eingerichtet. Diese Sitzung ist durch eine „Sitzungskennung“ eindeutig identifiziert.

11.2 Login

Die Sitzungskennung wird im Rahmen des Login-Vorgangs zugewiesen und gilt so lange, bis sich der Anwender wieder abmeldet. Mit Hilfe entsprechender Mechanismen wird die Verbindung zwischen dem Client und dem Server überwacht. Stoppt der Client unerwartet, wird dies serverseitig automatisch erkannt und die für diesen Client reservierten Ressourcen werden wieder freigegeben.

Wenn Sie sich am Server anmelden möchten, benötigen Sie dafür Ihren Login-Namen und Ihr Passwort. Das Ursprungspasswort kann vom Administrator bei der Erstellung des Anwenderkontos festgelegt werden, *Kapitel 14, „Anwender- und Gruppenverwaltung“*.

Hat der Administrator bei der Erstellung des Anwenderkontos die Option **Leer bis zum ersten Login** aktiviert, muss der Anwender beim ersten Login ein Passwort festlegen. Die beiden anderen Parameter mit Einfluss auf die Geltungsdauer von Passwörtern sind **Min. Zeit** und **Max. Zeit**, die auch vom Systemadministrator festgelegt werden. Einzelheiten unter *Kapitel 14, „Anwender- und Gruppenverwaltung“*

11.3 Zeitabhängiges Login/Logout

Ist ein Anwender zeitlich eingeschränkt, so kann er sich nur während der für ihn definierten Zeitintervalle einloggen. Außerdem wird ein derartiger Anwender automatisch ausgeloggt, sobald das ihm zugewiesene Zeitintervall überschritten wird. Ist für den Anwender das automatische Login aktiviert und wurde zuletzt ein automatisches Logout ausgeführt, so wird der Anwender automatisch zum nächstmöglichen erlaubten Zeitpunkt eingeloggt.

Mehr über zeitkontrolliertes Login/Logout findet sich in *Abschnitt 14.1.3, „Zeitabhängiges Login/Logout“*.

11.4 Logout

Um sich vom System abzumelden, wählen Sie **Client->Logout** aus dem Hauptmenü. Wenn sich ein Anwender ordnungsgemäß abmeldet, wird die Anwendersitzung normal beendet.

Anwendersitzungen

Logout

12 Erstellen individueller Ansichten

Sie sind bei Ihrer Arbeit nicht nur auf die von den Applikationen automatisch generierten Ansichten (d. h. Submaps und Bäume/Unterabschnitte) beschränkt. Mit dem Desktop können Sie auch Ihre eigenen Ansichten erstellen.

Objekt Container

Für jedes anwenderseitig generierte Symbol einer Submap ist der Menüeintrag **Neu->Objekt Container** verfügbar.

Mit Hilfe dieses Eintrages können Sie eigene Submap-Hierarchien einrichten. Wir beginnen auf der Root-Submap. Nur hier können Sie das erste Objekt als Root Ihres individuellen Submap-Bäume erzeugen. Sie können normalerweise keine Objekte auf Submaps erzeugen, die von Applikationen erstellt wurden. Verwenden Sie im Folgenden die Funktion **Neu->Objekt Container**, um ein vollkommen neues Objekt in die Datenbank aufzunehmen. Oder verwenden Sie die Option **Kopieren/Einfügen**, um ein bestehendes Objekt in eine andere Submap einzufügen. Sie können neue Objekte erzeugen und bestehende Objekte hinzufügen, um eine individuelle Netzwerkansicht einzurichten (z. B. eine Ansicht für bestimmte Systeme, die Sie im Auge behalten möchten). Sie können auch den Hintergrund für Ihre Submaps anpassen (*Abschnitt 5.8, „Hintergrundbild wählen“*). Für jedes anwenderdefinierte Objekt können Sie angeben, ob der Status des Objektes übertragen werden soll oder nicht. Verwenden Sie dazu das Kontrollfeld **Status-Propagierung**.

Wenn Sie das Erscheinungsbild einer Submap ändern, sind die neuen Einstellungen sofort für alle angemeldeten Anwender sichtbar, die gerade mit dieser Submap arbeiten.

Virtuelle Container

Während den zuvor beschriebenen Objekt-Containern die Objekte manuell hinzugefügt werden müssen, verfügen Virtuelle Container über die Fähigkeit, ihren Inhalt zur Laufzeit des OpenScape FM dynamisch zu ermitteln. Dies geschieht anhand von dem jeweiligen Container zugeteilten Regeln.

Virtuelle Container können über den Menüeintrag **Neu->Virtueller Container** erstellt werden.

Mehr über Virtuelle Container findet sich in der gesonderten *Control Center Bedienungsanleitung* ab Kapitel 4.

12.1 Versteckte Objekte

Das Erscheinungsbild einer Sicht kann auch dadurch verändert werden, dass einzelne Symbole bzw. Objekte versteckt werden können. Dies bedeutet, dass die entsprechenden Symbole nicht länger dargestellt werden. Ereignisse für versteckte Objekte werden weiterhin empfangen und im Ereignis-Browser dargestellt.

Versteckte Symbole können auf Wunsch wieder dargestellt werden.

Es stehen die folgenden Aktionen zu Verfügung:

- **Verstecken:**
  - Einzelne Symbole können über das Kontextmenü des betreffenden Symbols (**Bearbeiten->Verstecken**) versteckt werden.

  - Alle Symbole, die das gleiche Objekt repräsentieren, können über die Schaltfläche **Verstecken** in der Objektsuche versteckt werden.

- **Anzeigen:**
  - Alle Symbole, die auf einer Submap versteckt sind, können über das Kontextmenü der Submap oder des übergeordneten Objektes (**Bearbeiten->Zeige Versteckte Objekte**) sichtbar gemacht werden.
  - Alle versteckten Symbole, die das gleiche Objekt repräsentieren, können über die Objektsuche sichtbar gemacht werden (Schaltfläche **Anzeigen**).

13 Symbole und Statusanzeige

Objekte repräsentieren in der Regel real existierende (virtuelle) Objekte, die vom OpenScape FM überwacht werden. Diese Objekte werden in den Ansichten (Submaps und/oder Bäume) durch Symbole dargestellt. Dabei ist es normal, dass ein Objekt durch mehrere Symbole repräsentiert wird. So kann z.B. ein Host, der über mehrere Interfaces verfügt, durch Symbole in verschiedenen Netzwerken repräsentiert sein. Unabhängig davon auf welchem dieser Symbole eine Funktion ausgelöst wird, wirkt diese immer auf das gleiche interne Host-Objekt.

Im Allgemeinen beschreiben der **Umriss** und des **Bild** eines Symbols den Typ des repräsentierten Objektes, der darunter befindliche **Bezeichner** identifiziert das Objekt selbst, und die **Farbe** des Symbols zeigt den aktuellen Status des Objektes.

Die ersten Abschnitte dieses Kapitels beschäftigen sich mit dem Erscheinungsbild der Symbole:

- *Abschnitt 13.1* zeigt einige Standard-Symbol-Optiken, die das OpenScape FM Desktop automatisch den Symbolen zuweist, die einen bestimmten Objekttyp repräsentieren.
- *Abschnitt 13.2* zeigt, wie der Symbol-Typ und der Bezeichner bei Bedarf für jedes Symbol individuell angepasst werden können.

Die folgenden Abschnitte beschreiben, wie der Status von Objekten berechnet und die Berechnung konfiguriert werden kann, und wie der Status der Objekte und weitere Informationen über die Symbole dargestellt werden:

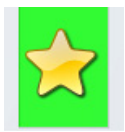
- *Abschnitt 13.3* beschreibt, wie der Status eines Objektes berechnet wird, und wie die Berechnungsmethode für einzelne Objekte angepasst werden kann.
- *Abschnitt 13.4* gibt an, wie die Verteilung des Status der Kindobjekte eines Symbols dargestellt wird.
- *Abschnitt 13.5* zeigt, wie neben dem Objektstatus zusätzlich die Erreichbarkeit eines Objektes dargestellt wird.
- *Abschnitt 13.6* zeigt, wie Symbole auf ihrer Submap um ein Informationsfenster erweitert werden können.

13.1 Symbol-Optiken

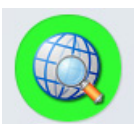
Dieser Abschnitt gibt einen kurzen Überblick über die vom Desktop standardmäßig verwendeten Symbole. Die Beschreibung der Plugin spezifischen Symbole findet sich in den jeweiligen Handbüchern.

13.1.1 Standardsymbole

- Anwendersymbol 

- Gruppensymbol 
- Rechtesymbol 
- Domänensymbol 
- Favoritensymbol 

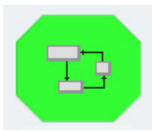
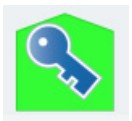
13.1.2 Topologiesymbole

- Netzwerksymbol 
- Teilnetzwerksymbol 
- Meta-Kanten-Symbol (Baumansicht) 

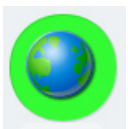
13.1.3 Protokollsymbole

- Protokollsymbol 
- Protokolldatei-Ansichtssymbol 

13.1.4 Systemsymbole

- Systemsymbol 
- Hilfesymbol 
- Startup Manager-Prozess-Symbol 
- License Manager-Symbol 

13.1.5 Mapsymbole

- Map Manager 
- Map-Symbol 

13.2 Symbol-Konfiguration

Das Erscheinungsbild jedes Symbols kann individuell über das zugehörige Kontextmenü geändert werden. Dabei kann der Umriss, das Bild und der Bezeichner jedes Symbols einzeln festgelegt werden.

Hinweis:
Bei Systemsymbolen ist dies jedoch nur bedingt zu empfehlen, da dies das Auffinden der Symbole erschweren könnte.

Die Konfiguration eines Symbols kann über den Kontextmenü-Eintrag **Eigenschaften** angestoßen und auf der Seite **Symbol->Symbol-Eigenschaften** durchgeführt werden.

Das Konfigurationsfenster besteht aus drei identisch aufgebauten Teilbereichen, in denen jeweils in der oberen Zeile der **Umriss** und das **Bild** und in der unteren Zeile der **Bezeichner** festgelegt werden können.

Beim Öffnen des Fensters werden die aktuell angezeigten Bezeichner angezeigt. Wird ein Bezeichner durch ein Makro bestimmt, so wird er in hellgrau statt schwarz dargestellt, um dies kenntlich zu machen.
Wird in das entsprechende Feld geklickt, wird das Makro selbst angezeigt.

Der untere der drei Bereiche definiert alle Symbole, die das ausgewählte Objekt repräsentieren, der mittlere Bereich definiert alle Symbole, die das ausgewählte Objekt in der aktuellen Map repräsentieren, und der obere Bereich definiert nur das Symbol, aus dessem Kontextmenü der Aufruf erfolgte.

Werden die Schaltfläche **OK** oder **Übernehmen** betätigt, werden alle Zeilen ausgewertet, deren Checkbox mit einem Haken versehen ist.

Soll eine Konfiguration auf die Standardeinstellung zurückgesetzt werden, muss ein leerer Eintrag mit markierter Checkbox übergeben werden.

Speziellere Konfigurationen überschreiben gegebenenfalls die allgemeineren. Wird also z.B. der erste und der letzte Bereich ausgefüllt, wird das aktuelle Symbol gemäß des oberen Bereichs angezeigt, und alle weiteren Symbole für das gleiche Objekt gemäß des unteren Bereichs.

Soll nur der Bezeichner geändert werden, kann dies auch vereinfacht über die Auswahl des Symbols in einer Submap oder im Baum durch drücken der Taste F2, oder über den Eintrag **Umbenennen** aus dem Kontextmenü des Symbols erfolgen.

13.3 Statusermittlung

Der Status eines Objektes beschreibt in der Regel, in welchem Zustand sich das Objekt aktuell befindet. Liegen z.B. keine Probleme vor, ist der Zustand ‚*Normal*', gibt es aktuell kritische Probleme, ist auch der Status ‚*Kritisch*'. Welcher Status aktuell anliegt, wird über die Farbe der Symbole dargestellt, die das entsprechende Objekt repräsentieren. Die Bedeutung der einzelnen Farben ist in *Abschnitt 5.11* beschrieben.

Um einen Hinweis darauf zu bekommen, warum sich ein Symbol in einem bestimmten Status befindet, kann der Menüeintrag **Statuserklärung** aus dem Kontextmenü eines Symbols aufgerufen werden. Dieser öffnet ein Informations-Fenster, das den Status des Symbols erklärt. Wenn der Status durch andere Objekte (zusammengesetzter Status) und entsprechende Ereignisse definiert ist, enthält das Fenster eine Liste von Objekten und Ereignissen, die für den aktuellen Status verantwortlich sind (siehe *Abschnitt 5.17*).

Im allgemeinen ergibt sich der Status für Objekt-Symbole aus dem schlimmsten nicht bestätigten Ereignis, das dem Objekt zugewiesen ist. Der Status von Objekt-Container-Symbolen ergibt sich aus dem schlimmsten Status eines Kind-Objektes.

Für individuelle Objekte kann jedoch festgelegt werden, wie der Status des Objektes berechnet werden soll, bzw. wie der Status des Objektes sich auf andere Objekte auswirken soll. Die Statuskonfigurationsseite kann über den Eintrag **Eigenschaften...** aus dem Kontextmenü des entsprechenden Objektes geöffnet werden. Sie befindet sich auf der Karteikarte **Propagation**. Die Karte besteht aus vier Unterseiten.

Väter:

Die Unterseite **Väter** enthält eine Auflistung aller Objekte, an die das aktuelle Objekt seinen Status weitergeben könnte. Diese Liste ergibt sich aus der aktuellen Struktur des Objektbaums.

Die Spalte **Objekt** identifiziert den jeweiligen Vaterknoten.

Die Spalte **Propagationsgewicht** definiert die absolute Gewichtung, mit der das Objekt für den Vater berücksichtigt werden soll. Ein Wert von 0 lässt das Objekt unberücksichtigt.

Die Spalte **Propagationsart** legt fest, ob nur das Objekt selbst (**Objekt**) oder auch alle Kindobjekte (**Hierarchisch**) berücksichtigt werden sollen.

Kinder:

Die Unterseite **Kinder** entspricht der Unterseite Väter. Hier werden jedoch alle Objekte aufgelistet, die sich auf den Status des aktuellen Objektes auswirken können.

Statusberechnung:

Auf der Unterseite **Statusberechnung** kann im Auswahlmenü **Statusberechnungsmethode** festgelegt werden, wie der Status des aktuellen Objektes bestimmt werden soll.

Grundlegend gibt es drei verschiedene Ansätze zur Berechnung des Objektstatus:

1. Der Status wird vom OpenScape FM unmittelbar dem Objekt zugewiesen. Alle anderen Einflüsse auf das Objekt werden ignoriert.

   Für diese Methode muss der Eintrag **Objekt** ausgewählt werden.

   Diese Methode wird z.B. für IP-Knoten bis einschließlich OpenScape FM V10 automatisch durch das OpenScape FM gesetzt, die nicht erreichbar sind. Sind sie später wieder erreichbar, ändert sich die Methode automatisch auf das *Maximum der Kindobjekte*. Die Methode *Objekt* sollte im Regelfall nicht manuell gesetzt werden.

2. Der Status bestimmt sich aus dem höchsten Status der nicht bestätigten Ereignisse, die dem Objekt direkt zugewiesen sind.

   Für diese Methode muss der Eintrag **Ereignis** ausgewählt werden.

3. Der Status bestimmt sich aus dem Status der Kindobjekte des Objektes.

   In diesem Fall gibt es die folgenden Methoden:

   - **Maximum der Kindobjekte**, **Minimum der Kindobjekte**: Der Status ergibt sich aus dem höchsten bzw. niedrigsten Status aller Kindobjekte, die nicht das Propagationsgewicht 0 besitzen.
   - **Absoluter Schwellwert**, **Prozentualer Schwellwert**: Der Status berechnet sich aus der absoluten bzw. prozentualen Verteilung der Kindobjekt-Statuswerte. Wie der Status genau berechnet wird, kann auf der Unterseite **Schwellwerte** festgelegt werden.
   - **Abgeleitet**: Der Status wird nach der Default-Methode ermittelt. Diese berücksichtigt die Anzahl der Kindobjekte, die sich im *Normal* Status befinden und die Anzahl der Kindobjekte die sich in einem fehlerbehafteten Status (*Critical*, *Major*, *Minor* oder *Warning*) befinden.

Der Status wird wie folgt berechnet:

- **Unknown**: kein Objekt fehlerbehaftet, kein Objekt *Normal*.
- **Normal**: kein Objekt fehlerbehaftet, mindestens ein Objekt *Normal*.
- **Warning**: genau ein Objekt fehlerbehaftet, mindestens zwei Objekte *Normal*.
- **Minor**: mindestens zwei Objekte fehlerbehaftet, mindestens zwei Objekte *Normal*.
- **Major**: mindestens ein Objekt fehlerbehaftet, genau ein Objekt *Normal*.
- **Critical**: mindestens ein Objekt fehlerbehaftet, kein Objekt *Normal*.

Schwellwerte:

Die Unterseite **Schwellwerte** legt fest, wie der Status festgelegt werden soll, falls die **Statuszusammenfassung** den absoluten oder prozentualen Schwellwert verwenden soll.

Jede Zeile der Unterseite definiert eine Regel für den jeweiligen **Status**. Dabei findet die Auswertung in der Reihenfolge der **Auswertungspriorität** statt, beginnend mit der höchsten Priorität.

Eine Regel ist zutreffend, wenn mindestens so viele Objekte den jeweiligen Status oder einen höherwertigen Status besitzen, wie in der Spalte **Schwellwert** gefordert werden. Je nach Auswahl der Statuszusammenfassung werden hier absolute bzw. prozentuale Zahlen, jeweils unter Berücksichtigung der Propagationsgewichte, für die Auswertung verwendet. Die erste zutreffende Regel legt den Status des Objektes fest.

Die Spalte **Aktueller Wert** zeigt an, wieviele Objekte gewichtet aktuell den jeweiligen Status (absolut bzw. in Prozent) besitzen.

Beispiel (Statuszusammenfassung: Prozentualer-Schwellwert, Default-Einstellungen für die Schwellwerte):

- Das Objekt bekommt den Status *Critical*, falls sich mindestens 5% (gewichtet) der Kindobjekte im Status *Critical* befinden.
- Das Objekt bekommt den Status *Major*, falls sich mindestens 10% (gewichtet) der Kindobjekte im Status *Major* oder *Critical* befinden.
- Das Objekt bekommt den Status *Minor*, falls sich mindestens 20% (gewichtet) der Kindobjekte im Status *Minor*, *Major* oder *Critical* befinden.
- ...

Mit Hilfe der **Schwellwerte** ist es möglich, dass ein Objekt einen Status annimmt, der weder von einem Ereignis noch von einem Kindobjekt angenommen wird. Legt man z.B. für den Status *Critical* 80% und für den Status *Major* 60% fest, wird z.B. der Status *Major* angenommen, falls sich 60% der Kinder im Status *Critical* befinden. Auf diese Weise kann auf den Teilweisen Ausfall von (redundanten) Kindobjekten flexibel reagiert werden.

13.4 Gesamtstatusanzeige

Die Farbe eines Map-Symbols signalisiert den aktuellen Status des zugehörigen Objekts. Hierbei kann es sich um einen Einzelstatus oder um einen zusammengesetzten Status handeln.

Ein Einzelstatus steht für den Status dieses bestimmten Objektes. So wird zum Beispiel ein Objekt als kritisch dargestellt, wenn für das Objekt selbst ein kritisches Ereignis vorliegt.

Ein zusammengesetzter Status liegt vor, wenn sich der Status eines Objektes aus dem Status der Objekte auf seiner Submap ergibt. Ein Netzwerk-Objekt kann zum Beispiel als kritisch angezeigt werden, wenn ein in diesem Netzwerk befindliches System den Status kritisch annimmt.

Wie der Status eines Objektes bestimmt werden soll, kann für Objekte individuell angepasst werden (siehe *Abschnitt 13.3, „Statusermittlung“*).

Wenn nicht alle untergeordneten Objekte eines Objektes den gleichen Status aufweisen, erscheint die Gesamtstatusanzeige neben dem Submap-Symbol (*Bild 15*). Sie zeigt einen Prozentsatz der Objekte, die sich in dem angezeigten Status befinden. Diese Relation bezieht sich auf den gesamten Objekt-Unterabschnitt in der Hierarchie und nicht nur auf die nächste dem Symbol untergeordnete Ebene. Ist beispielsweise eine Gesamtstatusanzeige sichtbar wie in *Bild 15* zu sehen, erkennt man, dass sich im Netzwerk eine bestimmte Anzahl von verwalteten Objekten in einem „kritischen“ Status befinden. Im Beispiel sind dies etwa die Hälfte aller verwalteten Objekte.

Hinweis:
Die Gesamtstatusanzeige berücksichtigt nur Symbole von Objekten, die sich in der Baumstruktur unterhalb des betrachteten Objektes befinden. Referenzsymbole (siehe *Abschnitt 16.2.2*) stehen für Objekte, die sich außerhalb einer angezeigten Submap befinden. Sie werden bei der Bestimmung der Gesamtstatusanzeige daher *nicht* berücksichtigt. Referenzsymbole können leicht durch ihre in << >> Klammern eingeschlossenen Bezeichner erkannt werden.

Bild 15 Netzwerksymbol mit Gesamtstatusanzeige

Über die Gesamtstatusanzeige des „Anwender“-Symbols kann beispielsweise erkannt werden, wie viele Anwender angemeldet waren:

- Grüne Anwendersymbole stehen für angemeldete Anwender.
- Blaue Anwendersymbole stehen für nicht angemeldete Anwender.
- Hellblaue Symbole zeigen einen fehlgeschlagenen Login-Vorgang an.

13.5 Erreichbarkeitsstatus

Jedes überwachte Objekt besitzt neben dem zuvor beschriebenen Status (siehe *Abschnitt 13.3*) einen **Erreichbarkeitsstatus**. Dieser gibt in der Regel an, ob das Objekt selbst zur Zeit erreichbar ist oder nicht.

Ein Objekt ist z.B. nicht erreichbar, wenn es innerhalb eines vorgegebenen Zeitintervalls nicht auf einen Ping antwortet.

Weicht der Status vom Erreichbarkeitsstatus ab, so wird der Erreichbarkeitsstatus rechts oberhalb des Objektsymbols als farbiger Punkt dargestellt (siehe *Bild 16*).

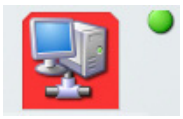


Bild 16 Erreichbarkeitsstatus

Der Host im obigen Bild besitzt einen ausgefallenen Dienst und wird daher im Status *Critical* dargestellt.

Da der Host selbst aber auf Pings reagiert, besitzt er den Erreichbarkeitsstatus *Normal*.

Umgekehrt würde ein ausgeschalteter PC ohne sonstige gemeldete Probleme mit dem Status *Normal* und dem Erreichbarkeitsstatus *Critical* dargestellt.

Da für die Objekte einiger Technologien der Erreichbarkeitsstatus individuell berechnet wird, sollte im Zweifelsfall auf die Statuserklärung des betreffenden Objektes zurückgegriffen werden (siehe *Abschnitt 5.17*).

Ein Netzwerk gilt als nicht erreichbar, wenn keines der Numbered Router Interfaces, die innerhalb des Netzwerkes bekannt sind, erreicht werden kann. In diesem Fall erhält das Netzwerk den Erreichbarkeitsstatus *Critical*. Zusätzlich geht in diesem Fall das OpenScape FM davon aus, dass die Nicht-Erreichbarkeit der enthalten Objekte durch das Netzwerk begründet ist. Diese erhalten deswegen *nicht* ebenfalls den Erreichbarkeitsstatus *Critical,* sondern so lange den Erreichbarkeitsstatus *Unknown* bis wieder mindestens eines der Numbered Interfaces des Netzwerkes erreicht werden kann.

13.6 Symbole als Fenster

Ist das Control Center Plugin initialisiert und lizenziert, können Symbole um ein Informationsfenster erweitert werden, das auf der gleichen Submap wie das Symbol angezeigt werden kann.

Ist für ein Symbol ein derartiges Fenster eingerichtet worden, kann es durch ein Fenstersymbol, welches in der rechten oberen Ecke des Symbols angezeigt wird, geöffnet und anschließend mit den üblichen Methoden verschoben und in der Größe angepasst werden.

Ob ein Fenster angelegt werden soll und welche Informationen es enthalten soll, kann über den Eintrag **Eigenschaften...** aus dem Kontextmenü des entsprechenden Symbols festgelegt werden. Die entsprechende Konfiguration findet sich auf der Karteikarte **Symbol als Fenster** und der Inhalt des Fensters kann im gleichnamigen Auswahlmenü festgelegt werden.

Wird ein Fensterinhalt festgelegt, ändert sich die Optik des Symbols entsprechend der Auswahl.

Soll kein Fenster mehr für das entsprechende Symbol angezeigt werden, kann dies über die Auswahl **Symboldarstellung zurücksetzen** erreicht werden.

14 Anwender- und Gruppenverwaltung

Der OpenScape FM Desktop bietet Verwaltungsfunktionen für die Durchführung anwenderbezogener Aufgaben wie Passwort-Änderungen, die Einrichtung neuer Anwenderkonten, die Erstellung neuer Anwendergruppen sowie die Zuweisung individueller Zugriffsrechte für Anwender/Anwendergruppen. Dieses Kapitel beschäftigt sich mit der Erstellung und Administration von Anwenderkonten und Anwendergruppen. Die Zuordnung und Konfiguration von Rechten wird in *Kapitel 15, „Zugriffsrechte“* beschrieben.

Der Startpunkt für die Anwender- und Gruppenverwaltungs-Administration ist das „Anwender Verwaltung“ Symbol der Root-Sicht. Auf der diesem Symbol untergeordneten Sicht sind die „Anwender“, „Gruppen“ und „Rechte“ Symbole angeordnet. Dem „Anwender“ Symbol sind die Funktionen zur Verwaltung einzelner Anwender untergeordnet. Das „Gruppen“ Symbol fasst die Funktionen der Gruppenverwaltung zusammen und das „Rechte“ Symbol dient als Sammelobjekt für alle definierten Rechte.

Bild 17 Die Root-Submap

Die Anwender-Verwaltung kann auch unmittelbar über den Hauptmenüeintrag **Server->Administration->Anwender Verwaltung...** geöffnet werden.

14.1 Anwender

Die Anwendersymbole befinden sich in der Ansicht **Anwender**. Für jeden im System definierten Anwender wird ein eigenes Symbol angezeigt. Über das Kontextmenü des jeweiligen Anwender-Symbols können die Konfigurationseinstellungen für diesen Anwender geändert oder das Anwenderkonto vollständig aus dem System entfernt werden.

Im Einzelnen sind folgende Operationen möglich:

- **Passwort:**
  - **Ändern...:** Hier kann das Passwort für einen bestimmten Anwender geändert werden. Ohne Administrator-Zugriffsrechte ist diese Option nur für den aktuell angemeldeten Anwender verfügbar. Ein Anwender kann sein Passwort auch über den Hauptmenüeintrag **Client->Passwort Ändern...** ändern.
  - **Änderungen erzwingen / Änderung nicht erzwingen:** Als Anwender mit Administratorrechten kann erzwungen werden, dass bestimmte Anwender beim nächsten Login ein neues Passwort festlegen bzw. einen solchen Zwang wieder aufheben müssen.
  - **Löschen:** Als Administrator kann das Passwort von bestimmten Anwendern gelöscht werden. So werden diese gezwungen, beim nächsten Login ein neues Passwort zu vergeben.

- **Anwender sperren/Anwender freigeben:** Mit Hilfe dieser Option kann ein Anwenderkonto vorübergehend gesperrt bzw. wieder freigeben werden. Für diese Operation sind Administrator-Zugriffsrechte erforderlich.
- **Konfigurieren:**
  - **Information:** Die angezeigte Seite enthält Anwenderdaten, die bei der Kontoeinrichtung angegeben wurden. Die hier angezeigten Anwenderinformationen können geändert werden. Diese Seite entspricht im Wesentlichen der Seite für die Definition neuer Anwender (siehe *Abschnitt 14.1.1*).
  - **Objektrechte:** In der angezeigten Seite können anwenderspezifische Objektrechte zugewiesen werden. Siehe hierzu auch *Abschnitt 15.7.1, „Zuweisen neuer Objektrechte“*.
  - **Domänenrechte:** In der angezeigten Seite können anwenderspezifische Domänenrechte zugewiesen werden. Siehe hierzu auch *Abschnitt 15.8.5, „Zuweisung von Domänenrechten“.*

  Wichtiger Hinweis:
  Beide Rechte-Seiten zeigen nur die Rechte an, die *unmittelbar* dem Anwender zugewiesen wurden. Rechte, die über die Mitgliedschaft in Gruppen erteilt wurden, werden hier nicht angezeigt.

14.1.1 Einrichten eines neuen Anwenderkontos

Die **Anwender**-Submap wird für alle anwenderbezogenen Verwaltungsaufgaben benötigt, die sich auf einen einzelnen Anwender beziehen. Sie können die Anwender-Submap durch einen Doppelklick auf das Anwendersymbol in der Submap des Anwender Verwaltung-Symbols öffnen.

Die Anwender-Submap besitzt den Eintrag **Neu->Anwender** in ihrem Kontextmenü. Dieser Befehl öffnet eine Eingabemaske für die Erfassung der neuen Anwenderdaten (*Bild 18*), die sich auf dem Reiter **Informationen** befindet.

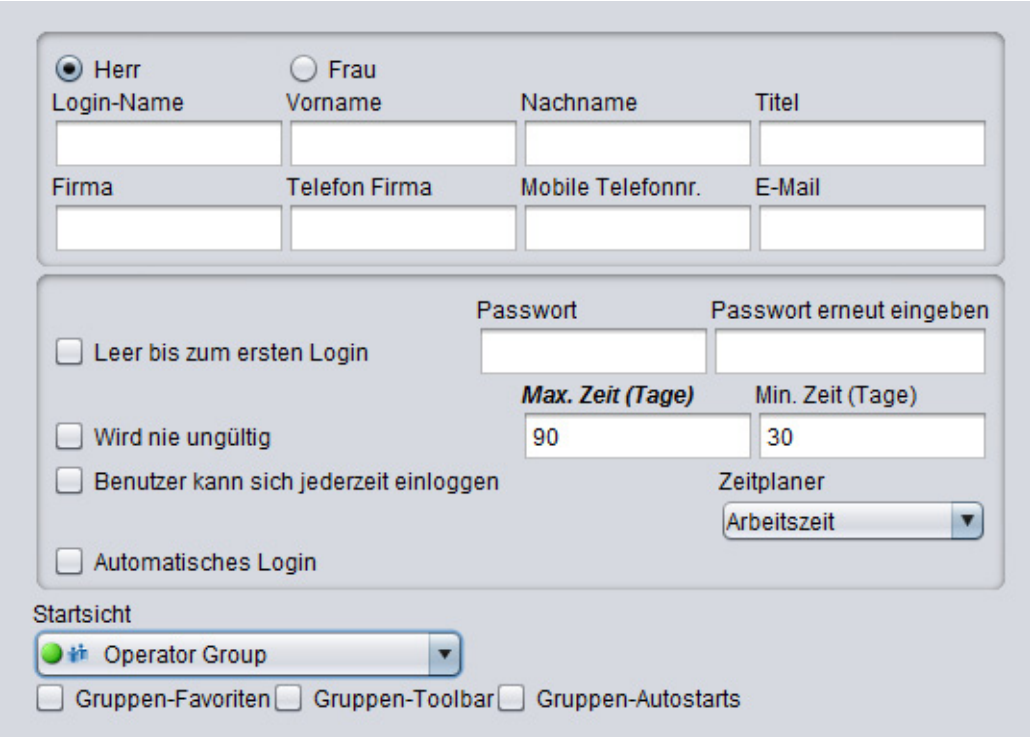


Bild 18 Hinzufügen eines neuen Anwenders

Felder:

- **Login Name**, **Vorname**, **Nachname**, **Titel:** geben Sie hier die erforderlichen Daten ein.
- **Firma**, **Telefon Firma**, **Mobile Telefonnr.**, **E-Mail:** geben Sie hier die erforderlichen Daten ein.
- **Passwort**, **Passwort erneut eingeben:** Eingeben und Bestätigen eines Passworts. Um 'unsichere' Passwörter zu verhindern, müssen die Passwörter einigen Richtlinien genügen (siehe dazu *Abschnitt 14.1.2, „Passwort-Richtlinien“*).
- **Max. Zeit:** maximale Anzahl von Tagen, nach denen das Passwort ungültig wird. Nach Ablauf dieser Zeitspanne muss der Anwender ein neues Passwort festlegen.
- **Min. Zeit:** minimale Gültigkeitsdauer des Passworts. Vor Ablauf dieser Zeitspanne kann der Anwender selbst das Passwort nicht ändern.

Kontrollfelder:

- **Leer bis zum ersten Login:** Das Passwort-Feld bleibt leer. Beim ersten Login muss der Anwender ein Passwort festlegen.
- **Wird nie ungültig:** Das für den Anwender vergebene Passwort bleibt dauerhaft gültig. Es kann jedoch auch jederzeit vom Anwender oder vom Administrator geändert werden.
- **Benutzer kann sich jederzeit einloggen:** Der Anwender kann sich jederzeit einloggen. Befindet sich kein Haken in diesem Kontrollfeld, so tritt das zeitabhängige Login/Logout in Kraft. Mehr darüber und zum **Automatischen Login** findet sich in *Abschnitt 14.1.3, „Zeitabhängiges Login/Logout“*.

Startsicht

Das Auswahlmenu und die darunter befindlichen Kontrollfelder legen fest, ob für den aktuellen Anwender die Einstellungen für die Favoriten (siehe *Abschnitt 5.15*), den Toolbar (siehe *Abschnitt 5.15.2*) und den Autostart des Anwenders (siehe *Abschnitt 5.15.1*) individuell für den Anwender festgelegt werden sollen, oder ob die Festlegung über eine ausgewählte Gruppe (siehe *Abschnitt 14.2*) erfolgen soll.

Im Auswahlmenü kann dazu dem Anwender eine **Startsicht** zugewiesen werden. Dabei kann es sich um den *Root*-Knoten des Navigationsbaum, die individuelle Sicht des *Anwenders*, oder um eine beliebige definierte Gruppe handeln.

Wird eine Gruppe ausgewählt, so sind die Kontrollfelder **Gruppen-Favoriten**, **Gruppen-Toolbar** und **Gruppen-Autostarts** aktiv.

Ist dies der Fall, so werden bei *unmarkiertem* Feld die Einstellungen des Anwenders und bei *markiertem* Feld die Einstellungen der ausgewählten Gruppe für die Favoriten, den Toolbar bzw. den Autostart des Anwenders verwendet.

Gruppen

Der nur beim Anlegen eines Anwenders vorhandene Reiter **Gruppen** kann verwendet werden, um festzulegen welchen Gruppen der aktuelle Anwender initial zugeordnet ist. Für eine spätere Änderung können die üblichen Gruppen-Funktionen verwendet werden (siehe *Abschnitt 14.2.2*).

Der Reiter enthält eine Auflistung aller definierten Gruppen mit zugehörigen Kontrollfeldern, mit denen die gewünschten Gruppenzugehörigkeiten festgelegt werden können.

Der Eintrag **Gruppenzuweisung anhand von Startsicht** kann ausgewählt werden, um den Anwender der Gruppe zuzuorden, die auf dem Reiter **Informationen** für ihn als **Startsicht** ausgewählt wurde (siehe oben).

14.1.2 Passwort-Richtlinien

Um die Benutzung von ’sicheren’ Passwörtern zu gewährleisten, gelten eine Reihe von Richtlinien, denen Anwender-Passwörter genügen müssen. Diese sind im Einzelnen:

- Ein Passwort muss mindestens eine Länge von 8 Zeichen besitzen.
- Es darf höchstens eine Länge von 16 Zeichen besitzen.
- Es muss mindestens einen Großbuchstaben (A-Z) enthalten.
- Es muss mindestens eine Ziffer (0-9) enthalten.
- Es muss mindestens ein Sonderzeichen aus der Menge
  ’! $ % & ( ) = ? / * - + @ # < >’
  enthalten.
- Es darf keinen Teilstring enthalten, der aus drei oder mehr identischen Zeichen besteht. (kein Zeichen darf sich mehr als einmal unmittelbar wiederholen).
- Ein neues Passwort muss sich von den letzten 5 für den Anwender zuvor definierten Passwörtern unterscheiden.

Wird bei einem Login-Versuch fünf Mal in Folge ein falsches unterschiedliches Passwort für einen Anwender eingegeben, so wird der betroffene Anwender gesperrt. Der Anwender kann dann von einem Administrator entsperrt werden, bevor er sich erneut anmelden kann. Ansonsten wird die Anmeldung nach 60 Minuten oder bei Server-Neustart freigegeben.

14.1.3 Zeitabhängiges Login/Logout

Der OpenScape FM Desktop stellt eine Funktion bereit mit deren Hilfe Zeitintervalle für den Login/Logout-Mechanismus des OpenScape FM für einzelne Anwender berücksichtigt werden können. Diese Funktion ist aktiviert, wenn das Kontrollfeld **Benutzer kann sich jederzeit einloggen** in *Bild 18* **keinen** Haken enthält.

Ist die Funktion aktiviert, so kann für einen Anwender ein Zeitfilter ausgewählt werden. Dies geschieht durch die Auswahl innerhalb des **Zeitplan** Auswahlmenüs. Dieser Filter enthält Zeitintervalle und eine Zeitzone. Der Anwender kann sich nur innerhalb der durch diesen Zeitfilter definierten Zeitintervalle einloggen. Mehr über die Definition und Konfiguration von Zeitplänen findet sich in *Kapitel 20, „Zeitpläne“*.

Immer wenn sich ein zeitlich beschränkter Anwender auf den OpenScape FM Server einloggt, überprüft der Server basierend auf dem zugeordneten Zeitfilter, ob der aktuelle Zeitpunkt innerhalb der erlaubten Zeitintervalle liegt. Ist dies nicht der Fall, so wird das Login abgewiesen. Ansonsten wird das Login erlaubt, und der OpenScape FM Server bestimmt den nächstliegenden Logout-Zeitpunkt und teilt diesen dem Client mit. Wird dieser Zeitpunkt erreicht, stößt der Client automatisch ein Logout auf dem Server an.

Wurde das Kontrollfeld **Automatisches Login** für den Anwender abgehakt, so bestimmt der Server während des automatischen Ausloggens den nächsten Zeitpunkt zu dem der Anwender sich wieder auf dem Server einloggen darf. Der OpenScape FM Client wartet dann bis zu diesem Zeitpunkt ab und verbindet den Anwender dann automatisch mit dem Server.

Loggt sich ein nicht zeitbeschränkter Anwender auf dem Server ein, so wird der automatische Login/Logout-Mechanismus nicht aktiviert.

Wichtiger Hinweis:
Finden Umkonfigurationen des ausgewählten Zeitfilters statt, während der OpenScape FM Client nicht mit dem Server verbunden ist und dieser auf den Zeitpunkt einer erneuten Verbindung wartet, so wird diese Umkonfiguration zunächst ignoriert. Der Zeitpunkt des nächsten automatischen Logout wird während der Login-Phase festgelegt.

Beispiel:
Einem Anwender ’Mustermann’ ist es erlaubt an beliebigen Tagen zwischen 19 Uhr und 9 Uhr mit dem OpenScape FM zu arbeiten. Er startet den Client an einem Dienstag um 20 Uhr und loggt sich auf dem Server ein. Der Client wird dann am Mittwoch-Morgen um 9 Uhr ein Autologout durchführen. Falls das automatische Login aktiviert ist, wird der Anwender am Abend um 19 Uhr automatisch mit dem Server verbunden. Dies wiederholt sich an den folgenden Tagen.

14.1.4 Der Anwender „root“

Während der Installation des OpenScape FM wird das „root“-Konto automatisch erstellt. Um mit OpenScape FM zu arbeiten, melden Sie sich als „root“ an. Lassen Sie dabei das Feld **Passwort** frei und klicken Sie auf **Login**. Sie werden anschließend aufgefordert das Passwort für „root“ festzulegen. Jetzt können Sie weitere Anwenderkonten einrichten.

14.1.5 Zuweisen von Zugriffsrechten für neue Anwender

Nach der Erstellung eines neuen Anwenderkonto hat der betreffende Anwender nur eingeschränkte Rechte. Er hat das Recht „Basis -> Map-Leser“ für alle Objekte, die Berechtigung „Anwender“ für das Root-Objekt sowie die Berechtigung „Basis -> Passwort ändern“ für eigene Objekte. Näheres zur Zuweisung weiterer Rechte für den betreffenden Anwender enthält *Abschnitt 15.7.1, „Zuweisen neuer Objektrechte“*.

14.1.6 Löschen eines Anwenderkontos

Um ein Anwenderkonto zu löschen, kann aus dem Kontextmenü des betreffenden Anwendersymbols der Eintrag **Bearbeiten->Objekt Löschen...**. Es können alle Konten außer dem „root“-Konto gelöscht werden.

14.1.7 Ändern des Passworts

Um das Passwort für einen Anwender zu ändern, muss zunächst das Symbol des betreffenden Anwenderkontos lokalisiert werden. Im Kontextmenü dieses Symbols kann der Befehl **Passwort->Ändern** gewählt und ein neues Passwort für das zugehörige Anwenderkonto eingeben werden (*Bild 19*).

Bild 19 Anwenderverwaltung: neues Passwort

Um ’unsichere’ Passwörter zu verhindern, müssen die Passwörter einigen Richtlinien genügen (siehe dazu *Abschnitt 14.1.2, „Passwort-Richtlinien“*). Die Änderungen werden beim nächsten Login wirksam.Ohne Administrator-Zugriffsrechte kann hier nur das eigene Passwort geändert werden.

Eine andere Methode das Passwort des aktuell eingeloggten Anwenders zu ändern stellt der Menüeintrag **Client->Passwort Ändern...** im Hauptmenü dar.

14.1.8 Sperren eines Anwenders

Über die Befehle **Anwender sperren** und **Anwender freigeben** des Kontextmenüs kann eine Login-Sperre für einen Anwender aktiviert bzw. diese Sperre wieder aufgehoben werden. Die Symbol-Namen gesperrter Anwender werden von Sternen eingeschlossen dargestellt und der Status des Anwenders wird auf *Critical* gesetzt. Die Sterne und der Status *Critical* werden entfernt, wenn der entsprechende Anwender wieder freigegeben wird.

Der Anwender ’root’ kann nicht manuell gesperrt werden.

Ein Anwender kann sich, mit Hilfe des Hauptmenüeintrages **Client->Benutzer sperren**, selbst sperren. Der Anwender kann danach nur durch einen Administrator entsperrt werden.

Fünf aufeinander folgende Fehlversuche bei der Anmeldung sperren den Anwender, um weitere Versuche zu unterdrücken. Wird der Anwender ‚root‘ automatisch gesperrt, so kann sein Konto über einen Neustart des OpenScape FM Servers reaktiviert werden.

14.1.9 Authentifikation durch Active Directory

Zusätzlich zur Erstellung und Verwendung interner Anwender-Konten, die nur für das OpenScape FM gelten, kann die Authentifikation der Anwender auch über den Active Directory Domain Service von Windows erfolgen.

Um diese Funktion zu aktivieren, muss die Active Directory Schnittstelle im OpenScape FM konfiguriert und freigeschaltet werden. Dies kann über den Aufruf des Hauptmenüeintrages **Server->Administration->Server Eigenschaften** geschehen. Auf der Seite **Active Directory-Konfiguration** kann nun der entsprechende Haken vor **Active Directory-Login erlauben** gesetzt und der **Host**, der **Port** und der **LDAP-Root-Kontext** des zu verwendenden Active Directory Domain Services konfiguriert werden.

Mit den Haken vor **Sicheres LDAP** kann festgelegt werden, ob LDAP über SSL (LDAPS) verwendet werden soll (Haken gesetzt).

Wird kein **LDAP-Root-Kontext** angegeben, wird der Anwender-Account im Active Directory über die ganze Datenbank gesucht. Durch eine Angabe wie z.B. `DC=bui` kann die Suche auf einen Domänen-Teilbaum eingeschränkt werden (im Beispiel auf Domänen, die mit `bui` beginnen).

Durch Entfernen des Auswahlhakens **Active Directory-Login erlauben** kann der Active Directory Zugriff jederzeit wieder allgemein gesperrt werden.

Für die Authentifikation über das Active Directory erfolgt die Anmeldung wie gewohnt über das übliche Anmeldefenster. Als Name dient jedoch die Active Directory Identifizierung „`<DOMÄNE>\<ANWENDER>`“ und es wird das entsprechende Active Directory Passwort erwartet.

Meldet sich ein Active Directory Anwender das erste Mal im OpenScape FM an, so wird im OpenScape FM ein neues Active Directory Anwender-Konto eingerichtet. Die Anmeldung auf ein derartiges Konto kann auch bei zukünftigen Anmeldungen ausschließlich über Active Directory erfolgen. Das Konto kann aber, wie jedes andere Konto, einzeln von einem Administrator im OpenScape FM gesperrt oder freigegeben werden.

Bei jeder Anmeldung auf ein Active Directory Anwender-Konto werden die aktuellen Gruppenzugehörigkeiten des Anwenders in Active Directory für die aktuelle OpenScape FM Sitzung verwendet. Außerdem werden die Benutzerinformationen synchronisiert und gegebenenfalls im OpenScape FM aktualisiert.

Ein Active Directory Anwender besitzt im OpenScape FM die Rechte aller Gruppen, denen er zum Zeitpunkt seiner Anmeldung in das OpenScape FM, im Active Directory zugeordnet ist. Existiert im OpenScape FM nicht mindestens eine dieser Gruppen, ist eine Anmeldung für den Anwender nicht möglich, und das Anwender-Konto wird im OpenScape FM entfernt. Das Konto wird ebenfalls gelöscht, wenn der entsprechende Anwender aus dem Active Directory entfernt wird.

Wichtiger Hinweis:
Die Gruppen selbst werden nicht im OpenScape FM automatisch angelegt. Gruppen mit entsprechenden Namen müssen im OpenScape FM manuell erstellt und mit Rechten ausgestattet werden.

14.1.10 Anwender exportieren/importieren

Das OpenScape FM erlaubt den Export aller eingerichteten Anwender (mit Ausnahme des Anwenders `root`).

Der Export erfolgt über die Auswahl des Menüeintrages **Bearbeiten->Daten exportieren...** aus dem Kontextmenü des Objektes **Root->Anwender Verwaltung->Anwender**. Wird der Export gestartet, kann in einem Datei-Browser der Name und der Speicherort einer Export-Datei ausgewählt werden. Anschließend wird die entsprechende Export-Datei im XML-Format erstellt.

Die Export-Datei enthält **alle** eingerichteten Anwender (außer `root`) und deren Informations- und Rechte-Konfiguration. Die Passworte und die Passwort-Einstellungen sind **nicht** Bestandteil des Exports.

Mit Hilfe des Menüeintrages **Bearbeiten->Daten importieren...** aus dem Kontextmenü des Objektes **Root->Anwender Verwaltung->Anwender** können die Anwenderdaten zu einem späteren Zeitpunkt wieder geladen werden.

Während des Importes werden Anwender, für die bereits ein Eintrag mit gleichem Login-Namen existiert, **NICHT** überschrieben. Ihre Import-Daten werden somit ignoriert.

Nicht vorhandene Anwender werden gemäß der importierten Daten angelegt. Es ist dabei zu beachten, dass diesen Anwendern **KEIN** Passwort zugewiesen wird. Die neu angelegten Anwender sollten daher evtl. zunächst gesperrt oder vom Administrator mit einem Passwort ausgestattet werden.

Durfte sich ein exportierter Anwender nur innerhalb eines aktiven Zeitplans anmelden, gilt dies auch für den importierten Anwender. Allerdings nur für den Fall, dass ein Zeitplan mit entsprechendem Namen zum Zeitpunkt des Imports existiert.

Der Export/Import kann z.B. verwendet werden, wenn die Rechte für einen Anwender angepasst werden sollen.

Ist das Ergebnis der Rechtevergabe nicht zufriedenstellend ausgefallen, muss lediglich der betroffene Anwender gelöscht und der zuvor durchgeführte Export importiert werden. Es werden dann die alten Einstellungen des gelöschten Anwenders wiederhergestellt. Die Einstellungen aller anderen Anwender bleiben vom Import unberührt.

14.2 Anwendergruppen

Eine Anwendergruppe ist eine Menge von Anwendern. Gruppen sind eine effiziente und flexible Möglichkeit, um gleiche Zugriffsrechte für eine Anzahl von Anwendern gleichzeitig zuzuweisen. Durch das Zuordnen eines spezifischen Rechts (Objekt- oder Mandat-Rechte) zu einer Anwendergruppe wird dieses Recht allen Mitgliedern der Gruppe zugewiesen (siehe *Abschnitt 14.1.5, „Zuweisen von Zugriffsrechten für neue Anwender“*). Wird ein neuer Anwender einer Anwendergruppe hinzugefügt, so erhält er automatisch alle Rechte, die aktuell der Anwendergruppe zugeordnet sind. Die Rechte, die einem Anwender zur Verfügung stehen, ergeben sich aus den Rechten, die durch die Gruppen zugewiesen werden, zu denen der Anwender gehört, und den spezifischen Rechten, die speziell dem Anwender zugeordnet sind.

Das Symbol „Gruppen“ ist das zentrale Objekt bezüglich der Administration von Anwendergruppen. Ausgehend von diesem Symbol können Gruppen erzeugt und Anwender diesen Gruppen zugewiesen werden. Die Sicht des „Gruppen“ Symbols enthält Symbole für alle definierten Anwendergruppen.

Das Symbol „Gruppen“ stellt die folgenden Operationen zu Verfügung:

Neu->Gruppe...:
Mit Hilfe dieses Menüeintrages können neue Anwendergruppen erzeugt werden.

Konfigurieren...:
Dieser Menüeintrag öffnet einen Dialog, der die Beziehungen zwischen Anwendern und Anwendergruppen darstellt. Außerdem ermöglicht der geöffnete Dialog die Zuweisung einzelner oder mehrerer Anwender zu einer oder mehreren Anwendergruppen.

14.2.1 Erzeugen von Anwendergruppen

Um eine neue Anwendergruppe zu erzeugen muss der Menüeintrag **Neu->Gruppe...** aus dem Kontext-Menu des „Gruppen“ Symbols ausgewählt werden. Dies öffnet ein Fenster, in dem der Name der neuen Anwendergruppe im Textfeld **Gruppen Name** eingegeben werden muss. Zusätzlich ist es möglich, eine Beschreibung der Anwendergruppe im Textfeld anzugeben.

Nach Betätigung der **Hinzufügen** Schaltfläche wird die neue Anwendergruppe auf der Sicht des „Gruppen“-Symbols hinzugefügt.

Das Betätigen der **Abbrechen** Schaltfläche schließt das Fenster ohne das eine neue Anwendergruppe erzeugt wird.

Für eine Anwendergruppe stehen in deren Kontextmenü über den Menüeintrag **Konfigurieren...** folgenden Operationen auf verschiedenen Seiten zur Verfügung:

- **Beschreibung:**
  Zeigt den Namen der ausgewählten Anwendergruppe und den dieser Gruppe zugeordneten Beschreibungstext an.
- **Objektrechte:**
  Mit Hilfe dieser Seite können der Anwendergruppe Objekt-Rechte zugeordnet werden.
- **Domänenrechte:**
  Mit Hilfe dieser Seite können der Anwendergruppe Mandaten-Rechte zugeordnet werden.

Zu Beginn ist eine neu erstellte Anwendergruppe 'leer'. D.h. es sind ihr keine Anwender oder Zugriffsrechte zugeordnet. In den nächsten Schritten müssen der neu erstellten Gruppe Anwender (*Abschnitt 14.2.2, „Zuordnung von Anwendern zu Anwendergruppen“*) und Zugriffsrechte (*Abschnitt 14.2.4, „Hinzufügen von Zugriffsrechten für Anwendergruppen“*) zugewiesen werden.

14.2.2 Zuordnung von Anwendern zu Anwendergruppen

Das zentrale Objekt für die Zuordnung von Anwendern zu Anwendergruppen ist das „Gruppen“ Symbol innerhalb der „Anwender Verwaltung“ Sicht. Dessen Kontextmenü bietet den Menüeintrag **Konfigurieren...** an. Die Auswahl dieses Menüeintrages öffnet eine Seite, die eine Matrix enthält, die die Zuordnung von Anwendern zu Anwendergruppen darstellt. Jede Zeile der Matrix repräsentiert einen Anwender. Alle Spalten außer der ersten repräsentieren eine Anwendergruppe. Und jede Zelle enthält ein Auswahlfeld das anzeigt, ob der Anwender der entsprechenden Zeile der Anwendergruppe der entsprechenden Spalte zugeordnet ist. Ist das Auswahlfeld aktiviert, so ist der Anwender ein Mitglied der Anwendergruppe, ansonsten nicht.

Auf der rechten Seite befindet sich ein Auswahlfeld für jede existierende Anwendergruppe und eine dazugehörige Schaltfläche  . Diese Elemente sind die wesentlichen Komponenten für die Zuordnung von Anwendern zu Anwendergruppen.

Falls keine Anwendergruppe definiert ist, enthält der Info-Browser lediglich eine Auflistung aller Anwender.

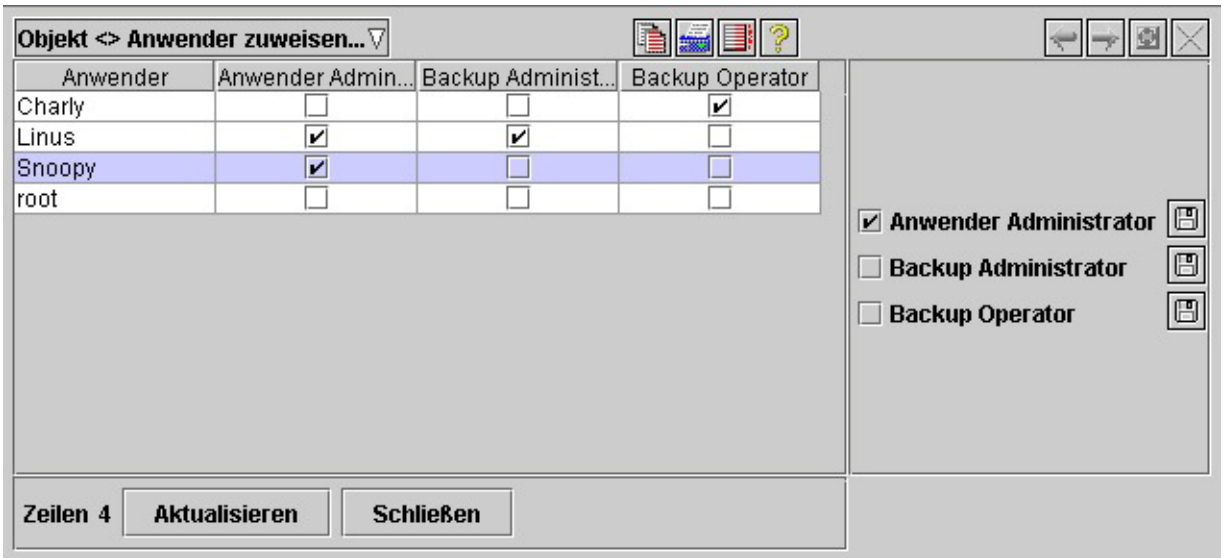


Bild 20 Zuordnung von Anwendern zu Anwendergruppen

Um einer Anwendergruppe einen Anwender zuzuweisen, muss die den Anwender repräsentierende Zeile selektiert werden. Anschließend muss der Haken in dem zur Anwendergruppe gehörenden Auswahlfeld gesetzt werden und die zugeordnete Schaltfläche  betätigt werden.

Es ist möglich, mehrere Anwender gleichzeitig einer oder sogar mehreren Anwendergruppen zuzuweisen, da der Info-Browser die Mehrfachselektion von Anwendern unterstützt. Alle Aktion bezüglich der Anwendergruppenzugehörigkeit werden mittels der Dialogkomponenten auf der rechten Seite des Fensters durchgeführt.

Das Betätigen der Schaltfläche hat folgende Auswirkungen:

- Die Matrix des Info-Browsers wird aktualisiert.
- Der neue Anwender wird der Sicht „Zugewiesene Anwender“ der entsprechenden Anwendergruppe hinzugefügt. Eine komfortable Methode um festzustellen, welche Anwender Mitglied einer Anwendergruppe sind, ist es daher, einen Blick auf die Sicht „Zugewiesene Anwender“ der Anwendergruppe zu werfen.
- Der Sicht „Zugewiesene Gruppen“ des Anwenders wird die Anwendergruppe hinzugefügt. Diese Sicht enthält alle Anwendergruppen, in denen der Anwender Mitglied ist.

14.2.3 Einen Anwender aus einer Anwendergruppe entfernen

Um einen Anwender aus einer Anwendergruppe zu entfernen, müssen folgende Schritte durchgeführt werden:

- Als erstes müssen Sie den „Anwender zuweisen“ Dialog öffnen. Dieser öffnet sich nach Betätigen des Menüeintrages **Konfigurieren** aus dem Kontextmenü des „Gruppen“-Symbols.
- In dem geöffneten Dialog muss die Zeile selektiert werden, die den entsprechenden Anwender repräsentiert.
- Danach muss auf der rechten Seite des Dialogs das Auswahlfeld der Anwendergruppe, aus der der Anwender entfernt werden soll, deaktiviert werden. Bitte vergessen Sie nicht anschließend die Schaltfläche zu betätigen, siehe auch *Bild 20*.

Nun, wird der Anwender aus dem Container „Zugewiesene Anwender“ der entsprechenden Anwendergruppe entfernt und die Anwendergruppe wird aus dem Container „Zugewiesene Gruppen“ des entsprechenden Anwenders entfernt. Als Konsequenz verliert der Anwender alle Rechte, die dem Anwender über die Anwendergruppe zugewiesen worden sind.

14.2.4 Hinzufügen von Zugriffsrechten für Anwendergruppen

Auf sich alleine gestellt erfüllen Anwendergruppen zunächst keine wirklich sinnvolle Funktion. Erst in Verbindung mit Zugriffsrechten stellen sie eine große Hilfe bei der Verwaltung von Anwendern dar. Durch Anwendergruppen ist es möglich, Zugriffsrechte gleichzeitig für eine Menge von Anwendern zuzuordnen, anstatt diese Rechte jedem Anwender einzeln zuordnen zu müssen. Wird ein Anwender einer Gruppe hinzugefügt, so erbt dieser automatisch alle Rechte der Gruppe und fügt diese Rechte den Rechten hinzu, die ihm bereits durch andere Gruppen oder durch direkte Zuordnung zugebilligt wurden.

Das Zuordnen von Zugriffsrechten für Anwendergruppen funktioniert nach den gleichen Prinzipien wie das Zuordnen von Rechten für einzelne Anwender. Dies bedeutet, dass auch die Zuordnung von Mandaten-Rechten möglich ist. Näheres zur Zuordnung von Rechten findet sich in *Kapitel 15, „Zugriffsrechte“*. Als kurze Einführung kann hier gesagt werden, dass das Basisobjekt für das Bearbeiten von Anwendergruppenrechten das entsprechende Gruppenobjekt ist. Diesem wird ein „Zugewiesene Rechte“ Container hinzugefügt, dessen Sicht die der Anwendergruppe zugeordneten Rechte enthält.

14.2.5 Löschen einer Anwendergruppe

Um eine Anwendergruppe zu entfernen kann der Menüeintrag **Bearbeiten->Objekt Löschen** des Anwendergruppen-Symbols aktiviert werden. Alle Anwender, die Mitglied der gelöschten Anwendergruppe waren, bleiben erhalten. Sie verlieren aber alle Rechte, die ihnen ausschließlich über die gelöschte Gruppe zugeordnet wurden. D.h. sie behalten nur die Rechte, die ihnen direkt oder durch andere Gruppen zugewiesen werden.

15 Zugriffsrechte

Innerhalb des OpenScape FM erteilt ein **Zugriffsrecht** einem spezifischen Anwender das Recht, eine spezifische Aktion auf einem spezifischen Objekt durchzuführen. Es wird daher als ein Triple, das aus einem **Anwender**, einem **Recht** und einem **Objekt** besteht, dargestellt.

Praktisch alles innerhalb des OpenScape FM wird durch Objekte dargestellt. Beispielsweise existieren Objekte für die überwachten physikalischen Geräte, für Container, welche die Objekte für die Anwender zusammenfassen und strukturieren, für Anwender, und selbst für die Komponenten des OpenScape FM selbst.

Rechte existieren für praktisch alle möglichen Aktionen, die innerhalb des OpenScape FM durchgeführt werden können. Dies kann das Recht sein, eine spezifische Schaltfläche zu betätigen, das Recht, einen spezifischen Menüeintrag zu aktivieren, oder das Recht ein Objekt sehen zu können.

Um eine Funktion auszuführen, benötigt der Anwender die notwendigen Rechte für die Funktion *und* für die Objekte, auf welche die Funktion angewendet werden soll.

Beispiel:
Um ein ECE-Modul (siehe *Event Correlation Engine Plugin Bedienungsanleitung*) einer ECE-Submap hinzuzufügen, werden Administrator-Rechte für die ECE-Submap benötigt. Soll das hinzugefügte Modul zur Überwachung von IP-Knoten eingesetzt werden, werden ebenfalls Rechte für die spezifischen IP-Knoten benötigt.

Mengen von Elementen für Zugriffsrechte:

Da es ausgesprochen mühsam wäre, Zugriffsrechte für jede spezifische Anwender/Recht/Objekt Kombination zu erteilen oder zu entziehen, können für alle drei Aspekte des Triples Platzhalter verwendet werden. Diese repräsentieren ganze Mengen von Anwendern, Rechten oder Objekten innerhalb eines Zugriffsrechts.

Gruppen (siehe *Abschnitt 14.2*) sind Mengen, die aus **Anwendern** bestehen. Wird einer Gruppe ein Zugriffsrecht erteilt, so hat jedes Mitglied der Gruppe dieses Zugriffsrecht. Ein Anwender kann beliebig vielen Gruppen angehören.

Domänen (siehe *Abschnitt 15.8*) sind Mengen, die aus einzelnen **Objekten** bestehen. Zugriffsrechte, die für eine Domäne erteilt werden, gelten für alle Objekte in der Domäne. Ein Objekt kann in beliebig vielen Domänen sein.

Eine zweite Methode, um Objektmengen zu definieren, ist die hierarchische Zuweisung von Objekten. Eine **Objekthierarchie** besteht aus einem Objekt und allen Objekten, die sich im Unterbaum dieses Objekts befinden.

Rechte können in **Rollen** zusammengefasst werden. Eine Rolle ist eine Menge von Rechten, die alle Rechte enthalten sollte, die notwendig sind, um die mit der Rolle verbundenen Aufgaben durchführen zu können.

Drei grundlegende Rollen sind im OpenScape FM vordefiniert:

- **Administrator**: Der Besitz dieser Rolle für ein Objekt erlaubt es einem Anwender, alle möglichen Aktionen für dieses Objekt durchzuführen.
  Diese Rolle erlaubt z.B. die Konfiguration der SNMP-Parameter, die Bestätigung der Ereignisse oder die Konfiguration der Netzwerk-Topologie des Objekts.

- **Operator**: Diese Rolle enthält die Rechte, um die Informationen, die Submap und die Ereignisse des Objektes zu sehen.
  Diese Rolle erlaubt es z.B. die Konfiguration der SNMP-Parameter des Objekts einzusehen, oder einen Report zu starten, der Objektdaten anzeigt.
- **User**: Diese Rolle bietet grundlegenden Zugriff. Sie erlaubt es Objekte zu sehen, aber nicht die Ausführung von Aktionen für diese Objekte.
  Die Rolle wird benötigt, um durch den Navigationsbaum zu navigieren.

Statt für Anwender/Recht/Objekt Kombinationen können Zugriffsrechte z.B. auch für Gruppe/Rolle/Domäne Kombinationen erteilt werden. Alle Anwender aus der Gruppe haben dann alle Rechte der Rolle für alle Objekte der Domäne. Dies liefert zahlreiche Anwender/Recht/Objekt Kombinationen durch eine einzelne Zuweisung.

Die Zuweisung von Mengen hat einen weiteren Vorteil: wird ein Anwender einer Gruppe hinzugefügt, oder ein Objekt einer Domäne, so gelten die gleichen Zugriffsrechte automatisch auch für die neuen Anwender oder Objekte.

Rechte entziehen:

Zugriffsrechte können spezifischen Anwendern und Objekten oder Objekthierarchien aktiv entzogen werden.

Im allgemeinen ist dies nicht notwendig, da die Tatsache, dass kein Recht erteilt wurde, der Tatsache entspricht, dass alle Rechte entzogen wurden.

Wurde aber z.B. ein Recht für eine Objekthierarchie erteilt, kann es erwünscht sein, dass Zugriffsrechte für einige Elemente der Hierarchie entzogen werden.

Vereinfachte Zuweisung:

Zwar können sehr komplexe Strukturen von Zugriffsrechten innerhalb des OpenScape FM generiert werden, meist ist es jedoch völlig ausreichend, Objekthierarchien, Anwender oder Gruppen und die vordefinierten grundlegenden Rollen zu verwenden. Für diese Fälle wird eine vereinfachte Methode zur Erteilung oder Entziehung von Rechten angeboten (siehe *Abschnitt 15.1*).

Aktive Rechte Anzeigen:

Für jedes Objekt können die aktuell aktiven Zugriffsrechte angezeigt werden (siehe *Abschnitt 15.9*).

Beispiel:

Gegeben sei eine Umgebung, in der sechs Teammitglieder ein Netzwerk überwachen sollen. Das Netzwerk selbst besteht aus zwei großen Regionen: *Region West* und *Region East*.

Zwei Mitglieder, *Chris* und *Clair*, sollen das ganze Netzwerk kontrollieren, es konfigurieren und die Administration des OpenScape FM übernehmen.

Zwei Mitglieder, *Will* und *Wilma*, sollen *Region West* überwachen und bearbeiten, aber sie sollen *Region East*. lediglich einsehen können.

Zwei Mitglieder, *Eric* und *Emily*, sollen *Region East*, überwachen und bearbeiten, aber sie sollen *Region West* lediglich einsehen können.

Um das Ziel mit möglichst geringem Aufwand zu erreichen, können die folgenden Schritte durchgeführt werden:

1. Erstellen von Anwendern: *Chris*, *Clair*, *Will*, *Wilma*, *Eric* und *Emily* (siehe *Abschnitt 14.1*).
2. Erstellen von Gruppen: *Control* mit *Chris* und *Clair*, *West* mit *Will* und *Wilma* und *East* mit *Eric* und *Emily* (siehe *Abschnitt 14.2*).
3. Erstellen einer sinnvollen Netzwerk-Topologie (siehe *Kapitel 16*): Erzeugen eines Containers *Regions*, der die Container *Region West* und *Region East* auf seiner Submap enthält. Die beiden Untercontainer sollten alle Objekte enthalten, die zu der entsprechenden Region gehören.
4. Erstellen von sieben Hierarchischen Zugriffsrechten mit den folgenden Trippeln (siehe *Abschnitt 15.1*):
   - Gruppe *Control* / Rolle *Administrator* / Objekthierarchie beginnend mit *Root*.
     Dies erlaubt es den Mitgliedern der Gruppe *Control* praktisch alles durchzuführen.
   - Gruppe *West* / Rolle *User* / Objekthierarchie beginnend mit *Root*.
     Dies erlaubt es den Mitgliedern der Gruppe *West* durch den Baum zu navigieren (sollte standardmäßig eingestellt sein).
   - Gruppe *East* / Rolle *User* / Objekthierarchie beginnend mit *Root*.
     Dies erlaubt es den Mitgliedern der Gruppe *East* durch den Baum zu navigieren (sollte standardmäßig eingestellt sein).
   - Gruppe *West* / Rolle *Administrator* / Objekthierarchie beginnend mit *Region West*.
     Dies erlaubt es den Mitgliedern der Gruppe *West* mit den Objekten der *Region West* zu arbeiten.
   - Gruppe *West* / Rolle *Operator* / Objekthierarchie beginnend mit *Region East*.
     Dies erlaubt es den Mitgliedern der Gruppe *West* die Informationen der Objekte aus *Region East* zu sehen.
   - Gruppe *East* / Rolle *Administrator* / Objekthierarchie beginnend mit *Region East*.
     Dies erlaubt es den Mitgliedern der Gruppe *East* mit den Objekten der *Region East* zu arbeiten.
   - Gruppe *East* / Rolle *Operator* / Objekthierarchie beginnend mit *Region West*.
     Dies erlaubt es den Mitgliedern der Gruppe *East* die Informationen der Objekte aus *Region West* zu sehen.

   Um diese Trippel zu erstellen, muss die Konfiguration für Hierarchische Zugriffsrechte für Standard-Rollen für die ersten drei Trippel vom *Root* Objekt aus geöffnet werden. Und jeweils einmal entsprechend von den Containern *Region West* und *Region East* für die letzten vier Trippel.

15.1 Hierarchische Zugriffsrechte für Standard-Rollen

Häufig sollen die allgemeinen Zugriffsrechte für die Rollen *Administrator*, *Operator* oder *User* für einen kompletten Teilbaum von Objekten erteilt oder entzogen werden.

In solchen Fällen können hierarchische Rechte (siehe *Abschnitt 15.3*) für die Standard-Rollen unmittelbar einem Objekt und allen seinen Kindobjekten zugewiesen oder verweigert werden.

Für diese Zuweisung muss der Eintrag **Eigenschaften** aus dem Kontextmenü des spezifischen Objektes ausgewählt und die Seite **Objektrechte** innerhalb des Eigenschaften-Fensters geöffnet werden.

Die Seite enthält eine Zeile für jeden Anwender und jede Anwendergruppe, welche die hierarchische Konfiguration des aktuellen Objekts zeigt.

Die Spalte **Name** zeigt die Namen der individuellen Anwender (vorangestellt ist das Piktogramm einer einzelnen Person) oder Anwendergruppen (Piktogramm mehrerer Personen) an.

Die Spalte **Berechtigung** zeigt, ob dem Anwender oder der Anwendergruppe aktuell *Administrator*, *Operator* oder *User* Rechte für das aktuelle Objekt zugewiesen sind, ob der Zugriff *Verweigert* ist, oder ob keine Regel zugewiesen wurde (kein Eintrag).

Wurde ein Recht erteilt oder verweigert, zeigt die Spalte **Vererbt** das Objekt an, für das die Regel definiert wurde. Dies kann entweder das Objekt selbst sein, oder das Objekt, welches sich am nächsten oberhalb in der Hierarchie befindet, und für das eine hierarchische Definition für den spezifischen Anwender oder die spezifische Anwendergruppe festgelegt wurde.

Wird das Recht über die Zugehörigkeit zu einer Gruppe vererbt, wird an dieser Stelle ein Gruppen-Symbol angezeigt, und die Spalte enthält den Namen der Gruppe, über die das Recht zugewiesen wurde.

Über das rechtsbefindliche Auswahlmenü **Berechtigung** und die zugehörige Schaltfläche können die Zugriffsrechte für einen selektierten Anwender oder eine selektierte Gruppe verändert werden.

Wird *Administrator*, *Operator* oder *User* ausgewählt und gespeichert, wird das entsprechende Zugriffsrecht dem aktuellen Objekt hierarchisch für den ausgewählten Anwender oder die ausgewählte Gruppe zugewiesen. Der Eintrag in der Spalte **Vererbt** verändert sich daher auf das aktuelle Objekt.

Die Auswahl *Verweigert* funktioniert entsprechend, aber alle Rollenrechte werden hierarchisch verweigert.

Die Auswahl *Löschen* entfernt die aktuell angezeigte Regel. Selbst dann, wenn die Regel für ein anderes Objekt als dem aktuellen vorgenommen wurde. Stattdessen wird die nun geltende Regel angezeigt.

Wichtiger Hinweis:
Die Auswahl von *Löschen* kann unerwünschte Nebeneffekte haben, falls die Vererbung nicht vom aktuellen Objekt selbst kommt. Es sind dann nicht nur Objekte, die sich unterhalb des aktuellen Objekts befinden, von der Löschung betroffen. Im Extremfall können die Zugriffsrechte für alle Objekte betroffen sein.

15.2 Die Rechte-Hierarchie

Der OpenScape FM Desktop bietet verschiedene Zugriffsrechte, die sich auf die Darstellung der Hauptmenüleiste, Objekt-Kontextmenüs, die Rechte zum Ausführen von Aktionen für Objekte, die Sichtbarkeit von Objekten auf Submaps und die Sichtbarkeit von Ereignissen im Ereignis-Browser auswirken. Wenn ein Anwender beispielsweise nicht über alle Rechte für die Hauptmenüleiste verfügt, sieht er nur eine Teilmenge des Menüs.

Grundsätzlich können Zugriffsrechte für Anwender oder für Anwendergruppen erteilt werden. Dabei steht der Begriff Anwendergruppe für eine Menge von Anwendern.

Durch das Zuweisen bzw. Nicht-Zuweisen spezieller Rechte für bestimmte Objekte an einen Anwender/eine Anwendergruppe kann ein Administrator den Zugriff von Anwendern auf das OpenScape FM-System individuell einschränken. Die Zuweisung eines Rechts erfolgt grundlegend durch Auswählen eines vorhandenen Anwender bzw. einer vorhandenen Anwendergruppe, Öffnen des Browsers „Objektrechte zuweisen“, Auswählen eines

speziellen Rechts in diesem Browser und eines dazugehörigen Objekts (siehe *Abschnitt 15.6, „Zuweisen von Zugriffsrechten“*). Auf diese Weise wird eine spezielle Zugriffsrecht-Relation für einen bestimmten Anwender bzw. eine bestimmte Anwendergruppe, ein Objekt und einem Recht eingerichtet.

Handelt es sich um eine Anwendergruppe, so wird das Recht für alle Anwender, die Mitglied der Gruppe sind, erteilt. Wird ein neuer Anwender einer Gruppe zugeteilt, erhält er automatisch alle Rechte, die zu diesem Zeitpunkt für die Gruppe freigegeben sind. Die Rechte, die für einen Anwender freigegeben sind, ergeben sich aus den Rechten, die die Anwendergruppen besitzen, in denen der Anwender Mitglied ist und den Rechten, die speziell für den einzelnen Anwender freigegeben sind.

Der OpenScape FM Desktop bietet sechsHauptkategorien für Zugriffsrechte: **Administrator**, **Domänen-Administrator**, **Kunden-Administrator**, **Technischer Administrator**, **Operator** und **Anwender**. Diese Hauptrechte stellen eine hierarchische Ansammlung von grundlegenden Rechten dar und definieren sogenannte „Rollen“.

Die folgenden vordefinierten Administratorrollen sind zu verwenden, wenn ein Secure Single Sign On (SSSO)-Zugriff auf spezielle Element Manager konfiguriert werden muss:

Der **Administrator**, **Domänen-Administrator**, **Kunden-Administrator** und **Technischer-Administrator** stehen für den Superadministrator, der über Lese-/Schreibzugriff auf alle OpenScape FM Management-Systeme, die OpenScape FM Management-Anwendungen, die Element Managers und die Administratorprofile, einschließlich mandatfähige Konfigurationen verfügt.

Die Rolle, die ein Anwender für ein spezielles Objekt ausübt, wird während des Aufrufs (SSSO) des Element Managers übergeben, der die übergebene Rolle evaluieren muss.

Ein Anwender, dem für ein bestimmtes Objekt die Rolle **Administrator** zugewiesen wurde, hat vollen Zugriff auf alle von diesem Objekt bereitgestellten Funktionen.

Die Rolle **Operator** ermöglicht einem Anwender, die Submaps und Ereignisse von Objekten anzuzeigen und Informationen von Objekten abzurufen, für die ihm diese Rolle zugewiesen wurde. Ein Operator darf keine Aktionen mit Objekten durchführen und keine Änderungen an Objekten vornehmen. Bei HiPath 4000-Systemen kann er beispielsweise die Submaps der HiPath 4000-Systeme sehen, er kann Fault-, Topologie-, Hardware- und Software-Informationen von den HiPath 4000-Systemen abrufen, er ist jedoch nicht berechtigt, Discoveries zu starten, die Anordnung im Topologie-Baum zu ändern oder Vorgänge zur Änderung von „verwaltet/nicht verwaltet“ durchzuführen.

Eine weitere Rolle ist die des **Anwenders**. Diese Rolle kann als Grundtyp angesehen werden. Der Anwender kann alle Submaps von Objekten öffnen, für die ihm die Rolle des **Anwenders** zugewiesen wurde. Er sieht alle Symbole (Systeme) auf diesen Submaps. Er kann jedoch keine Aktionen für diese Symbole durchführen, weil er nicht das verbundene Kontextmenü sieht.

Ein Anwender kann spezielle Rechte für bestimmte Objekte haben. Er kann beispielsweise die Rolle „Administrator“ für Objekt „A“ und die Rolle „Operator“ für Objekt „B“ haben.

Die Rechte sind, wie alle Objekte in OpenScape FM, in hierarchischer Reihenfolge angeordnet. OpenScape FM ist eine hoch entwickelte Anwendung, die auf dem objektorientierten Modell basiert. Die Objekt-Hierarchie wird also durch die Rechte bestimmt. Diese Rechte-Hierarchie bietet einen Gesamtüberblick über die grundlegenden und Plugin-spezifischen Zugriffsrechte. Alle Module wie der Desktop und seine verschiedenen Plugins enthalten spezifische Rechte für die Anzeige und die Änderung des Zugriffs auf das OpenScape FM-System.

Ein Administrator kann natürlich auch alle feinabgestimmten Rechte von der Rechte-Hierarchie zuweisen.

15.3 Geltungsbereiche für Rechte

Rechte sind für individuelle Funktionen oder für Gruppen von Funktionen definiert, die innerhalb des OpenScape FM ausgeführt werden können. Jedes Recht wird durch ein Symbol innerhalb des Rechte-Navigationsbaums repräsentiert.

Regeln für Zugriffsrechte erlauben oder verbieten die Verwendung dieser Funktionen für spezifische Objekte oder Objektgruppen durch Anwender oder Anwender-Gruppen.

Jede Regel besteht daher aus vier Basisparametern:

- Das Recht (die Funktionalität die erlaubt oder verboten werden soll).
- Der Anwender oder die Gruppe (wer soll die Funktion nutzen oder nicht nutzen).
- Das Objekt oder Objekte (wofür wird die Funktion erlaubt oder verboten).
- Der Regeltyp (erlaubend oder verbietend).

Es gibt drei mögliche Optionen die Objekte für eine spezifische Regel festzulegen:

- Eine Regel kann *Allen* Objekten zugewiesen werden.
- Eine Regel kann für *Ein* spezifisches Objekt gelten.
- Eine Regel kann einer Objekt-*Hierarchie* zugewiesen werden. Dies bedeutet zu einen spezifischen Objekt und allen Objekten im Teilbaum unterhalb des Objektes.

Wird eine hierarchische Zuweisung verwendet, wird die Regel allen Objekten innerhalb des entsprechenden Teilbaums zugewiesen. Diese Zuweisung wird entzogen, falls ein Objekt aus diesem Teilbaum heraus verschoben wird. Sie wird automatisch Objekten hinzugefügt, die zu einem späteren Zeitpunkt in den Teilbaum verschoben, oder in diesem erzeugt werden.

Hinweis:
Regeln für Anwender definierte Objektgruppen (genannt Domänen - siehe *Abschnitt 15.8*) sind ein Sonderfall der hierarchischen Regeln. Die Regeln werden hierarchisch dem entsprechenden Domänen-Objekt zugewiesen. Dieses enthält alle Objekte der Domäne in seiner Submap.

Wie Regeln ausgewertet werden wird im folgenden *Abschnitt 15.4* behandelt.

15.4 Auswertungsreihenfolge für Rechte

Dieser Abschnitt beschreibt, wie die Regeln für Zugriffsrechte ausgewertet werden, um zu entscheiden ob eine spezifischen Funktionalität für den aktuellen Anwender des OpenScape FM ausgeführt werden kann.

Um eine Funktion für ein Objekte ausführen zu dürfen, müssen zwei Bedingungen erfüllt sein:

- Es muss mindestens eine Regel existieren, welche die gewünschte Funktion für das aktuelle Objekt und den aktuellen Anwender erlaubt.
- Es darf keine Regel mit einem gleichen oder höheren Rang existieren, welche die Funktion für das aktuelle Objekt und den aktuellen Anwender verbietet.

Im allgemeinen haben spezifischere Regeln einen höheren Rang als weniger spezifische Regeln. So sind z.B. Regeln für einen Anwender spezifischer sind als Regeln für eine Gruppe, die den Anwender enthält. Regeln für ein individuelles Objekt sind spezifischer als hierarchische Regeln für einen Objekt-Container, welche wiederum spezifischer sind als hierarchische Regeln für ein umschließendes Container-Objekt.

Beispiel:
Für den Fall, dass der Container *AlleRegionen* die Container *RegionEins* und *RegionZwei* enhält, und ein Anwender nur die Objekte aus *RegionEins* sehen soll, ist es möglich dem Container-Objekt *AlleRegionen* eine erlaubende hierarchische Regel zuzuweisen, und dem Container-Objekt *RegionZwei* eine verbietende hierarchische Regel.

Die Auswertung der Zugriffsrechte führt die folgenden Schritte in Reihenfolge aus, um zu entscheiden, ob die Funktion durch den Anwender und für das spezifische Objekt ausgeführt werden darf.

Trifft innerhalb eines Ausführungsschritts eine verbietende Regel zu, wird der Zugriff verweigert

Trifft innerhalb eines Ausführungsschritts eine erlaubende und keine verbietende Regel zu, wird der Zugriff erlaubt.

Trifft für einen Ausführungsschritt keine Regel zu, wird der nächste Schritt durchgeführt.

Gibt es keine weiteren Schritte und es wurde keine zutreffende Regel gefunden, wird der Zugriff verweigert.

Ausführungsschritte:

1. Es werden Regeln für den aktuellen Anwender, die spezifische Funktion und *Alle* Objekte überprüft.
2. Es werden Regeln für den aktuellen Anwender, die spezifische Funktion und das *Eine* spezifische Objekt überprüft.
3. Es werden Regeln für den aktuellen Anwender, die spezifische Funktion und alle minimalen *Hierarchischen* Sets von Objekten, die das spezifische Objekt enthalten, überprüft. Da das Objekt durch mehrere Symbole repräsentiert werden kann, kann dies mehr als ein Set sein.

   Ein Set ist minimal, wenn kein anderes hierarchisches Set existiert, welches das spezifische Objekt enthält und vollständig im Set enthalten ist.
4. Es werden Regeln für den aktuellen Anwender, die spezifische Funktion und alle kleinsten *Hierarchischen* Sets von Objekten, die das spezifische Objekt enthalten, überprüft..

   Ein Set gehört zu den kleinsten Sets, falls kein anderes hierarchisches Set existiert, welches noch nicht überprüft wurde, und welches das Set vollständig enthält.

   Dieser Schritt wird wiederholt, bis alle Sets überprüft sind.
5. Die Schritte 1 bis 4 werden wiederholt. Dabei wird jedoch die spezifische Funktion durch ihre Vaterfunktion ersetzt (die allgemeinere Funktion, welche die aktuelle Funktion in ihrer Submap enthält).

   Dieser Schritt wird so lange wiederholt, wie es für die zuletzt überprüfte Funktion noch eine Vaterfunktion gibt.
6. Die Schritte 1 bis 5 werden wiederholt, aber der aktuelle Anwender wird durch eine Gruppe ersetzt, welcher der Anwender angehört.

   Dieser Schritt wird mit der nächsten passenden Gruppe wiederholt bis keine Gruppen mehr übrig sind. Die Gruppen werden in der Reihenfolge der Gruppenerstellung überprüft.

15.5 Funktionen der einzelnen Rechte

Die Beschreibung der einzelnen Rechte erfolgt in Form eines Tool Tip für das jeweils zugehörige Rechte-Symbol. Dabei ist es egal, ob sich das Rechte-Symbol im Objekt-Baum oder auf einer Submap befindet.

Der Tool Tip enthält jeweils die folgenden Informationen:

- Den Namen des Plugins und des Rechtes.
- Die Objekttypen (**Zielobjekt**) auf die das Recht wirkt.
- Die Information, ob es sich um ein einzelnes Recht, oder um eine Zusammenfassung von Rechten handelt (**Kategorie**).
- Den **Geltungsbereich**, in dem das Recht zur Anwendung kommt (z.B. kann ein Recht einen Menüpunkt oder eine Funktion/einen Prozess freischalten)
- Eine **Beschreibung** der Auswirkungen des Rechtes.

Die Namen der Rechte des Desktops beginnen mit der Plugin-Kennzeichnung *Base*.

Rechte, die durch zusätzliche geladene Plugins hinzugefügt werden, werden ebenfalls in den Rechte-Baum eingefügt, und diese werden mit entsprechenden Tool Tip beschrieben.

15.6 Zuweisen von Zugriffsrechten

Rechte können für einzelne Anwender oder für Anwendergruppen zugewiesen werden. Soll mehr als ein Anwender die gleichen Rechte für die gleichen Objekte erhalten, ist es sinnvoll, eine Anwendergruppe einzurichten und die Anwender dieser Gruppe zuzuordnen. Der Vorteil dieser Vorgehensweise ist, dass die Zuweisung der Rechte nur einmal für die Anwendergruppe erfolgen muss, anstatt für jeden betroffenen Anwender einzeln. Soll nur ein einzelner Anwender Rechte für eine Menge von Objekten erhalten, so können ihm diese direkt zugewiesen werden, oder es kann eine Anwendergruppe erzeugt werden, die diesen Anwender als einziges Mitglied enthält. Die zweite Vorgehensweise hat den Vorteil, dass wenn zu einem späteren Zeitpunkt ein weiterer Anwender die gleiche Rolle wie der erste Anwender einnehmen soll, dieser nur zu der Anwendergruppe hinzugefügt werden muss, und er dann die rollenbezogenen Rechte automatisch zugewiesen bekommt.

Die Schritte, die notwendig sind, um einem Anwender oder einer Anwendergruppe Rechte zuzuweisen, sind im Wesentlichen identisch. Der Unterschied liegt lediglich im Startobjekt.

Das Zuweisen von Rechten für einen einzelnen Anwender beginnt mit der Auswahl des Menüeintrags **Konfigurieren** aus dem Kontext-Menü des dem Anwender zugeordneten Symbols innerhalb der „Anwender Verwaltung->Anwender“ Sicht. Die Seiten **Objektrechte** bzw. **Domänenrechte** dienen für die entsprechende Konfiguration.
Beide Seiten zeigen nur die Rechte an, die *unmittelbar* dem Anwender zugewiesen wurden. Rechte, die ausschließlich über die Mitgliedschaft in Gruppen erteilt wurden, werden hier nicht angezeigt.

Das Zuweisen von Rechten für eine Anwendergruppe erfolgt ebenfalls über die Auswahl des Menüeintrages **Konfigurieren** auf den Seiten **Objektrechte** bzw. **Domänenrechte**. Allerdings handelt es sich hierbei um das Kontext-Menü des der Anwendergruppe zugeordneten Symbols aus der Sicht „Anwender Verwaltung->Gruppen“.

In beiden Fällen öffnet sich der gleiche Dialog. Lediglich der Geltungsbereich des Dialogs unterscheidet sich.

Auf der Seite **Objektrechte** können Sie die Rechte für ein spezielles Objekt oder alle Objekte zuweisen und löschen (siehe auch *Abschnitt 15.7, „Objektrechte“*).

Auf der Seite **Domänenrechte** können auf effiziente Weise Rechte für eine vordefinierte Objektgruppe, eine so genannte „Domäne“, zugewiesen und gelöscht werden. Domänen stellen Objektgruppen dar (weitere Informationen finden sich in *Abschnitt 15.8, „Domänen“*). Bevor Zugriffsrechte für Domänen zugewiesen werden können, muss zuvor eine Domäne erstellt worden sein (siehe *Abschnitt 15.8.1, „Anlegen einer Domäne“*), die alle Objekte enthält, die zu der Domäne gehören sollen. Eine Domäne enthält immer dieselbe Objektgruppe für alle Anwender. Der Vorteil der Verwendung von Domänen besteht darin, dass auf effiziente Weise spezielle Rechte für einen Anwender oder eine Anwendergruppe für den Zugriff auf alle Objekte in der Domäne zuwiesen werden können. Es muss nicht mehr für jedes einzelne Objekt für jeden Anwender bzw. jede Anwendergruppe einzeln ausgewählt werden.

Rechte können also auf zwei Arten zuwiesen werden: für *spezielle* Objekte (Objektrechte) und/oder für *Objektgruppen* (Domänenrechte), die Domänen. Ein Anwender bzw. eine Anwendergruppe kann demnach berechtigt sein, auf ein oder mehrere Objekte und/oder auf ein oder mehrere Domänen zuzugreifen.

Wichtiger Hinweis:
Es spielt keine Rolle, ob ein Recht für ein Objekt als Objektrecht auf der Seite **Objektrechte** oder als Recht für eine Domäne auf der Seite **Domänenrechte** zugewiesen wurde. Die Rechte eines Anwenders für ein Objekt setzen sich aus den als einzelnen Objektrechten erteilten Rechten und den als Teil eines Domänenrechts erteilten Rechten zusammen. Wenn ein Recht für ein Objekt mehr als einmal über verschiedene Methoden erteilt wurde, so macht dies keinen Unterschied. Als einzige Tatsache zählt, „dass dem Anwender das Recht erteilt wurde“. Es sind Redundanzen bei der Zuweisung von Rechten möglich.

Wichtiger Hinweis:
Wenn Sie Rechte nur für ein bestimmtes Objekt unter der Container-Root zuweisen wollen, sollten Sie zumindest **Benutzer**-Rechte für alle Objekte im Hierarchiepfad zu diesem Objekt erteilen. Diese Objekte sind das Objekt selbst und alle seine übergeordneten Objekte bis zum Startobjekt der Map. Andernfalls kann der Anwender nicht zu diesem Objekt navigieren.

15.6.1 Liste von Rechtebedingungen für einen Anwender oder eine Anwendergruppe

In der OpenScape FM Objekthierarchie wird jedes Recht, das *direkt* einem Anwender zugewiesen wurde, durch ein „RightGranted“ Symbol im Container „Zugewiesene Rechte“ innerhalb der Anwender-Sicht repräsentiert. Für Anwendergruppen werden zugewiesene Rechte ebenfalls durch RightGranted Symbole repräsentiert. Diese befinden sich in diesem Fall im Container „Zugewiesene Rechte“ innerhalb der Anwendergruppen-Sicht. Rechte, die einem Anwender über dessen Anwendergruppen zugebilligt werden, erhalten **keinen** eigenen Eintrag in der Sicht des Anwenders. Daher ist es mit Hilfe des Navigationsbaumes leicht möglich zu erkennen, ob einem Anwender ein Recht direkt zugewiesen wurde, oder ob es ihm über eine Anwendergruppe zugeteilt wird.

Rechte, die Objekten zugewiesen sind, werden mit einem *grünen* Symbol dargestellt.

Rechte, die explizit für Objekte ausgeschlossen sind (siehe *Abschnitt 15.7.1*), werden mit einem *roten* Symbol dargestellt.

Rechte, die mindestens einem Objekt zugewiesen sind, und die mindestens für ein anderes Objekt ausgeschlossen sind, werden mit einem *gelben* Symbol dargestellt.

Jedes Kontextmenü eines erteilten Rechts enthält den Menübefehl **Rechtekonfiguration anzeigen**, über den eine Liste aller Objektattribute (Namen und Domänen) angezeigt werden kann, für die dem Anwender bzw. der Anwendergruppe dieses Recht erteilt bzw. ausgeschlossen wurde. Die Spalte **Wert** zeigt den Namen des Objektes an.
Die Spalten **Tabelle** und **Spalte** werden in *grün* dargestellt, falls das Recht dem entsprechenden Objekt zugewiesen wurde. Sie werden in *rot* dargestellt, falls das Recht ausgeschlossen wurde.
Die beiden Spalten enthalten die Einträge `*/*` falls das Recht *global* zugewiesen wurde, die Einträge `group/leaf` falls das Recht *hierarchisch* zugewiesen wurde oder die Einträge `names/selectionName` falls das Recht *individuell* dem Objekt zugewiesen wurde.

15.6.2 Liste der Anwender bzw. Anwendergruppen für ein Recht

Um sich anzusehen, welchen Anwendern bzw. Anwendergruppen ein bestimmtes Recht erteilt wurde, wählen Sie **Anwender/Gruppen anzeigen** in dem Kontextmenü des speziellen Rechts aus: es wird eine Liste mit allen Anwendern bzw. Anwendergruppen angezeigt, die über dieses Recht verfügen, wobei jedes Recht auf ausgewählte Objekte beschränkt sein kann.

Die Spalte **Typ** zeigt an, ob ein Recht für einen Anwender („Anwender“) oder für eine Anwendergruppe („Gruppe“) erteilt wurde. Der Name des Anwenders bzw. der Anwendergruppe wird in der Spalte **Name** angezeigt. Wenn ein ausgewähltes Recht allen Objekten zugewiesen wurde (durch Verwenden der Schaltfläche **>>>>** in der Bedienoberfläche „Objektrechte zuweisen“), ist der Haken in der Spalte **Global** gesetzt. Andernfalls ist der Haken nicht gesetzt.

15.7 Objektrechte

Im folgenden Abschnitt werden Objektrechte behandelt. Es wird beschrieben, wie diese Rechte zugewiesen (*Abschnitt 15.7.1, „Zuweisen neuer Objektrechte“*) und wie sie wieder gelöscht werden können (*Abschnitt 15.7.2, „Löschen von Objektrechten“*).

15.7.1 Zuweisen neuer Objektrechte

Das Zuweisen von Objektrechten für einen Anwender bzw. eine Anwendergruppe beginnt in der Submap des Anwenders bzw. der Anwedergruppe. Zunächst müssen Sie auf das Symbol des Anwenders bzw. der Anwendergruppe in einer Ansicht (Baum oder Submap) gehen und das entsprechende Kontextmenü öffnen. Wählen Sie **Konfigurieren** und die Seite **Objektrechte** aus, um die Objektrechte-Bedienoberfläche zu öffnen. Wählen Sie aus dem **Rechte**-Baum auf der linken Seite das Recht aus, das Sie dem Anwender bzw. der Anwendergruppe zuweisen wollen. Wählen Sie anschließend das Objekt, für das Sie dieses Recht zuweisen wollen, aus dem **Objekte**-Baum in der Mitte aus. Diese Bäume sind spezielle Navigationsbäume, welche die OpenScape FM-Systemhierarchie von Rechten und Objekten darstellen. Die Zuweisung eines bestimmten Rechts schließt auch die untergeordneten Rechte ein.

Bitte beachten Sie, dass dies **nicht** für den **Objekte**-Baum gilt: im **Objekte**-Baum werden die untergeordneten Objekte **nicht automatisch hinzugefügt**. Sie müssen jedes Objekt auswählen, für das dieses Recht explizit eingeräumt werden soll. Über die `Strg`-Taste bzw. die `Umschalt`-Taste ist eine Mehrfachauswahl möglich, so dass Sie ein Recht einem Anwender gleichzeitig für mehrere Objekte zuweisen können.

Wenn Sie das Recht und das Objekt ausgewählt haben, klicken Sie auf die Pfeilschaltfläche **Zuweisen** / **>>** (die nach rechts zeigt): das Objekt wurde zu der rechten Spalte **Objekte für Recht** hinzugefügt.

Die für das markierte Recht ausgewählten Objekte erscheinen in der Liste **Objekte für Recht** auf der rechten Seite.

Um einem Anwender bzw. einer Anwendergruppe ein Recht global (für alle Objekte) zuzuweisen, klicken Sie auf die Schaltfläche **>>>>** (global zuweisen). Wenn es andere Objekte gegeben hat, sind diese grau gefärbt. Das Recht wurde auch für diese Objekte zugewiesen. Diese Objekte bleiben in der Liste, denn wenn Sie die globale Zuweisung über die Schaltfläche **<<<<** (global entfernen) entfernen, soll unter Umständen die vorherige Objektauswahl erhalten bleiben.

Wichtiger Hinweis:
Soll ein Recht für ein einzelnes Objekt unterhalb des Root-Containers vergeben werden, so sollten für alle Objekte, die sich in der Hierarchie zwischen dem Objekt und dem Root-Container befinden, zumindest **User**-Rechte vergeben werden. Dies betrifft das Objekt selbst, und alle Vater-Objekte bis hinauf zum Wurzel-Objekt der Map. Geschieht dies nicht, so kann der Anwender nicht zu dem betreffenden Objekt navigieren.

Beispiel:
Soll einem Anwender für ein Netzwerk das **Administrator**-Recht vergeben werden, so sollte der Anwender **User**-Rechte für das Wurzel-Objekt und die Netzwerk-Topologie erhalten.

Rechte ausblenden:
Mit den Schaltflächen **!>** bzw. **!>>>** kann ein Recht für ein einzelnes Objekt bzw. für einen Objektbaum ausdrücklich ausgeschlossen werden. Mit diesen Funktionen ist es möglich für einzelne Objekte global oder übergeordnet zugewiesene Rechte wieder zu negieren. Um festzulegen, ob für ein Objekt ein Recht vorliegt oder nicht, überwiegt stets das speziellere Recht. D.h. es wird der Pfad vom Objekt zur Wurzel verfolgt, bis eine einschließende oder ausschließende Rechte-Zuweisung gefunden wird.

Rechteanzeige:
Öffnen Sie die Submap eines Anwenders oder einer Anwendergruppe, um die entsprechenden Zugriffsrechte anzuzeigen. Öffnen Sie die Sicht des gewünschten Anwenders bzw. der gewünschten Anwendergruppe. Alle zugewiesenen Rechte werden als Rechtesymbole im „Zugewiesene Rechte“ Container dargestellt, wobei die Rechte möglicherweise nur für ausgewählte Objekte gelten.

15.7.2 Löschen von Objektrechten

Um einem bestimmten Anwender oder einer bestimmten Anwendergruppe ein Recht oder einen Rechteausschluss zu entziehen, öffnen Sie die Objektrechte-Bedienoberfläche über das Kontextmenü des Anwenders bzw. der Anwendergruppe. Wählen Sie das Recht in der Spalte **Rechte** aus. Nun werden die Objekte, für die das Recht erteilt wurde, in der Spalte **Objekte für Recht** aufgelistet. Markieren Sie das/die Objekt(e), für die das Recht nicht mehr gelten soll, und klicken Sie auf die nach links zeigende Pfeilschaltfläche **Entfernen** / **<<**.

Wenn Sie das Recht für alle Objekte zugewiesen haben (über die Schaltfläche **>>>>** / global zuweisen), müssen Sie auf die Schaltfläche **<<<<** (global entfernen) klicken, um das Recht zu entfernen.

Sie können ein erteiltes Recht auch über den Standard-Menübefehl **Bearbeiten->Objekt Löschen** löschen. In diesem Fall wird das Recht für alle Objekte, für die es freigegeben war, entzogen (für den aktuellen Anwender).

15.8 Domänen

Einige Unternehmen, die über große Netzwerke verfügen, beschäftigen eine ganze Belegschaft von Servicetechnikern. Bei diesen Unternehmen ist es möglicherweise erforderlich, dass bestimmte Gruppen von Technikern bestimmte Wartungsaufgaben an speziellen Teilbereichen des gesamten Netzwerks durchführen. Außerdem soll nicht jeder Techniker in einer Servicegruppe in der Lage sein, jede Wartungsaufgabe durchzuführen. Daher ist es unbedingt erforderlich, dass unterschiedlichen Personen spezielle Rechte für den gleichen Teilbereich des Netzwerks zugewiesen werden können.

In einer solchen Umgebung bietet die Mandatfähigkeit die Lösung: sie ermöglicht es, Objektgruppen (Domänen) zu definieren und für alle Objekte in einer Domäne anwender-/anwendergruppen-spezifische Rechte zuzuweisen. Auf diese Weise kann ein Administrator oder Servicetechniker zum Beispiel das System eines bestimmten Netzwerks „A“ (in Domäne „A“ enthalten) verwalten, er kann jedoch nicht auf Daten eines anderen Netzwerks „B“ (in Domäne „B“ enthalten) zugreifen.

OpenScape FM unterstützt hierfür so genannte „Domänen“. Eine Domäne stellt eine Objektgruppe dar.

Wichtiger Hinweis:
Hinsichtlich der Rechte eines Anwenders bzw. einer Anwendergruppe für ein Objekt spielt es keine Rolle, ob diese Objektrechte als spezifische Objektrechte oder als Rechte für die Domäne, zu der das Objekt gehört, erhalten hat. Die Anwenderrechte für ein Objekt sind also die Summe aller Rechte, die entweder als Einzelrechte (über die Seite **Objektrechte**) oder als Mandatrechte (über die Seite **Domänenrechte**) erteilt wurden.

Wenn Sie einem Anwender bzw. einer Anwendergruppe den Zugriff auf eine Domäne einräumen wollen, müssen Sie zwei Schritte ausführen: eine Domäne erstellen (siehe *Abschnitt 15.8.1, „Anlegen einer Domäne“*) und dem Anwender bzw. der Anwendergruppe die Rechte für diese Domäne zuweisen (siehe *Abschnitt 15.8.5, „Zuweisung von Domänenrechten“*). Änderungen in Domänen werden sofort auf die einem Anwender/einer Anwendergruppe erteilten Mandatrechte übertragen.

Über eine Option im Hauptmenü können Sie sich rasch einen Überblick über alle vorhandenen Domänen verschaffen (siehe *Abschnitt 15.8.4, „Schneller Überblick über alle Domänen“*).

15.8.1 Anlegen einer Domäne

Das zentrale Objekt für Domänen befindet sich im Navigationsbaum an der Position **Root->Anwender Verwaltung->Domänen**.

Neue Domänen können erstellt werden, indem aus dem Kontextmenü dieses Objektes der Eintrag **Neu->Domäne** ausgewählt wird. In dem sich öffnenden Fenster kann ein eindeutiger Name für die neue Domäne und ein Beschreibungstext angegeben werden.

Es wird ein neues Domain-Containerobjekt erzeugt und auf der Submap des Domänen-Objektes platziert.

15.8.2 Einfügen eines Objekts in eine vorhandene Domäne

Alle Objekte, die zu einer Domäne gehören, befinden sich als Kopie auf der Submap des entsprechenden Domänen-Containerobjektes.

Objekte können per Kopieren/Einfügen oder per Drag&Drop innerhalb des Navigationsbaumes in die Sumbap des Domänen-Symbols eingefügt und so der Domäne hinzugefügt werden.

Alternativ kann für ein beliebiges Objekt der Menüeintrag **Eigenschaften...** ausgeführt werden.

Auf der Seite **Domänen** der sich öffnenden Seite sind alle definierten Domänen aufgelistet. Über die **>>** Pfeiltaste können ausgewählte Domänen dem aktuellen Objekt hinzugefügt werden. Ein Doppelklick auf einen Eintrag verschiebt ihn aus einer Liste in die andere.

15.8.3 Löschen eines Objekts aus einer Domäne

Objekte werden aus einer Domäne entfernt, indem ihr Symbol aus dem entsprechenden Domänen-Containerobjekt entfernt werden. Dies kann durch die Ausführung des Menüeintrages **Bearbeiten->Symbol Entfernen** geschehen.

Alternativ kann für ein beliebiges Objekt der Menüeintrag **Eigenschaften...** ausgeführt werden.

Auf der Seite **Domänen** der sich öffnenden Seite sind alle definierten Domänen aufgelistet. Über die **<<** Pfeiltasten können ausgewählte Domänen für das aktuellen Objekt entfernt werden. Ein Doppelklick auf einen Eintrag verschiebt ihn aus einer Liste in die andere.

15.8.4 Schneller Überblick über alle Domänen

Aus dem Hauptmenü kann über **Server**–>**Administration->Anwender Verwaltung** ein Navigationsbaum mit einem Container **Domänen** geöffnet werden, der alle Domänen und alle darin enthaltenen Objekten anzeigt.

15.8.5 Zuweisung von Domänenrechten

Der Prozess der Zuweisung von Mandatrechten entspricht weitgehend dem Prozess der Zuweisung von Objektrechten (*Abschnitt 15.7.1, „Zuweisen neuer Objektrechte“*). Zunächst müssen Sie auf das Symbol des Anwenders bzw. der Anwendergruppe gehen, dem Sie Zugriffsrechte erteilen wollen, **Konfigurieren...** aus dem Kontextmenü auswählen und auf die Seite **Domänenrechte zuweisen...** wechseln.

Rechte können, wie für Objektrechte beschrieben, erteilt oder ausgeblendet werden. In diesem Fall werden im Baum **Domänen** die Domänen ausgewählt, für die ein Recht erteilt oder ausgeblendet werden soll.

Die Rechte werden dann für alle Objekte der entsprechenden Domäne erteilt oder entzogen, die in der Domäne enthalten sind, wenn das Recht benötigt wird.

15.9 Aktuelle Zugriffsrechte

Die Zugriffsrechte auf ein einzelnes Objekt und dessen Funktionen können von einer Vielzahl von Regeln beeinflusst werden.

Regeln können für das Objekt selbst, hierarchisch oder global definiert sein.

Verschiedenen Anwendern oder Anwender-Gruppen können verschiedene Rollen-Rechte oder sogar Zugriffsverbote erteilt worden sein.

Um einen Überblick über die Zugriffsrechte zu erhalten, die einem spezifischen Objekt zugewiesen sind, kann der Eintrag **Eigenschaften** aus dem Kontextmenü des Objektes ausgewählt und die Seite **Zugewiesene Objekte** geöffnet werden.

Die Seite enthält eine Tabelle in der jede Zeile für eine Zugriffsrechte-Regel steht, die einen Einfluss auf das aktuelle Objekt haben kann (siehe *Abschnitt 15.3*).

Die Spalte **Typ** zeigt, ob eine Regel speziell für das Objekt (*Objekt*), hierarchisch (*Hierarchisch*) oder für alle Objekte gilt (*Global*).

Die Spalte **Name** zeigt an, für welchen Anwender oder welche Anwender-Gruppe die Regel zugewiesen wurde.

Die Spalte **Recht** zeigt an, für welches Zugriffsrecht oder für welche Rolle, die Regel gilt.

Die Spalte **Objekt** führt das Objekt auf, dem die Regel zugewiesen wurde. Bei hierarchischen Zuweisungen ist dies das Wurzelobjekt der Hierarchie. Der Eintrag ist grün für erlaubende und rot für verbietende Regeln.

Wichtiger Hinweis:
Die Seite zeigt nicht an, welche Rechte gerade wirksam sind, sondern alle Regeln, die das aktuelle Recht betreffen könnten. Die wirksamen Rechte können jedoch aus der Liste bestimmt werden (siehe *Abschnitt 15.4*).

Wichtiger Hinweis:
Die Seite kann verbietende Regeln enthalten, die nicht explizit definiert , sondern implizit durch das System erstellt wurden. Z.B. generiert die Rolle *Operator* auf dem gleichen Objekt eine verbietende Regel für die Rolle *Administrator*.

16 Netzwerk Topologie Verwaltung

Das Topologie Manager Plugin wird vom OpenScape FM als allgemeine Grundlage für eine einheitliche Topologiedarstellung verwendet.Der Topologie Manager erzeugt initial ein neues Objekt auf der Root-Sicht. Dieses Objekt erhält die Bezeichnung '*Netzwerk Topologie*'. Dieses Objekt und der darunter liegende Objektbaum ist die zentrale Sammelstelle für alle Topologie-Objekte.

Der Topologie Manager ist verantwortlich für die Darstellung und die Verwaltung von komplexen hierarchischen Topologien, die aus Knoten, Kanten und Container-Objekten bestehen. Dabei werden die Knoten und Kanten durch OpenScape FM Desktop Technologie Plugins generiert. Knoten repräsentieren real existierende Netzwerk-Elemente und deren Sub-Komponenten wie z.B. Untersysteme, Boards oder Software-Module. Kanten repräsentieren physikalische oder logische (Kommunikations-) Verbindungen zwischen Knoten. Für HiPath 4000 Systeme z.B. wird eine Kante verwendet, um eine Verbindungen zwischen einem Quell- und einem Ziel-HiPath 4000 System (Knoten) darzustellen. Der Topologie Manager wertet die Verbindungen aus, um eine hierarchische Struktur zu erzeugen, die die Konnektivität visualisiert.

Bei der hierarchischen Anordnung von Knoten und Kanten werden Container-Objekte implizit erzeugt. Diese werden durch den Topologie Manager verwaltet. Die Hierarchie ist frei konfigurierbar, und kann verwendet werden, um z.B. geographische, administrative oder andere organisatorische Strukturen darzustellen. Es gibt zwei unterschiedliche Typen von Container-Objekten: Netzwerk-Container und Teilnetzwerk-Container. Sinn dieser Unterscheidung ist es, eine optimale Darstellung auch Komplexer Netzwerkstrukturen zu ermöglichen.

Netzwerk- und Teilnetzwerk-IDs bieten die Möglichkeit die Struktur des Hierarchie-Baumes zu bestimmen. Durch ihre Angabe wird ein Pfad bestimmt, der angibt, wo der Knoten in dem Hierarchie-Baum eingegliedert wird. Basierend auf der Netzwerk- und Teilnetzwerk-Id, die einem Knoten zugeordnet ist, erstellt der Topologie Manager, automatisch die Netzwerk- und Teilnetzwerk-Container des Netzwerk-Baumes. Der Knoten selbst wird automatisch dem letzten Container des Pfades zugeordnet. Jeder Knoten besitzt einen Vaterknoten (z. B. seinen Netzwerk- oder Teilnetzwerk-Container) und kann Kindobjekte besitzen (z. B. Unter-Komponenten).

Ein neuer Topologie-Container kann erstellt werden, indem der Menüeintrag **Neu->Topologie Container...** ausgewählt wird. Neue Knoten können dem Container mit dem Menüeintrag **Neu->Netzknoten...** hinzugefügt werden. Bereits bekannte Knoten können mit Hilfe der Kopieren/Einfügen Funktionen oder mittels Drag&Drop in die Submap des Containers hinzugefügt werden.

16.1 Topologie und hierarchische Netzwerk Strukturen

Knoten, Kanten und Container-Objekte sind die Grundbausteine der hierarchischen Netzwerkstuktur. Container repräsentieren entweder ein Netzwerk oder ein Teilnetzwerk und werden durch den Topologie Manager verwaltet. Knoten repräsentieren u. a. IP-Knoten oder andere Systeme (z.B. HiPath 3000 Systeme oder HiPath 4000 Systeme). Knoten werden von den entsprechenden Plugins verwaltet. So ist z. B. das IP Manager Plugin für die Verwaltung der IP-Knoten verantwortlich.

Einem Knoten kann eine Netzwerk- und/oder eine Teilnetzwerk-Id zugewiesen werden. Diese Zuweisung bestimmt die Position des Knotens innerhalb des Topologie-Baumes und der Topologie Manager trägt die Verantwortung für die Verwaltung und Erzeugung dieses Baumes. Die Zuweisung von Netzwerk- oder Teilnetzwerk-Ids kann entweder durch IP-Discovery-Regeln oder durch den Anwender (siehe *IP Manager Plugin Bedienungsanleitung*) erfolgen. Wird einem Knoten weder eine Netzwerk- noch eine Teilnetzwerk-Id zugewiesen,

wird dieser Knoten nicht vom Topologie Manager verwaltet. Der Knoten wird dann nur innerhalb der Plugin-spezifischen Sichten dargestellt (ein IP-Knoten z.B. wird dem IP-Knoten-Container seines Vaterknotens zugeordnet.)

Zunächst werden die meisten IP Knoten nicht durch den Topologie Manager verwaltet. Wenn IP-Knoten neu erkannt werden, werden sie zunächst der IP-Container-Sicht zugeordnet (IP-Container sind Kindobjekte des zugehörigen IP-Netzwerkes). Nur wenn IP-Discovery-Regeln, die die Zuordnung von Standard-Netzwerk-Ids und Standard-Teilnetzwerk-Ids bestimmen, gefunden werden, werden sie durch den Topologie Manager verwaltet.

Es gibt eine Reihe von Netzwerk-Elementen, die nicht frei im Topologie-Baum angeordnet werden können. Beispielsweise werden Unterkomponenten eines Knotens immer relativ zu ihrem Vaterknoten angeordnet. Ihre Position kann nicht durch die Angabe einer Netzwerk- oder Teilnetzwerk-Id beeinflußt werden.
IP-Netzwerke werden durch den IP-Manager kreiert und werden nicht wie Knoten behandelt. Zwar können IP-Netzwerke ebenfalls im Topologie-Baum angeordnet werden, der zugehörige IP-Container bekommt aber stets eine Position relativ zu seinem IP-Netzwerk zugewiesen und kann nicht separat positioniert werden.

16.1.1 Konfiguration Hierarchischer Netzwerke

Wie bereits erwähnt, unterstützt OpenScape FM Desktop die hierarchische Strukturierung von Netzwerken, um Administratoren in die Lage zu versetzen, klar arrangierte graphische Repräsentationen zu erzeugen. Dies ist insbesondere dann hilfreich, wenn große Netzwerke so graphisch dargestellt werden sollen, dass eine eingängige Struktur entsteht, und der Netzwerk Administrator unterschiedliche Abstraktions-Sichten verwenden möchte. Unternehmensbezogene Strukturprinzipien können gewählt werden: z.B. kann die Struktur eines Firmennetzwerkes so gewählt werden, dass sie nach geographische oder organisatorischen Gesichtspunkten aufgebaut wird. Im ersten Fall könnten unterschiedliche Länder durch Topologie-Container dargestellt werden. Im zweiten Fall könnten die Topologie-Container unterschiedliche Abteilungen symbolisieren. Der folgende Abschnitt geht eingehender auf dieses Thema ein.

Ein Netzwerk wird strukturiert durch die Anordnung von Knoten (Netzwerk-Elementen) innerhalb einer konzeptionellen Hierarchie, die durch den Netzwerk-Administrator definiert wird. Es gibt zwei Parameter, die im Allgemeinen verwendet werden, um die Position eines Knotens innerhalb der Hierarchie zu bestimmen: die Netzwerk-Id und die Teilnetzwerk-Id. Aus Gründen der Vollständigkeit soll hier ebenfalls die Primäre-Domänen-Id erwähnt werden, obwohl sie für die hierarchische Strukturierung nicht notwendig ist.

- Die **Netzwerk Id** definiert einen Pfad (siehe unten) durch die Hierarchie bzw. den Baum zu einem Topologie-Container in dem der Knoten plaziert werden soll.
- Die **Teilnetzwerk Id** stellt eine zusätzliche Möglichkeit bereit, um die Netzwerk-Hierarchie zu strukturieren. Der Hauptvorteil bei der Verwendung von Teilnetzwerken besteht in der Verkürzung der Bezeichner, die den Pfad beschreiben (siehe *Bild 21*). Außerdem werden Teilnetzwerke durch ein spezielles Teilnetzwerk-Symbol dargestellt.
- Die **Primäre Domänen Id** wird für Kanten verwendet, und identifiziert die Ziel-Domäne in welche der Zielknoten der Kante gefunden werden soll. Dies wird in *Abschnitt 16.4* genauer beschrieben.

Die **Netzwerk-Id** zusammen mit der **Teilnetzwerk-Id** definiert einen Pfad durch einen Baum. Ein Pfad besteht dabei aus einer Serie von Namen, die durch das Zeichen “/” getrennt werden. Der erste Pfadname bestimmt die Wurzel, der letzte den Ziel-Topologie-Container. Jeder Name im Pfad identifiziert ein Container-Objekt, das

graphisch durch ein Netzwerk-Symbol repräsentiert wird. Alle Knoten mit der gleichen Netzwerk-Id (und Teilnetzwerk-Id Kombination) werden in den gleichen Ziel-Topologie-Container gruppiert und in der Submap dieses Containers angezeigt.

In dem in *Bild 21* gezeigten Beispiel wird für den Knoten ‘System 121’ ein Netzwerk und zwei Teilnetzwerke erzeugt: Ein Netzwerk “Country A” mit dem Kindobjekt/Teilnetzwerk “State P” welches selbst das Kindobjekt/ Teilnetzwerk “State P/Town Y” enthält. Die Objektbezeichner stellen bereits die Netzwerk-Hierarchie da, was den Überblick über große Netzwerk-Strukturen erleichtert.

Soll das Zeichen”/” selbst in einem Namen verwendet werden, ohne dass ein neuer Topologie-Container erzeugt werden soll, muß dem Zeichen ein zweites “/” Zeichen vorangestellt werden.

Es können auch mehrere Knoten gleichzeitig in die Netzwerk-Hierarchie bzw. in Topologie-Container eingeordnet werden. Im nächste Abschnitt wird dieses Verfahren näher beschrieben.

Wird durch die Zuordnung von Knoten zu einem Topologie-Container ein neues (Teil-)Netzwerk konfiguriert, oder wird ein Topologie-Container vollständig geleert, so wird die Topologie-Darstellung sofort aktualisiert.

16.1.1.1 Mengen-Operationen für die Zuweisung von Netzwerk- und Teilnetzwerk-Ids

Das Kontextmenü des Topologie-Netzwerk-Symbols ist der Ausgangspunkt für alle Mengen-Operationen. Um die Topologie-Parameter für mehrere Knoten eines Topologie-Containers gleichzeitig zu ändern oder zu betrachten, muss der Menüeintrag **Eigenschaften...** selektiert werden. Dies öffnet einen Browser/Dialog, der auf der Seite **Topologie->Netzwerk Konfiguration** eine Liste der Topologie-Parameter aller Knoten des Containers enthält (siehe *Bild 21*). Hier können ein oder mehrere Knoten selektiert, und eine neue Netzwerk- oder Teilnetzwerk-Ids zugewiesen werden. Das Drücken der jeweiligen  Schaltfläche schließt die Operation ab. Die Topologie-Sicht wird sofort aktualisiert.

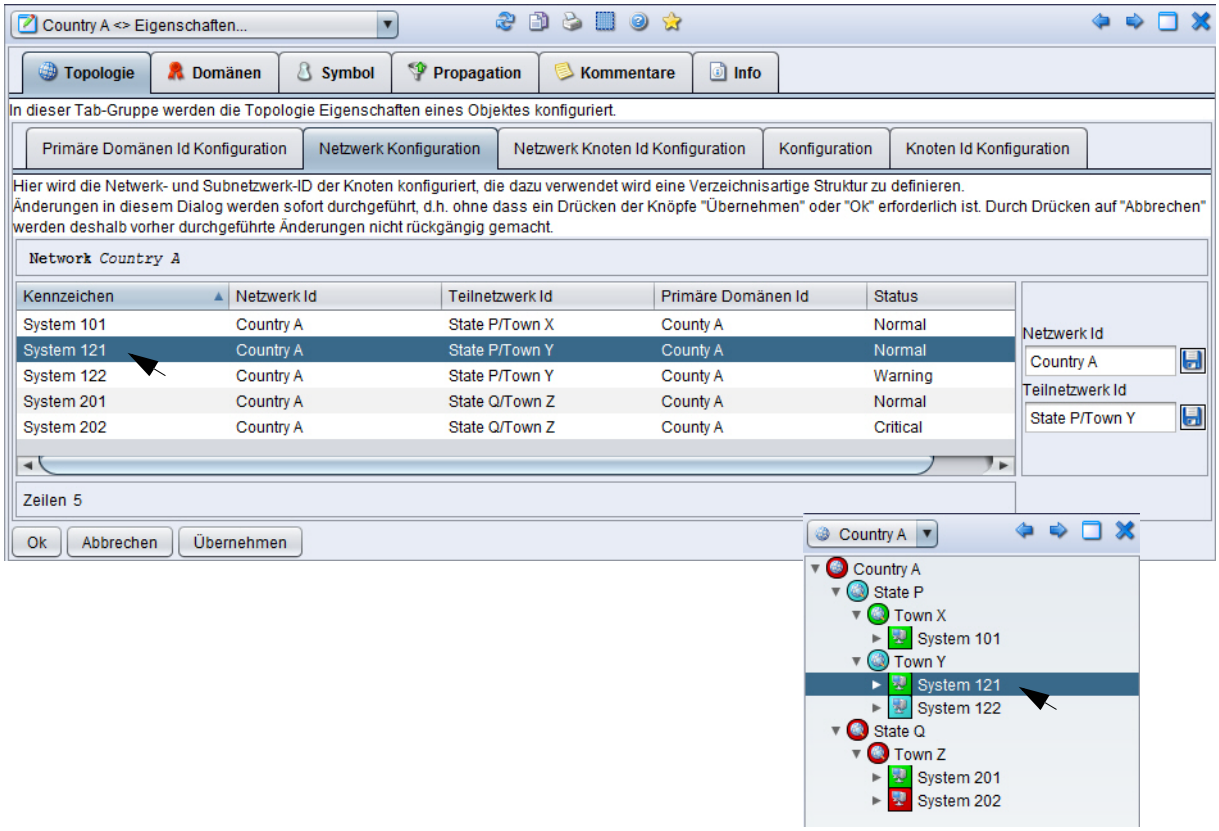


Bild 21 *Konfiguration der Netzwerk-Parameter als Mengen-Operation*

16.1.1.2 Mengen-Operation für die Zuweisung der Primären-Domänen-Id

Um die Primäre-Domänen-Id für mehrere Knoten eines Topologie-Containers gleichzeitig zu setzen/ändern, kann der Menüeintrag **Eigenschaften...** aus dem Kontextmenü des Netzwerk-Containers selektiert werden. Es öffnet sich ein Browser, der auf der Seite **Topologie->Primäre Domänen Id Konfiguration** eine Liste der Parameter aller Knoten des Netzwerk-Containers enthält. Um die Primäre-Domänen-Id für spezifische Knoten zu setzen, müssen die entsprechenden Knoten selektiert und die Schaltfläche betätigt werden.

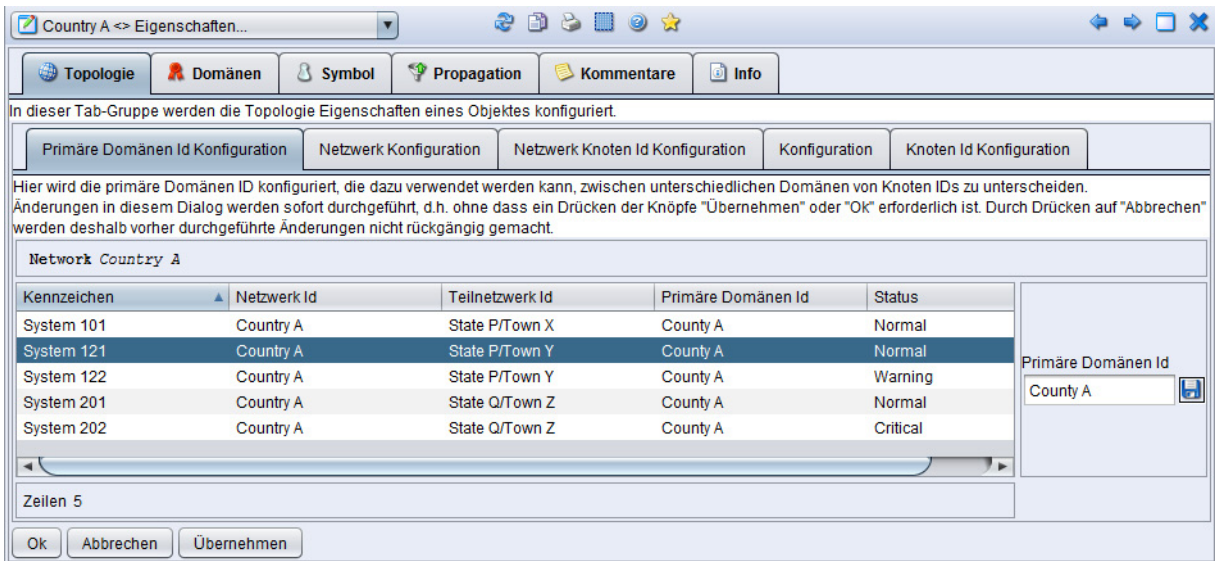


Bild 22 Mengen-Operation für die Konfiguration der Primären-Domänen-Id

16.1.1.3 Zuordnung von Netzwerk-, Teilnetzwerk- und Primärer-Domänen-Id auf Knoten-Ebene

Natürlich können die Netzwerk-, Teilnetzwerk- und Primäre-Domänen-Id auch im Kontext eines einzelnen Knotens definiert werden. Wird der Menüpunkt **Eigenschaften...** aus dem Kontextmenüs eines Knotens ausgewählt, können auf der Seite **Topologie->Konfiguration** die Parameter Netzwerk-Id, Teilnetzwerk-Id und Primäre-Domänen-Id des Knotens eingegeben werden.

Sind mehrere Knoten selektiert, kann diese Konfiguration ebenfalls über den Menüpunkt **Eigenschaften** eines der Knoten stattfinden. Dazu können einzelne Knoten in der auf der Seite **Topologie** angezeigten Liste ausgewählt, und über die Felder rechts die einzelnen Werte angepasst werden.

16.2 Topologie-Kanten und hierarchische Konnektivität

Topologie-Kanten werden verwendet, um die Verbindung zwischen einem Start- und einem oder mehreren Zielknoten zu repräsentieren. In diesem Fall stellt eine Kante eine gerichtete Verbindung dar, die bei ihrem Startknoten beginnt und im Zielknoten endet. Gerichtete Kanten repräsentieren einen spezifischen Verbindungstyp, der an jeweils einen spezifischen Startknoten gebunden ist. Sie verbinden den Startknoten mit dem Zielknoten, aber nicht umgekehrt. Gerichtete Kanten werden beispielsweise verwendet, um die Konnektivität von HiPath 3000 Ports oder HiPath 4000 Bündeln zu repräsentieren.

Existiert zusätzlich eine gerichtete Verbindung vom Zielknoten zum Startknoten, bezeichnet man die Kante als bi-direktional. IP-Interfaces stellen ein Beispiel für bi-direktionale Kanten dar.

Der Startknoten einer Kante wird bei der Erzeugung der Kante festgelegt, und bleibt für immer unverändert. Der/die Zielknoten einer Kante können verändert werden.

Die **Zielknoten-Id**(s), die einer Kante zugeordnet sind, werden benötigt, um den oder die Zielknoten der Kante zu bestimmen. Der Topologie Manager überprüft automatisch, ob in der Topologie Knoten vorkommen, deren Knoten-Id mit der **Zielknoten-Id** einer Kante entsprechen. Ist dies der Fall, wird überprüft, ob sich der Knoten in der gleichen **Domäne** wie die Kante befindet (siehe *Abschnitt 16.4, „Domänen-Ids und Ziel-Domänen-Ids“*). Tritt dies ebenfalls zu, wird dieser Knoten zu einem Zielknoten der Kante. Dieser Vorgang wird “implizite Zielknoten-Zuweisung” genannt.
Zusätzlich gibt es auch die “explizite Zielknoten-Zuweisung”. Diese kann z.B. durch verschiedene Plugins (z.B. für IP-Interface-Kanten) oder manuell durch den Anwender verwendet werden. Eine explizite Zuweisung, die durch den Anwender erfolgt, kann später rückgängig gemacht werden. In diesem Fall werden vom Topologie Manager bereits vorhandene implizite Zuweisungen erneut verwendet, um die Zielknoten der betroffenen Kante zu bestimmen. Die Konfiguration von expliziten Zielknoten-Zuweisungen wird in *Abschnitt 16.3, „Manuelle explizite Zielknoten-Zuweisung“* behandelt.

Üblicherweise ist einer Kante lediglich ein einziger Zielknoten zugeordnet. In einigen Netzwerk-Umgebungen werden einzelnen Kanten jedoch mehrere Zielknoten zugewiesen. Wie mehrfache Zielknoten verwendet und repräsentiert werden, ist in *Abschnitt 16.5, „Verwendung von Mehrfach-Zielknoten“* beschrieben.

Kann für eine Kante kein passender Zielknoten gefunden werden, wird ein “Fremdsystem” erzeugt. Dieses “Fremdsystem”-Objekt wird in der gleichen Sicht dargestellt wie der Startknoten der Kante.

16.2.1 Meta-Kanten

Meta-Kanten werden verwendet, um die Konnektivität zwischen zwei Knoten in der Topologie-Hierarchie zu repräsentieren. Eine Meta-Kante ist ein Kanten-Container, der eine oder mehrere einfache Kanten-Objekte repräsentiert und enthält. Wird das letzte Kanten-Objekt aus einer Meta-Kante entfernt, wird die Meta-Kante gelöscht.

Meta-Kanten werden ausschließlich vom Topologie Manager erzeugt und dienen dazu, die hierarchische Konnektivität zwischen zwei Topologie-Knoten/-Containern darzustellen. Jede Meta-Kante besitzt genau einen Start- und einen Ziel-Knoten/-Container. Jede Kante, die vom Topologie Manager verwaltet wird, ist das Kindobjekt von mindestens einer Meta-Kante. Abhängig von der hierarchischen Netzwerkstruktur, können Kanten aber auch in mehreren Meta-Kanten enthalten sein. Die Kindobjekte einer Meta-Kante sind der Startknoten und der durch die Zielknoten-Id der Kante definierte(n) Zielknoten.

Um beschreiben zu können, warum und wann Meta-Kanten erzeugt werden, wird der Begriff “Knoten-Unterhierarchie” eingeführt. Diese beschreibt eine Menge von Knoten. Die zu einem spezifischen Knoten gehörende “Knoten-Unterhierarchie” besteht aus dem Knoten selbst, aus allen Knoten, die über von dem Knoten ausgehende Kindbeziehungen erreicht werden können und aus dem “Wurzelknoten” (siehe unten).

In *Bild 23* wird die Knoten-Unterhierarchie des Teilnetzwerkes “State P” dargestellt. Mitglieder der Unterhierarchie sind das Teilnetzwerk “State P” als Wurzelknoten, alle in “State P” enthaltene Knoten, alle untergeordneten Topologie-Container und alle in diesen enthaltene Knoten.

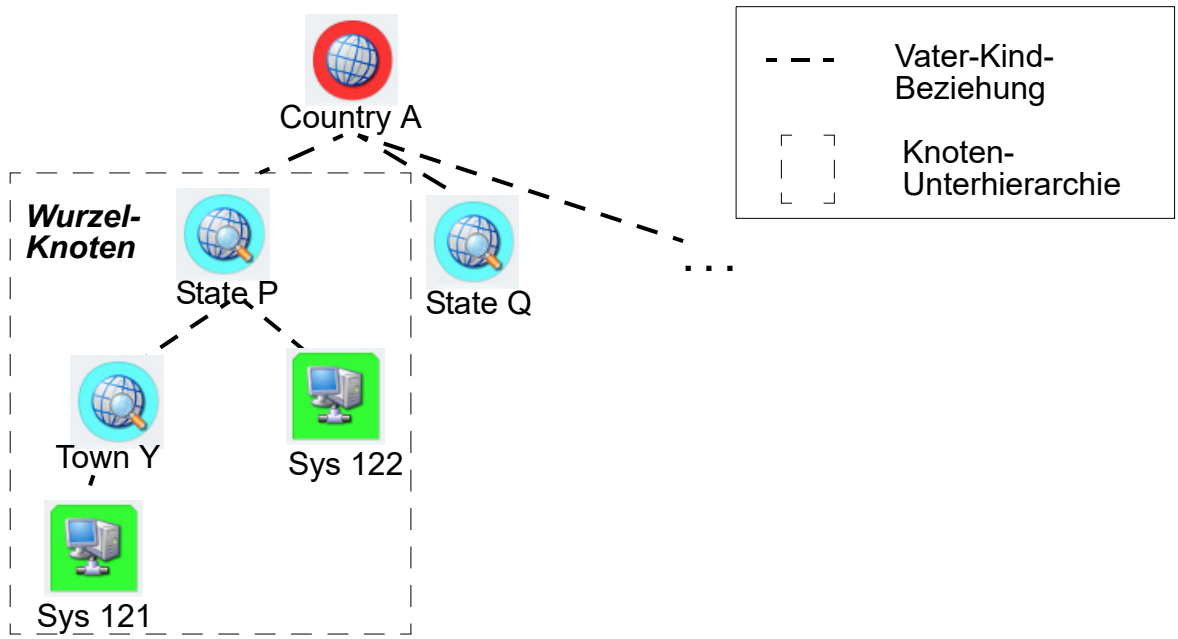


Bild 23 *Knoten-Unterhierarchie*

Eine Meta-Kante, die den Knoten “Start” mit dem Knoten “Ziel” verbindet, repräsentiert eine Konnektivität zwischen zwei “disjunkten” Knoten-Unterhierarchien. Disjunkt bedeutet, dass kein Knoten existiert, der in beiden Knoten-Unterhierarchien enthalten ist. Die Wurzelknoten zweier verbundener Knoten-Unterhierarchien besitzen den gleichen Vaterknoten. Der Wurzelknoten der Knoten-Unterhierarchie, die “Start” enthält, wird im folgenden “Start-Wurzel” genannt, der Wurzelknoten des Knotens “Ziel” “Ziel-Wurzel”.

Die folgenden Zeichnungen präsentieren Beispiele unterschiedlicher Knoten-Unterhierarchien.

Bild 24 zeigt ein Beispiel, bei dem sich der Start- und der Ziel-Knoten im gleichen Teilnetzwerk (Sicht) befinden. Sie besitzen das gleiche Vaterobjekt. Daher ist der Knoten “Start” gleichzeitig der Startknoten und die Start-Wurzel und der Knoten “Ziel” ist gleichzeitig der Zielknoten und die Ziel-Wurzel.

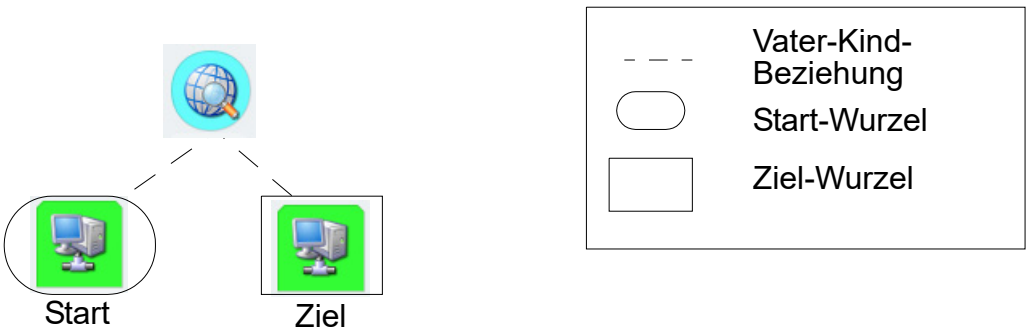


Bild 24 *Start- und Ziel-Knoten in der selben Sicht*

Bild 25 zeigt das Erste von drei Beispielen, bei denen sich der Start- und der Ziel-Knoten in unterschiedlichen Sichten befinden. In diesem Beispiel gehört der Startknoten zum Teilnetzwerk “Dortmund”. Da “Ziel” und “Dortmund” sich in der gleichen Sicht befinden, besitzen sie, in diesem Fall mit dem Teilnetzwerk “State P”, den gleichen Vater. Aus diesem Grund ist “Town Y” die Start-Wurzel und “Ziel” ist der Zielknoten und die Ziel-Wurzel.

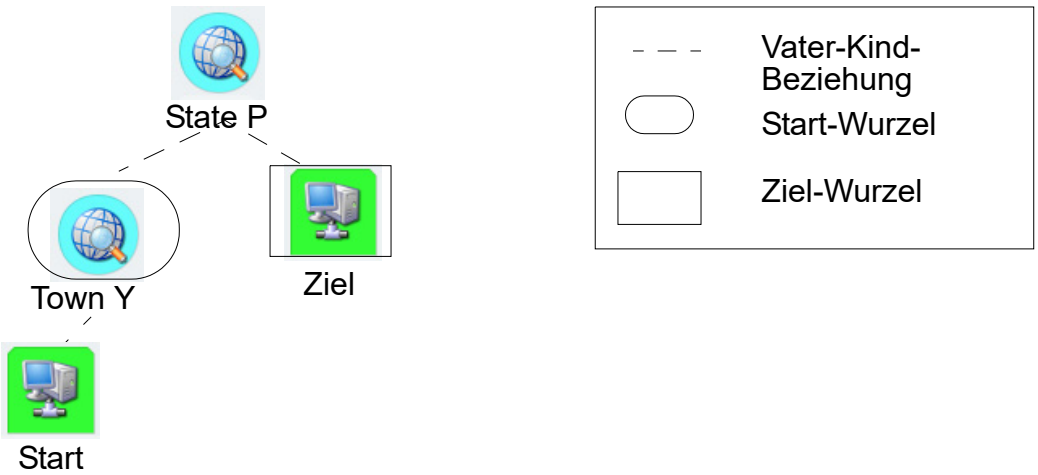


Bild 25 *Start- und Ziel-Knoten in verschiedenen Sichten (1)*

In *Bild 26* ist der Knoten “Start” sowohl Startknoten wie auch Start-Wurzel und der Knoten “Ziel” gehört zu einem Teilnetzwerk (“Town X”), welches auch die Ziel-Wurzel ist.

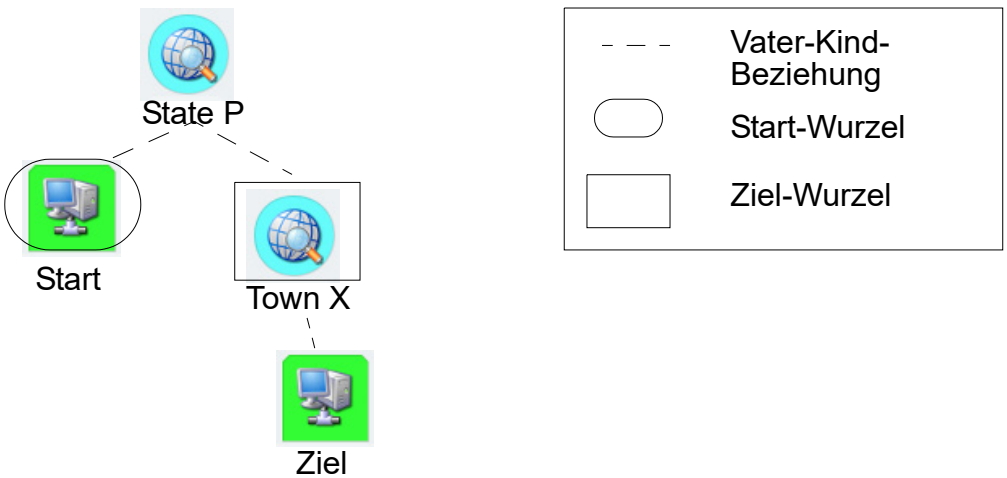


Bild 26 *Start- und Ziel-Knoten in verschiedenen Sichten (2)*

Bild 27 zeigt ein Beispiel, bei dem sich die Knoten “Start” und “Ziel” in unterschiedlichen Sichten befinden, nämlich den Teilnetzwerken “Town Y” und “Towmn X”. Da beide Teilnetzwerke den gemeinsamen Vater “State P” besitzen, ist “Town Y” die Start-Wurzel von “Start” und “Town X” ist die Ziel-Wurzel von “Ziel”.

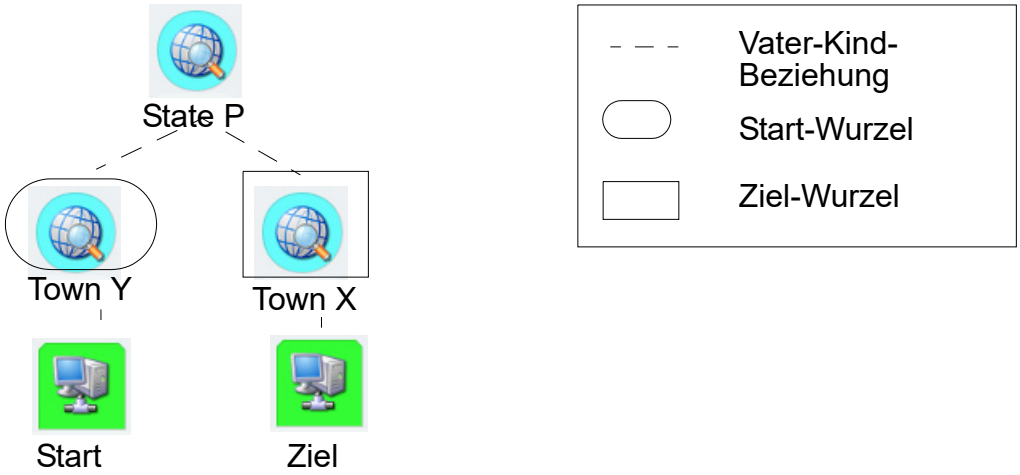


Bild 27 Start- und Ziel-Knoten in verschiedenen Sichten (3)

Ist ein Startknoten mit einem Zielknoten verbunden, so werden Meta-Kanten generiert, die vom Startknoten, der Start-Wurzel und allen Topologie-Containern dazwischen ausgehen, und zur Ziel-Wurzel führen. Die Ziel-Wurzel ist das Zielobjekt der Meta-Kante und die Start-Wurzel bestimmt, wie viele Meta-Kanten gezeichnet werden. Die Konnektivität zwischen dem Start- und dem Zielknoten ist so in allen Ebenen zwischen dem Startknoten und der Start-Wurzel innerhalb der Knoten-Unterhierarchie sichtbar, zu welcher der Startknoten gehört.

Ist zum Beispiel der Knoten “Start” zugleich die Start-Wurzel, wird lediglich eine Meta-Kante, die “Start” und “Ziel” verbindet, erzeugt.

Ist “Start” nicht die Start-Wurzel, so werden mehrere Meta-Kanten generiert, die mit der Ziel-Wurzel verbunden werden. Diese sind:

- der Knoten “Start”,
- die Start-Wurzel des Knotens “Start”,
- und alle Topologie-Container, die sich auf dem Pfad zwischen “Start” und der Start-Wurzel befinden.

Befindet sich das Startobjekt einer Meta-Kante nicht in der selben Sicht wie die zugehörige Ziel-Wurzel, so wird ein **Referenzsymbol** erzeugt, das die Ziel-Wurzel repräsentiert und die Verbindung wird mit diesem Referenzsymbol verbunden.

16.2.2 Referenzsymbole

Referenzsymbole sind Platzhalter für Symbole, die sich auf anderen Submaps befinden. Sie unterscheiden sich von einem normalen Symbol optisch darin, dass ihre Statusfarbe etwas heller dargestellt wird, und der ursprüngliche Bezeichner in << >> Klammern eingeschlossen ist.

16.3 Manuelle explizite Zielknoten-Zuweisung

In einigen Fällen ist es möglich, die durch die Plugins erstellte implizite Zielknoten-Zuweisung durch eine explizite Zielknoten-Zuweisung zu überschreiben. Mit anderen Worten: Einer existierenden Kante soll ein neuer Zielknoten zugewiesen werden, was den gleichen Effekt hat, als würde die alte Kante zu einem neuen Zielknoten umgeleitet werden. Beispielsweise kann eine Verbindung zwischen den Knoten System1 und System2 so konfiguriert werden, dass sie nun System1 mit System3 verbindet. Falls es möglich ist auf physikalischer Ebene einer Kante mit Hilfe von Konfigurationsfunktionen des zugehörigen Element-Manager einen neuen Zielknoten zuzuweisen (z.B. die direkte Konfiguration eines HiPath 4000 Bündels), ist es sinnvoll diese Konfigurationsfunktionen zu verwenden. Die explizite Zuweisung sollte nur verwendet werden, wenn die Konfiguration auf der physikalischen Ebene nicht möglich ist, oder wenn Systeme unterschiedlicher Technologietypen verbunden werden sollen.

Für die explizite Zielknoten-Zuweisung muss zunächst der gewünschte Zielknoten mit Hilfe des in seinem Kontextmenü befindlichen Menüeintrages **Bearbeiten->Verknüpfen** vorgemerkt werden. Dann muss die zu konfigurierende Kante gesucht werden, der das neue Zielsystem zugewiesen werden soll. Im Kontextmenü dieser Kante muss der Menüeintrag **Bearbeiten->Zielsystem angeben** selektiert werden. Der Zielknoten der Kante wird dann sofort verändert und die Topologie-Darstellung der entsprechenden Sichten angepasst (d.h. Submaps und/oder Bäume).

Befinden sich das Quell- und das Ziel-Symbol auf der gleichen Submap, wird eine Verbindung zwischen den beiden Symbolen angelegt.

Befinden sich die System auf unterschiedlichen Submaps, kann ausgewählt werden, ob auf der Quell- und/oder Ziel-Submap entsprechende Referenzsymbole angelegt werden sollen.

Um die Zuweisung rückgängig zu machen, muss der Menüeintrag **Bearbeiten->Objekt Löschen** der entsprechenden Kante ausgewählt werden.

Wichtiger Hinweis:
Die Anwendung dieser Zuweisungsform beeinflusst ausschließlich die OpenScape FM Desktop Datenbasis. Um den Zielknoten einer Kante dauerhaft zu verändern, müssen die Funktionen der technologietyp-spezifischen Element-Manager verwendet werden, um diese zu löschen.

16.4 Domänen-Ids und Ziel-Domänen-Ids

Der folgende Abschnitt motiviert die Verwendung von “Domänen-Ids” und “Ziel-Domänen-Ids”.

Domänen-Ids sollten immer dann verwendet werden, wenn doppelte Knoten-Ids existieren, und dadurch der Namensraum für Knoten-Ids nicht mehr eindeutig ist. In diesem Fall können Domänen-Ids verwendet werden, um den Namensraum für die Knoten-Ids wieder eindeutig zu machen. Die Knoten-Id der Knoten wird um die Domänen-Id erweitert. Durch die Verwendung unterschiedlicher Domänen-Ids kann so die Eindeutigkeit wieder erreicht werden. Ein Knoten kann mehreren Domänen zugewiesen werden.

16.4.1 Identifizierung von Knoten durch die Domänen-Id/Knoten-Id

Eine Kante verbindet Knoten, einen Startknoten und einen oder mehrere Zielknoten. Die Kante besitzt eine Zielknoten-Id und eine Zieldomänen-Id, die vom Topologie Manager verwendet werden, um die Zielknoten zu finden und die Verbindungen zwischen den Knoten zu zeichnen. Kanten, die einen HiPath 3000 Port oder ein HiPath 4000 Bündel repräsentieren, haben eine entsprechende Zielknoten-Id. Die Zieldomänen-Id einer Kante entspricht der primären Domänen-Id des zugehörigen Startknotens. Im einfachen Fall, dass alle Knoten-Ids eindeutig sind und alle Knoten einer Domäne angehören, kann der Topologie Manager jede Kante dem richtigen Zielknoten zuordnen. In Netzwerkumgebungen, in denen identische Knoten-Ids existieren, d.h. in denen mehrere Knoten die gleiche Knoten-Id besitzen, ist der Administrator dafür verantwortlich, dass alle Kanten dem oder, in komplizierteren Fällen, den richtigen Zielknoten zugeordnet werden. Der Administrator muss alle Knoten näher bestimmen, die als Ziel für eine Kante dienen sollen. Dies sind die Knoten, die eine Knoten-Id besitzen, die der Zielknoten-Id der Kante entspricht, und bei denen die Domänen-Id der Zieldomänen-Id der Kante entspricht. Der Topologie Manager ist dann in der Lage eine Beziehung zwischen der Zielknoten-Id und der Zieldomänen-Id der Kante mit allen Knoten zu generieren, die ein passendes Knoten-Id/Domänen-Id Paar besitzen.

Jeder Knoten hat eine Menge von ihm zugewiesenen “Domänen-Id/Knoten-Id”-Paaren. Ein “Domänen-Id/Knoten-Id”-Paar kann durch ein Plugin oder manuell durch einen Anwender zugewiesen werden. Knoten-Ids können dabei nur in Verbindung mit einer Domänen-Id zugewiesen werden. Üblicherweise sollten alle “Domänen-Id/Knoten-Id”-Paare eines Knotens an die primäre Domänen-Id des Knotens gebunden sein. In einzelnen Fällen ist dies aber nicht der Fall. Beispielsweise wenn Verbindung erzeugt werden soll, die zwei Knoten in unterschiedlichen Domänen verbinden soll.

Alle Knoten, denen ein “Domänen-Id/Knoten-Id”-Paar zugewiesen ist, das dem “Zieldomänen-Id/Zielknoten-Id”-Paar einer Kante entspricht, bilden einen Zielknoten dieser Kante. In den meisten Fällen wird dies ein einzelner Knoten sein.

Automatische Anpassung im Falle von Domänen-Id/Knoten-Id-Paar-Zuweisungen:

Wird einem Knoten ein neues “Domänen-Id/Knoten-Id”-Paar zugewiesen, werden alle Kanten, deren Zielknoten diesem Paar entspricht, mit dem Knoten verbunden. Waren diese Kanten vorher mit einem Fremdsystem verbunden, werden die entsprechenden Kanten zum neuen Zielknoten umgeleitet, und die entsprechenden Fremdsysteme werden gelöscht.

Wird ein “Domänen-Id/Knoten-Id”-Paar eines Knotens gelöscht, werden die Zielknoten aller eingehenden Kanten aktualisiert. Wurde der letzte Zielknoten einer Kante entfernt, wird ein passendes “Fremdsystem” erzeugt, mit dem die betroffene Kante verbunden wird. Als Bezeichner des “Fremdsystems” wird die Zielknoten-Id verwendet.

16.5 Verwendung von Mehrfach-Zielknoten

Eine Kante, die ihr Ziel durch eine Knoten-Id identifiziert (z.B. HiPath 3000, HiPath 4000), kann mehrere Zielknoten besitzen. Besitzen mehrere Knoten das Ziel-”Domänen-Id/Knoten-Id”-Paar der Kante, werden zu all diesen Knoten Verbindungen gezogen. Die Bezeichnung des Kantensymbols zeigt die Anzahl der Zielknoten an. Auf der Sicht des Kantenobjektes (z.B. Submap) werden alle Start- und Zielknoten repräsentiert.

16.6 Manuelle indirekte Zielknoten-Zuweisung

Die Repräsentation einer Verbindung zwischen Systemen unterschiedlicher Technologietypen kann durch die manuelle Zuweisung eines Domänen-Id/Knoten-Id-Paares an einen bestimmten Knoten erfolgen. Diese Domänen-Id/Knoten-Id-Paar-Zuweisung wird nur innerhalb der OpenScape FM-Desktop-Datenbasis gesichert.

Wichtiger Hinweis:
Um Systeme des gleichen Technologietyps zu verbinden ist die empfohlene Methode, das entsprechende Zielsystem über entsprechende Management-Werkzeuge direkt für die Kante zu konfigurieren.

16.6.1 Manuelle Knoten-Id- und Domänen-Id-Konfiguration von Knoten

Der Eintrag **Eigenschaften** für vom Topologie Manager verwaltete Knotenobjekte stellt die Seite **Topologie->Knoten Id Konfiguration** zu Verfügung. Diese stellt die folgenden Informationen bereit:

Domänen Id: Enthält die Domänen-Id(s) des Knotens.

Knoten Id: Enthält die Knoten-Id,

Eingangstyp: zeigt an, ob die zugehörige Knoten-Id manuell durch einen Anwender, oder automatisch durch ein Plugin gesetzt wurde. Wurde die Knoten-Id automatisch gesetzt, wird hier der Erzeugertyp der Knoten-Id angezeigt. Für IP-Knoten z.B. lautet der Eintrag “ip internet”. Wurde die Knoten-Id manuell erzeugt, lautet der Eintrag “Manual”.

Domänen Id Schreibbar: Ist die Domänen-Id für den Anwender manuell veränderbar, ist das Feld abgehakt. Ein Beispiel für nicht schreibbare Domänen-Ids sind Knoten-Ids vom Typ “ip internet”.

Knoten Id Schreibbar: Dieses Feld ist abgehakt, wenn die Knoten-Id von Anwender verändert werden kann. Dies ist nur bei manuell erzeugten Knoten-Ids der Fall.

Löschbar: Dieses Feld ist abgehakt, wenn die Knoten-Id durch den Anwender entfernt werden kann. Dies ist nur bei manuell erzeugten Knoten-Ids der Fall.

Mit Hilfe der Textfelder auf der rechten Seite können die **Domänen Id** und die **Knoten Id** verändert werden. Durch Betätigung der Schaltfläche **Erzeugen** wird ein neues Domänen-Id/Knoten-Id-Paar erzeugt und mit Standardwerten initialisiert.

Um die Werte für einen Eintrag zu verändern, muss die entsprechende Zeile selektiert werden, der neue Wert eingegeben werden und anschließend die Schaltfläche  , die sich neben dem Wert befindet, betätigt werden.

Wird eine manuell erzeugte Knoten-Id nicht mehr länger benötigt, kann die entsprechende Zeile selektiert und diese anschließend durch Auswahl der Schaltfläche **Löschen** entfernt werden.

16.6.2 Kopieren und Einfügen von Knoten-Id/Domänen-Id-Paaren für Fremdsysteme

Speziell für Fremdsystem-Objekte bietet die Knoten-Id/Domänen-Id-Konfiguration die Möglichkeit, ein Knoten-Id/Domänen-Id-Paar zu kopieren und einem anderen Knoten zuzuweisen. Als Ergebnis wird die Verbindung zu diesem Knoten umgeleitet und das Fremdsystem-Objekt wird gelöscht. Die folgenden Aktionen müssen dabei durchgeführt werden: Aus dem Kontextmenü des Fremdsystems muss der Menüeintrag **Topologie->Domänen Id & Knoten Id kopieren** ausgewählt werden. Diese Aktion führt dazu, dass sich das System das Knoten-Id/Domänen-Id-Paar des Fremdsystems merkt. Anschließend muss das Kontextmenü des Knotens, zu dem die Verbindung umgeleitet werden soll geöffnet werden. In diesem Kontextmenü muss der Menüeintrag **Topologie->Domänen Id & Knoten Id einfügen** ausgewählt werden. Die Verbindung/Kante wird dann umgeleitet und auf der “Knoten-Id konfigurieren”-Seite des neuen Zielknotens findet sich ein neuer Eintrag, der die neue Zuweisung beschreibt.

16.6.3 Manuelle Knoten-Id- und Domänen-Id-Konfiguration für Netzwerke

Die Domänen- und Knoten-Ids aller Knoten, die sich in einem Netzwerk befinden, können über das Netzwerk verändert werden. Um dies zu erreichen, muss im Kontextmenü des Netzwerkobjektes der Menüeintrag **Konfigurieren** und im Fenster die Seite **Topologie->Netzwerk Knoten Id Konfiguration...** ausgewählt werden. Daraufhin öffnet sich der bereits in *Abschnitt 16.6.1, „Manuelle Knoten-Id- und Domänen-Id-Konfiguration von Knoten“* beschriebene Browser, es werden jedoch nur die Knoten aufgelistet, die in dem Netzwerk enthalten sind und vom Topologie Manager verwaltet werden. Um Werte zu ändern, muss die entsprechende Zeile selektiert werden, die neuen Werte eingegeben werden und anschließend die entsprechende  Schaltfläche betätigt werden. Der Browser wird daraufhin aktualisiert und die Topologie wird entsprechend der neuen Werte reorganisiert.

17 Hilfefunktionen

Der OpenScape FM Desktop bietet drei verschiedene Hilfefunktionen an(siehe *Bild 28*):

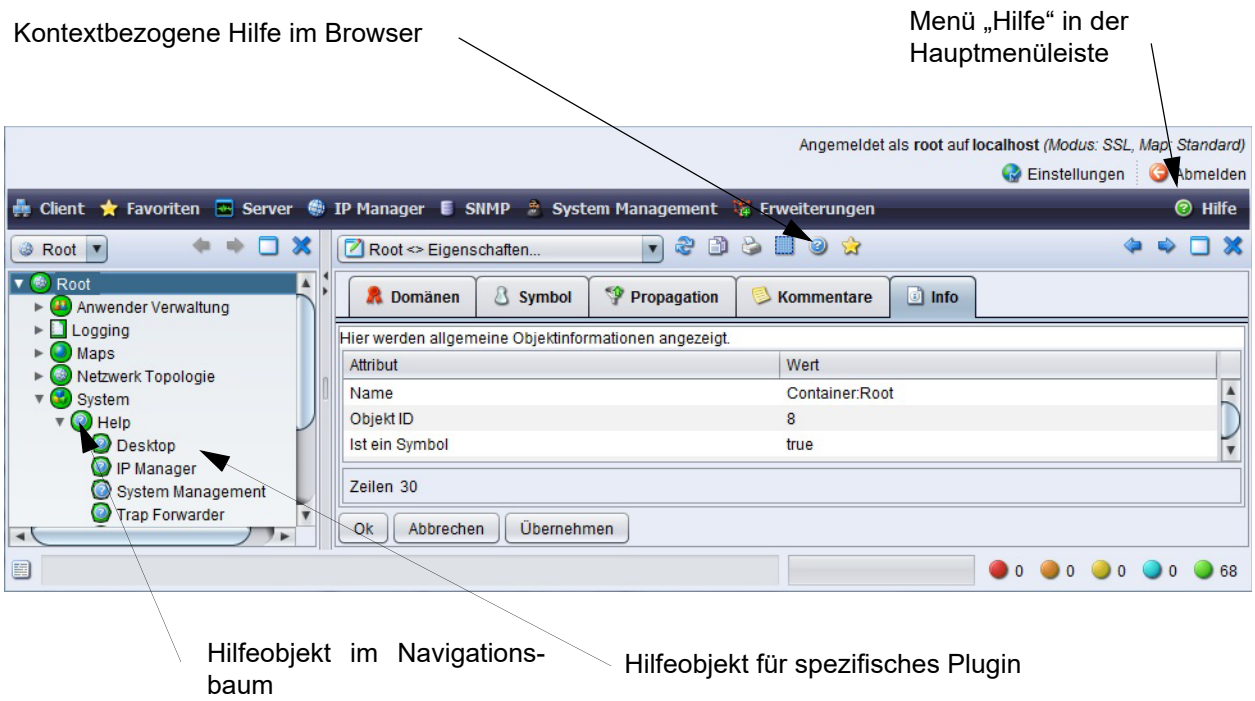


Bild 28 Hilfesystem

- Das Hauptmenü **Hilfe** enthält Einträge für alle initialisierten Plugins. Über den entsprechenden Menüeintrag öffnet sich das Inhaltsverzeichnis (TOC) der Hilfe für das ausgewählte Modul.
  Über das Baum-Objekt **System->Hilfe** kann die Plugin-spezifische Hilfe auch über das Hilfeobjekt aufgerufen werden, das den gleichen Namen hat wie das zugehörige Plugin.
- Das Hauptmenü **Hilfe** enthält zusätzlich den Eintrag **Übersicht**, der über eine Index-Seite den Zugriff auf alle deutschen und englischen Handbücher (auch der nicht initialisierten Plugins) ermöglicht.
- Zahlreiche Fenster bieten **Fenster-spezifische Hilfe** an. Ist eine solche Hilfe verfügbar, kann über die Schaltfläche  (kontextbezogene Hilfe) die Online-Hilfe genau an der betreffenden Stelle für dieses spezifischen Fenster geöffnet werden. Von dort kann der Inhalt der Hilfe beliebig durchsucht werden.

18 Protokollierung

OpenScape FM Desktop bietet eine Protokollierungsfunktion für externe OpenScape FM-Applikationen und interne Vorgänge (d. h. OpenScape FM-Basiskomponenten). Die Dateien befinden sich unter

`<OpenScape FM Installationsverzeichnis>/server/logging.`

Bei der Installation eines OpenScape FM-Servers werden die folgenden Dateien erstellt:

```
activity.log
error.log
trace.log
```

Alle OpenScape FM-spezifischen und sicherheitsrelevanten Vorgänge werden in der Datei `activity.log` gespeichert.

Alle Protokolldateien enthalten verschiedene Felder (Spalten):

- **Zeit**: Uhrzeit des OpenScape FM Servers zum Zeitpunkt als der Logging-Eintrag geschrieben worden ist
- **Zeitzone**: Zeitzone des Systems, wo die Logging-Applikation installiert ist
- **Typ**: Typ des Logging-Eintrags (Activity, Error, Trace)
- **Gruppe**: Wird verwendet, um die verschiedenen Logging-Einträge innerhalb eines Logging-Typs zu unterscheiden
- **Quelle IP**: IP-Adresse des Systems, die den Logging-Eintrag schreibt
- **Applikation**: Name der Applikation, die den Logging-Eintrag verursacht hat
- **Anwender**: Zuständiger Anwender
- **Mnemonic**: Kurze Beschreibung der Meldung

Die OpenScape FM-Managementapplikationen können über die RMI-Schnittstelle in die oben erwähnten drei Dateien schreiben. Die Konfiguration dieses Vorgangs kann jedoch nicht über die OpenScape FM-Bedienoberfläche vorgenommen werden, sondern hängt von der Implementierung des jeweiligen Programms ab.

Der Client dient dabei lediglich als Hilfsmittel zum Management der Protokolldatei und zur Erstellung spezifischer Ansichten. Eine Ansicht (wie in einer relationalen Datenbank) enthält einen festgelegten Teilbereich einer der Protokolldateien und erhöht die Lesefreundlichkeit bestimmter Protokolleinträge. So lassen sich beispielsweise nur Einträge von einer Applikation anzeigen, obwohl die Protokolldatei Einträge von mehreren Applikationen enthalten kann. Des Weiteren kann ein Systemadministrator den Zugriff auf die Ansichten durch Vergabe ansichtsspezifischer Rechte an bestimmte Anwender kontrollieren. Weitere Informationen zur Vergabe von Objektrechten finden Sie in *Kapitel 15, „Zugriffsrechte“*.

Um mit dem Protokollmodul zu arbeiten, öffnen Sie den Eintrag „Protokollierung“ auf der Root-Submap (siehe Protokollierungssymbol in *Kapitel 13, „Symbole und Statusanzeige“*). Die Submap enthält drei vorgegebene Symbole für `activity.log`, `error.log` und `trace.log`, die die zuvor beschriebenen Dateien darstellen. Jedes Symbol/Objekt bietet über das zugehörige Kontextmenü verschiedene Optionen.

- **Anzeigen** öffnet die Protokolldatei und zeigt Informationen zu in den Spalten enthaltenen Feldern (*Bild 29*). Wie in allen Tabellen unter OpenScape FM können Sie die Einträge der Protokolldatei durch einen Doppelklick auf den jeweiligen Spaltentitel sortieren. Sobald eine Zeile ausgewählt wird, wird die Schaltfläche **Show Description** aktiviert. Über diese Schaltfläche kann dann die ausführliche Beschreibung für die ausgewählte Zeile eingesehen werden.

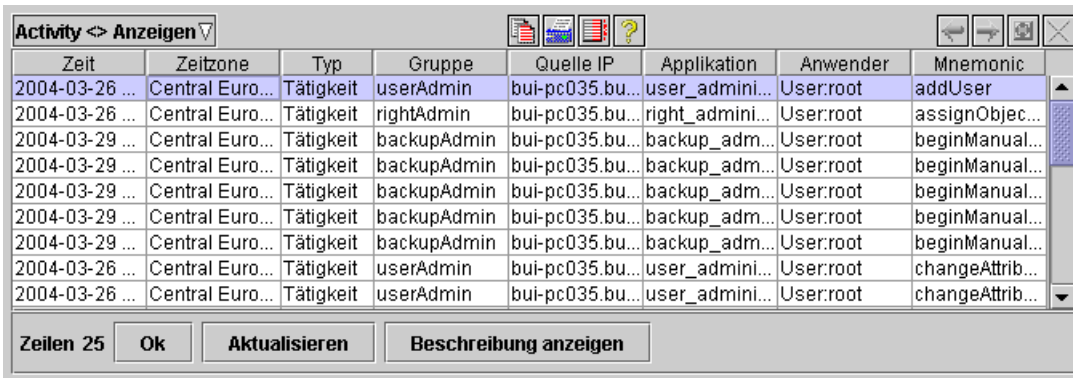


*Bild 29 Darstellung einer Protokolldatei über **Anzeigen***

- **Einrichten** steht als Menübefehl nur Anwendern der Rechtekategorie „Administrator“ zur Verfügung. Über diesen Befehl lassen sich der Pfad der Protokolldatei und die Parameter für die Dateigröße festlegen. Siehe *Abschnitt 18.1, „Einrichtung einer Protokolldatei“*.
- Über **Ansicht hinzufügen** und **Ansicht entfernen** können Sie eine Protokolldatei-Ansicht erstellen bzw. löschen (siehe Ansichtssymbol in *Kapitel 13, „Symbole und Statusanzeige“*). *Abschnitt 18.2, „Protokolldatei-Ansichten“* enthält weitere Informationen zu Ansichten.

18.1 Einrichtung einer Protokolldatei

Bild 30 zeigt die Bedienoberfläche zur Protokolldatei-Einrichtung für Anwender der Rechtekategorie „Administrator“. Im Feld **Dateiname** wird der Pfad der Datei angezeigt. Der Dateiname selbst kann nicht verändert werden. Im Feld **Max. Dateigröße** können Sie die Größe der Datei festlegen und über **Teile** können Sie bestimmen, aus wie vielen für den Anwender transparenten Teil-Protokolldateien die definierte Gesamtdatei bestehen soll.

Bild 30 Einrichtung einer Protokolldatei

Geben Sie beispielsweise einen Wert von 5 an, so werden fünf Einzeldateien erstellt: `activity.log.1`, `activity.log.2`, `activity.log.3`, `activity.log.4` und `activity.log.5`. Bei der Verwaltung der Protokolldateien ist jedoch nur die Datei `activity.log` von Bedeutung (die Einzeldateien sind für Sie nicht wichtig). Die Dateien werden von OpenScape FM automatisch zusammengefügt. Wenn die maximale Dateigröße erreicht ist, wird der älteste Teil der Protokolldatei von OpenScape FM gelöscht und es wird eine neue Teildatei erstellt. Es ist daher nicht möglich, den Wert im Feld **Teile** auf 1 zu setzen, da in diesem Fall die gesamte Datei gelöscht würde.

18.2 Protokolldatei-Ansichten

Wenn Sie über den Befehl **Ansicht hinzufügen** aus dem Kontextmenü eines Protokolldatei-Symbols eine neue Ansicht erstellt haben, finden Sie das Symbol der neuen Ansicht auf der Submap der Protokolldatei. Dort können Sie nun die Ansicht mit Hilfe von Filtern einrichten. Wie bereits erwähnt, besteht eine Ansicht aus einem definierten Teilbereich der Informationen einer Protokolldatei. Nehmen wir an, Ihre Protokolldatei wäre sehr groß und würde etliche Anwender umfassen. Sie könnten also das Protokoll filtern und nur die Einträge für Anwender XY anzeigen. Den Filter können Sie über das Kontextmenü der Ansicht definieren.

- Über **Anzeigen** wird die Ansicht angezeigt, d. h. nur die Zeilen, die den Filter passieren.
- Über **Filter** kann der Filter eingerichtet werden, *Abschnitt 18.2.1, „Einrichtung von Filtern“*
- **Einrichten** steht nur Anwendern der Rechtekategorie „Administrator“ zur Verfügung. Über diesen Befehl können Einschränkungen (*Abschnitt 18.2.1, „Einrichtung von Filtern“*) festgelegt werden, die für alle Anwender gelten, d. h. die Anwender können die durch Root vorgegebenen Filterkriterien nur einschränken, jedoch nicht erweitern.
- Über **Ansicht entfernen** wird die Ansicht gelöscht.

18.2.1 Einrichtung von Filtern

Über die Menüeinträge **Filter** und **Einrichten** aus dem Kontextmenü des Ansichtssymbols wird die Bedienoberfläche für die Filtereinrichtung geöffnet (*Bild 31* und *Bild 33*). Ein Filter wird mit Hilfe von Regulären Ausdrücken definiert, die für jedes Feld (Spalte) der Protokolldatei angegeben werden können. Da Reguläre Ausdrücke ein sehr komplexes Thema sind, ist eine umfassende Erläuterung an dieser Stelle nicht möglich. Im nächsten Abschnitt werden wir deshalb versuchen, einige Beispiele zu nennen, die einem Administrator häufiger begegnen können. Ausführliche Informationen finden Sie darüber hinaus in entsprechenden Fachbüchern, beispielsweise O'Reilly, Jeffrey E.F. Friedl: „Regular Expressions".

Regulare Ausdrücke: Beispiele für Suchmuster

`.*`	Beliebiges alphanumerisches Muster (Standardeinstellung für jede Spalte)
`^[Ss].*`	Beliebiges alphanumerisches Muster, das mit dem Klein- oder Großbuchstaben S beginnt. So würde folgendes Suchmuster beispielsweise die Anwendernamen „Schmidt", „schmidt" und „sander" in der Spalte mit dem Anwendernamen finden User:[Ss].*
`.*User.*`	Beliebiges Muster mit dem Substring „User". Mit diesem Muster könnten Sie beispielsweise alle User-Operationen im Mnemonic-Feld suchen.
`.*\.sun\.com$`	Beliebiges Muster, das mit dem Substring „.sun.com"endet. Da der Punkt in Regulären Ausdrücken eine Sonderbedeutung hat (steht für ein beliebiges Zeichen), muss der mit einem Backslash maskiert werden. Dieses Muster könnten Sie beispielsweise in der Spalte „Source IP" eingeben, um nach allen Protokolleinträgen zu suchen, die sich auf Systeme in der Domain sun.com beziehen.

Es gibt zwei Filter, die nacheinander angewendet werden. Zunächst wird die Protokolldatei vom Root-Filter gefiltert. Dieser kann vom Root-Anwender über **Einrichten** definiert werden. Anschließend erfolgt eine Filterung durch den Anwender-Filter, der sich über den Befehl **Filter** einrichten lässt. In der anzeigten Ansicht erscheinen lediglich die Zeilen, die beide Filter passiert haben.

18.2.1.1 Von „Administrator"-Anwendern eingerichtete Filter

Der Root-Anwender kann Filter über den Befehl **Einrichten** aus dem Kontextmenü der Ansicht definieren. In der Bedienoberfläche für die Einrichtung von Root-Filtern (*Bild 31*) können Reguläre Ausdrücke für alle Felder der Protokolldateizeilen angegeben werden. Der Root-Filter verwendet die originalen Einträge der Protokolldatei. Des Weiteren kann der Root-Anwender entscheiden, ob die Einträge der originalen Version oder die einer lokalisierten Version gefiltert werden sollen. Um den Filter zu lokalisieren, aktivieren Sie das Kontrollfeld **Lokalisiert**. Dadurch wird die Lokalisierung der Protokolldateieinträge aktiviert. Näheres hierzu siehe *Abschnitt 18.2.1.2, „Lokalisierte Ansicht von Protokolldateien"*.

Außerdem kann in dieser Bedienoberfläche zwischen der Ansicht selbst und dem zur Erstellung verwendeten Filter umgeschaltet werden. So können Sie Ergebnisse Ihrer Filterdefinitionen immer umgehend prüfen. Verwenden Sie dazu die Schaltflächen **Einrichten** (in der Ansicht) und **Ansicht** (in der Einrichtungsoberfläche).

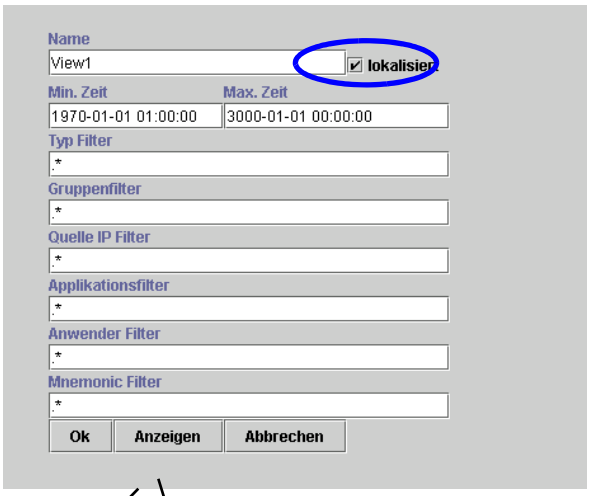
Bild 31 Bedienoberfläche zur Einrichtung von Root-Filtern

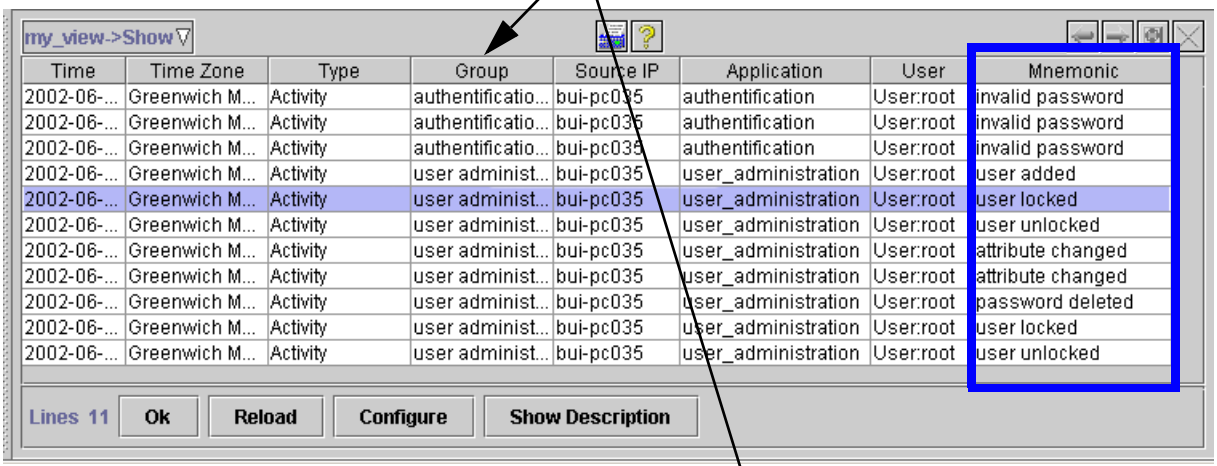
18.2.1.2 Lokalisierte Ansicht von Protokolldateien

Die Log-Datei-Einträge sind nicht immer verständlich, da sie in einer anderen Sprache geschrieben sein können. Die Protokollfunktion ermöglicht die Lokalisierung von Protokolleinträgen. Um die Lokalisierung dieser Einträge zu aktivieren, markieren Sie das Statusfeld **Lokalisiert** (dieses Feld ist standardmäßig aktiviert) im Dialogfenster für die Einrichtung der Protokolldateiansicht. Klicken Sie auf die Schaltfläche **Anzeigen**, um eine lokalisierte Ansicht der Protokolldatei zu erhalten. Die Schaltfläche **Anzeigen** funktioniert in ähnlicher Weise wie der Befehl **Anzeigen** im Menü **Log File View**. Für jeden Eintrag werden folgende Felder lokalisiert:

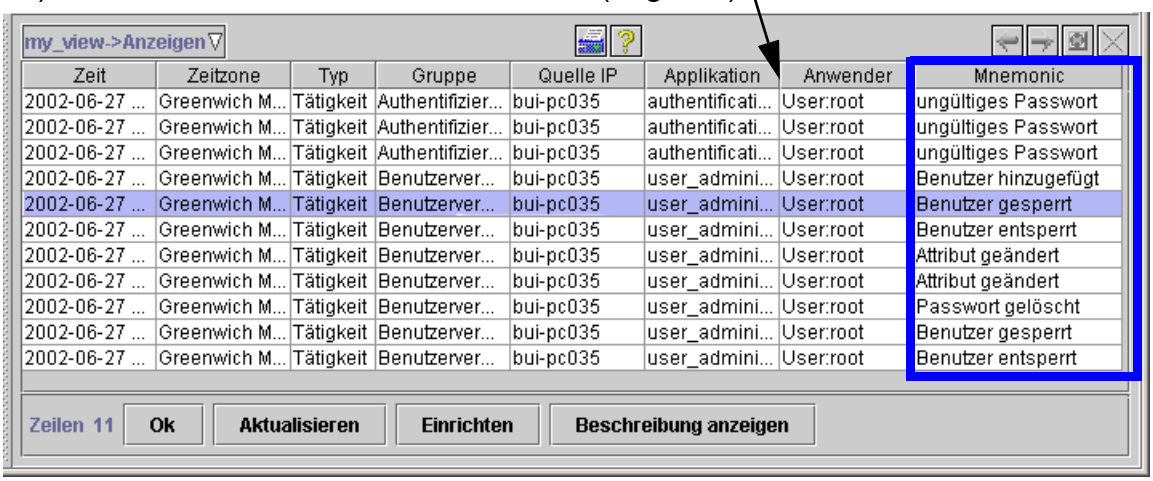
- Typ
- Gruppe
- Mnemonic
- Beschreibung

a)





b) Lokalisierte Ansicht der Protokolldatei (englisch)



b) Lokalisierte Ansicht der Protokolldatei (deutsch)

Bild 32 Lokalisierte Ansicht der Protokolldatei (englisch und deutsch)

18.2.1.3 Von regulären Anwendern eingerichtete Filter

Die Anwender-Filter verwenden immer lokalisierte Einträge. Wenn Sie beispielsweise die Protokolleinträge des Anwenders „Snoopy“ anzeigen lassen möchten, sich aber nicht sicher sind, ob der Name mit einem Großbuchstaben beginnt, richten Sie einfach einen Filter ein, wie in *Bild 33* dargestellt. Der von Ihnen eingerichtete Filter wird nur auf die Einträge angewendet, die den Root-Filter bereits passiert haben, wenn Sie zur Anzeige der Einträge berechtigt sind.

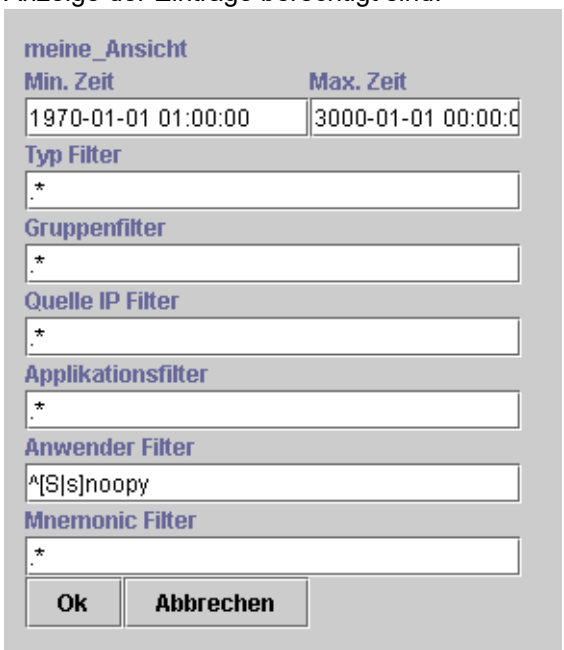


Bild 33 Bedienoberfläche zur Einrichtung von Anwender-Filtern

Die Protokolldatei wird Zeile für Zeile gefiltert und das Ergebnis wird als „meine_Ansicht“ angezeigt, wobei nur die Zeilen aufgeführt werden, die mit einem Eintrag „Snoopy“ oder „snoopy“ beginnen.

So können Sie eine Ansicht für jede Auswahl erstellen, die Sie aus der Protokolldatei auslesen möchten.

19 Backup und Wiederherstellung

Der OpenScape FM Desktop verfügt über einen Backup Management Service, der auch für andere OpenScape FM Management-Anwendungen zur Verfügung steht. Der Backup Management Service wird über den Backup-Manager bereitgestellt, der auch die beiden Basisfunktionen dieses Sicherungsdienstes verwaltet: „Speichern“ *(Backup)* und „Wiederherstellen“ *(Restore)*. Der Backup-Manager unterstützt eine Schnittstelle, über die sich OpenScape FM Management-Anwendungen beim Backup Management Service anmelden können. Somit können nur OpenScape FM Management-Anwendungen, die diese Schnittstelle unterstützen, den Sicherungsdienst von OpenScape FM Desktop nutzen. Die OpenScape FM Management-Anwendung definiert in diesem Fall selbst, welche Dateien gesichert werden sollen (siehe hierzu auch die Dokumentation der jeweiligen Anwendung). Der Backup Management Service fordert alle registrierten OpenScape FM Management-Anwendungen in regelmäßigen Abständen auf, einen Sicherungslauf zu starten. Die OpenScape FM Management-Anwendungen sind selbst für die Generierung konsistenter Daten-Backups verantwortlich.

Wichtiger Hinweis:
Wird das System Management Plugin verwendet (siehe separate Bedienungsanleitung) so wird die Konfiguration der System Management Agenten nicht automatisch durch die allgemeinen Backup-Mechanismen gesichert. In diesem Fall muss für jeden Agenten ein Backup Monitor konfiguriert werden, falls eine entsprechende Sicherung gewünscht ist.

Der Backup-Manager steuert bzw. überwacht die Dienste „Backup“ und „Restore“.

Backup: Unterstützt werden sowohl manuelle als auch automatische Sicherungslaufe *(Backups)*. Manuelle Backups werden von einem Anwender mit dem Zugriffsrecht „Backup Administrator“ (nachfolgend wird dieser Anwender als Backup-Administrator bezeichnet) eingeleitet. Automatische Backups werden in regelmäßigen Abständen vom Backup-Manager durchgeführt. Eine registrierte Anwendung wird vom Backup-Manager aufgefordert, die eigenen Daten selbst zu sichern. Die Anwendung greift in diesem Fall auf die Backup-Bedienoberfläche zu, um die angeforderte Datensicherung durchzuführen. Der Backup-Dienst sichert die Daten in einem Verzeichnis, das vom Backup-Administrator über die OpenScape FM GUI vereinbart werden kann. Bei erfolgreichem Abschluss eines Sicherungslaufs gibt die Anwendung eine entsprechende Meldung an den Backup-Manager aus und protokolliert dies in einem „Aktivitätenprotokoll“; siehe *Kapitel 18, „Protokollierung“*.

Restore: Eine Restore-Operation muss von einem Backup-Administrator eingeleitet werden. Die hiervon betroffene OpenScape FM Management-Anwendung wird in diesem Fall vom Backup-Manager aufgefordert, mit der Datenwiederherstellung zu beginnen. Bei erfolgreichem Abschluss eines Wiederherstellungslaufs gibt die Anwendung eine entsprechende Meldung an die Restore-Operation aus und protokolliert dies im „Aktivitätenprotokoll“ *(Activity Logging)*; siehe *Kapitel 18, „Protokollierung“*.

Zwei Betriebsebenen für Backup- und Restore-Operationen sind zu unterscheiden:

1. Vorgänge und Konfigurationsaufgaben für den Backup-Manager und
2. Vorgänge und Konfigurationsaufgaben für eine bestimmte Backup-Anwendung

Die Einstellungen auf Backup-Manager-Ebene können als globaler Administrationspunkt benutzt werden. Es ist aber auch möglich nur die Standardparameter für alle neu registrierten Backup-Anwendungen zu konfigurieren. Ein manueller Backup-Vorgang auf Backup-Manager-Ebene wird für alle registrierten und verwalteten Backup-Anwendungen durchgeführt.

Die Einstellungen für eine bestimmte Backup-Anwendung überschreiben die Standardparameter für diese Anwendung. Auf diese Weise erhalten Sie individuelle Konfigurationen für alle vorhandenen Backup-Anwendungen. Sämtliche Vorgänge auf Ebene einer bestimmten Backup-Anwendung betreffen nur diese Anwendung.

Zunächst wird nur der OpenScape FM Desktop für den Backup-Dienst registriert (OpenScape FM Database). Die OpenScape FM Desktop-Anwendung ist standardmäßig registriert und immer verfügbar (außer wenn die Anwendung den Status „Unverwaltet“ hat; siehe *Abschnitt 19.5, „Verwaltung aktivieren/deaktivieren“* für Backup- und Restore-Operationen.

Hinweis:
Ein Backup für die OpenScape FM Desktop-Anwendung gilt nur für die OpenScape FM Desktop-Datenbank, die alle Netzwerk-Management relevanten Informationen und Enterprise MIB Definitionen beinhaltet; vorhandene Bilddaten (z. B. Hintergrundbilder) und Lizenzen werden nicht gesichert.

19.1 Backup-Manager

Das Symbol „Backup Manager“ erscheint unter dem Symbol **Root->System->Server->Administration**. Es handelt sich hierbei um ein Container-Objekt für alle registrierten Backup-Anwendungen.

Das Symbol „Backup Manager“ verfügt über ein zweigeteiltes Kontextmenü: der obere Teil dieses Menüs enthält die allgemeinen OpenScape FM-Menübefehle; der untere Teil enthält eine Reihe von objektspezifischen Menüeinträgen. Zusätzlich befinden sich die gleichen Menüeinträge mit gleicher Funktion in Hauptmenü unter **Server->Administration->Backup Manager**:

- **Backup Parameter bearbeiten...:** Über diesen Befehl können die Standard-Backup-Parameter für alle **neu** registrierten Backup-Anwendungen eingestellt werden; siehe *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*.
- **Backups anzeigen...:** Über diesen Befehl wird ein Browser geöffnet, in dem die Backups **aller registrierten und verwalteten** Backup-Anwendungen aufgelistet sind. Über diesen Browser lassen sich bei Bedarf Backups für Backup-Anwendungen wieder herstellen; siehe *Abschnitt 19.4, „Anzeigen und Wiederherstellen von Backups“*)
- **Sofortbackup:** Über diesen Befehl kann ein manuelles Backup für **alle registrierten und verwalteten** Backup-Anwendungen gestartet werden; siehe *Abschnitt 19.3, „Sofortbackup“*.

Mit einem Doppelklick auf das Symbol „Backup Manager“ kann eine Submap mit allen registrierten Backup-Anwendungen geöffnet werden. Eine Backup-Anwendung, die bereits registriert ist und für den Backup/Restore-Betrieb zur Verfügung steht, ist hier mit einem grünen Symbol markiert; die übrigen Zustände werden in *Abschnitt 19.7, „Anwendungsstatus“* beschrieben. Zusätzlich zu den bekannten Befehlen des Backup-Managers enthält dieses Kontextmenü folgende Befehle:

- **Backup Parameter bearbeiten...:** Über diesen Befehl können die Backup-Parameter für **diese Backup-Anwendung** konfiguriert werden; siehe *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*.

- **Backups anzeigen...:** Über diesen Befehl kann ein Browser geöffnet werden, in dem alle Backups **dieser Backup-Anwendung** aufgelistet sind. Über diesen Browser kann eine Restore-Operation gestartet werden; siehe *Abschnitt 19.4, „Anzeigen und Wiederherstellen von Backups“*. Auch können hier einzelne Backups manuell gelöscht werden.
- **Sofortbackup:** Über diesen Befehl kann ein manuelles Backup **für diese Backup-Anwendung** gestartet werden; siehe *Abschnitt 19.3, „Sofortbackup“*.
- **Abbrechen:** [Dieser Menübefehl ist nur verfügbar, wenn eine Restore- oder Backup-Operation aktiv ist.] Über diesen Befehl kann ein aktiver Prozess abgebrochen werden; siehe *Abschnitt 19.6, „Abbruch“*.

19.2 Bearbeiten von Backup-Parametern

Um die Backup-Parameter für Datensicherungen zu konfigurieren, muss zunächst das Dialogfenster **Backup Parameter bearbeiten...** geöffnet werden.

Hinweis:
Das Dialogfenster kann sowohl im Backup-Manager Kontext als auch im Kontext einer Backup-Anwendung geöffnet werden. Wenn das Dialogfenster im Kontext einer Backup-Anwendung geöffnet wird, gelten die Parameter **nur für diese Backup-Anwendung**.

Kontextmenü des Backup-Managers:

- Hauptmenü **Server->Administration->Backup-Manager->Backup Parameter bearbeiten...**
- Symbol „Backup Manager“->**Backup Parameter bearbeiten...**

Kontextmenü einer Backup-Anwendung:

- Symbol „Backup Application“ -> **Backup Parameter bearbeiten...**

Die Struktur und Funktionalität der Dialoge sind für den Backup-Manager sowie für Backup-Anwendungen weitestgehend gleich. Der Unterschied liegt im Anwendungsbereich der konfigurierten Parameter.

- Im Dialogfenster Edit Backup Parameters kann das Zeitintervall für die Ausführung automatischer Backups gewählt werden. Hier lässt sich beispielsweise vereinbaren, dass ein Backup jeden Tag zu einer bestimmten Uhrzeit, jeden *n*-ten Tag zu einer bestimmten Uhrzeit oder alle *n* Stunden (*n* Minuten) durchgeführt werden soll. Bei Einrichtung einer bestimmten Backup-Konfiguration muss im Feld **Backup alle** zunächst ein Zeitintervall für den Abstand zwischen zwei Backup-Operationen definiert werden. Anschließend wird die Zeiteinheit (Minuten, Stunden oder Tage) für das Zeitintervall der automatischen Backups gewählt. In der folgenden Zeile (**Nächster Start am**) wird dann angegeben, zu welchem Zeitpunkt der erste Sicherungslauf durchgeführt und das Intervall für die nächsten Sicherungen gestartet werden soll. Durch zweimaliges Anklicken des Datum- und des Zeitfeldes kann der Backup-Zeitpunkt über die Benutzeroberfläche gesetzt werden.
- **Anzahl gesicherter Backups:** Gibt an, wie viele Backups beibehalten werden. Wird ein neues Backup angelegt und hierbei die „Anzahl gesicherter Backups“ erreicht, hat dies automatisch die Löschung des jeweils ältesten Backups zur Folge. Wird beispielsweise jeden Tag ein Backup durchgeführt und für die Anzahl der beizubehaltenden Backups der Wert „5“ vereinbart, so werden fünf Backups beibehalten; bei Erstellung des sechsten Backups wird das älteste Backup gelöscht. Wird für die Anzahl der beizubehaltenden Backups ein

kleinerer Wert vereinbart, wird nach einem Backup nur der jeweils älteste Backup-Eintrag gelöscht. Beispiel: Es sind bereits fünf Backups erstellt worden und der Wert für die beizubehaltenen Backups wird in „2“ geändert. Nach einem Backup wird nur der älteste Backup-Eintrag gelöscht und im Backup-Verzeichnis befinden sich nach wie vor fünf Backups.

- **Max. Anzahl Wiederholungen:** Bestimmt die maximale Anzahl Wiederholversuche für eine Backup- oder Restore-Operation, bevor die Ausführung dieser Operation abgebrochen wird. Beispiel: Steht die Backup-Anwendung während einer Backup-Operation vorübergehend nicht zur Verfügung und wurden bereits mehrere Dateien übermittelt, wiederholt der Backup-Manager die Übertragung der letzten Backup-Datei, bis die Backup- bzw. Restore-Operation abgeschlossen ist oder die maximale Anzahl Wiederholversuche erreicht ist.

- Im Feld **Backup auf** wird ein Verzeichnis für die Speicherung der Backups vereinbart. Die Pfadeingabe kann hierbei manuell oder durch Auswahl des gewünschten Verzeichnisses über den Remote File Chooser (per **Auswählen...**) erfolgen.
  Hierbei sind zwei Fälle zu unterscheiden:

  - **Fall 1:** Wird das Backup-Verzeichnis über den Backup-Manager angegeben, verweist dieser Eintrag auf ein Verzeichnis mit Unterverzeichnissen für jede registrierte Backup-Anwendung. In diese Unterverzeichnisse werden die Backup-Dateien der jeweiligen Anwendungen gespeichert. Die Standardeinstellung für das Backup-Verzeichnis lautet `/<OpenScape FM Installation directory/server/backup/`.

  - **Fall 2:** Erfolgt die Angabe des Backup-Verzeichnisses über das Kontextmenü einer Backup-Anwendung, verweist dieser Eintrag auf ein Verzeichnis mit allen Backup-Dateien dieser Anwendung. Standardmäßig wird der Eintrag für „Backup to“ über den Backup-Manager definiert und hierbei zusätzlich das Unterverzeichnis für die jeweilige Backup-Anwendung ergänzt.

- Im Feld **Erforderlicher freier Plattenplatz für Backup** wird festgelegt, wieviel Platz auf dem gewählten Dateisystem mindestens noch verfügbar sein muss, damit mit einem Backup begonnen wird.
  Ist beim Versuch ein Backup zu starten nicht genügend Platz vorhanden, wird pro zu sichernder Komponente ein Ereignis mit Status *Major* erzeugt, und eine entsprechende Meldung angezeigt. Dabei ist es egal, ob es sich um ein automatisches oder manuelles Backup handelt.

- Über das Statusfeld **Automatisches Backup aktiviert** wird der automatische Backup-Betrieb aktiviert bzw. deaktiviert.

- Das Statusfeld **Konfigurationen für alle registrierten Clienten überschreiben** ist nur im Backup Manager Kontext verfügbar. Es zeigt an, ob die konfigurierten Parameter für **alle** Backup-Anwendungen (bereits registrierte und neue) oder nur für **neu** registrierte Backup-Anwendungen gesetzt werden soll. Wenn das Statusfeld ausgewählt ist, überschreiben die konfigurierten Parameter nach Betätigung der **OK** Schaltfläche die bereits existierende Konfiguration aller registrierten Backup-Anwendungen. Ist das Statusfeld nicht ausgewählt werden die konfigurierten Parameter nur für neu registrierte Backup-Anwendung verwendet. Standardmäßig ist das Statusfeld ausgewählt.

Bei Betätigung der Schaltfläche **OK** werden zunächst die Lese- und Schreibberechtigungen für das Backup-Verzeichnis (**Backup auf**) geprüft, anschliessend werden die Pfadänderung und die anderen Werte übernommen. Im Kontext einer Backup-Anwendung wird das neue Verzeichnis nach Backup-Einträgen für diese Anwendung durchsucht.

Wichtiger Hinweis:
Ist der Dialog im Backup-Manager-Kontext geöffnet und das Statusfeld **Konfigurationen für alle registrierten Clienten überschreiben** ausgewählt, werden nach Betätigung der **OK** Schaltfläche immer die Parameter aller Backup-Anwendungen überschrieben. Dies ist auch der Fall, wenn keine Änderungen vorgenommen worden sind.

Hinweis: [Backup-Anwendung]
Ist eine Backup- oder Restore-Operation aktiv, während ein oder mehrere Parameter über die Bedienoberfläche geändert werden, treten die Änderungen erst nach Beendigung des aktuellen Vorgangs in Kraft!

Besteht für das gewählte Verzeichnis nur ein Lesezugriff:

- erscheinen vor und hinter der Beschriftung des entsprechenden Anwendungssymbols Sternchen (*Bild 34*).
- ist kein **Sofortbackup** über das Kontextmenü der Anwendungen möglich.
- werden keine automatischen Backup-Operationen durchgeführt.
- kann eine Restore-Operation nach wie vor gestartet werden.

Werden zu einem späteren Zeitpunkt Schreibzugriffe für das Verzeichnis vereinbart, muss die Backup-Anwendung zunächst reinitialisiert werden. Dazu muss die Verwaltung zunächst deaktiviert und anschließend wieder aktiviert wird (siehe *Abschnitt 19.5, „Verwaltung aktivieren/deaktivieren“)* oder eine manuelle Backup-Operation für diese Anwendung gestartet werden (siehe *Abschnitt 19.3, „Sofortbackup“)*. In diesem Fall werden die Sternchen in der Anwendungsbeschriftung entfernt.

Bild 34 *Backup-Anwendung: Verzeichnis mit Lesezugriff*

19.3 Sofortbackup

Unabhängig vom automatischen Backup-Verfahren können bei Bedarf manuelle Backups durchgeführt werden. Ebenso wie im Dialogfenster „Backup Parameter bearbeiten“ sind diese manuellen Backups im Backup-Manager sowie in mehreren Backup-Anwendungen möglich.

Um eine Backup-Operation für eine **Anwendung** umgehend zu starten, muss der Menübefehl **Sofortbackup** im Kontextmenü der jeweiligen Anwendung aktiviert werden. Ein Backup **für diese Backup-Anwendung** wird umgehend durchgeführt und im vereinbarten Verzeichnis gespeichert (siehe *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*).

Über den Menübefehl **Sofortbackup** im Kontextmenü des **Backup-Managers** oder über den gleichen Eintrag aus dem Hauptmenü **Server->Administration->Backup Manager** kann der Anwender ein umgehendes Backup **für alle registrierten und verwalteten** Anwendungen starten.

Die sich öffnende Seite zeigt zunächst eine Liste aller dem Backup bekannten Komponenten. Dabei steht ein führender grüner Haken für Komponenten, die als aktiv registriert sind, und die eine Verbindung zum OpenScape FM Server besitzen.

Ein Anklicken der Schaltfläche **Sofortbackup** startet die eigentlichen Backup-Prozesse.

Die Backups werden unmittelbar durchgeführt und im entsprechenden Verzeichnis gespeichert (siehe *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*).

Ein Sanduhr-Symbol steht für einen aktuell noch laufenden Backup-Prozess, ein doppelter grüner Haken für einen erfolgreich beendeten Prozess, und ein rotes Kreuz für einen mit Fehler abgebrochenen Prozess.

Ein Fehler tritt dabei z.B. auf, wenn die Verbindung zu einem zu sichernden Agenten verloren geht, oder wenn der Speicherplatz für die Sicherungsdatei nicht ausreichend ist.

Beim Start eines Backups erhält das Symbol den Status „Test“ (hierdurch wird dem Anwender signalisiert, dass ein Backup aktiv ist; siehe *Abschnitt 19.7, „Anwendungsstatus“*). Darüber hinaus zeigt die Symbolbeschriftung der Backup-Anwendung einige nützliche Informationen zu den Übertragungsstatistiken (siehe *Bild 35*).

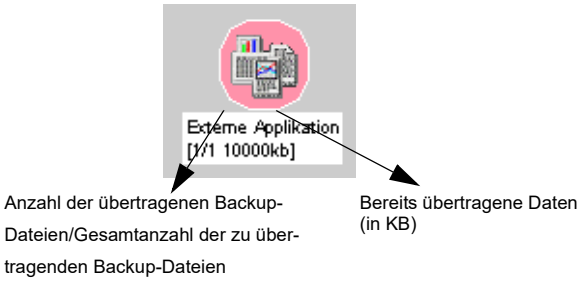


Bild 35 Backup-Anwendung: Aktives Backup

Hinweis:
Der Menübefehl **Sofortbackup** ist nur verfügbar, d. h., wenn derzeit keine Backup- oder Restore-Operation aktiv ist, wenn die Anwendung den Status „Normal“ hat (*Abschnitt 19.7, „Anwendungsstatus“*).

19.4 Anzeigen und Wiederherstellen von Backups

In diesem Kapitel wird beschrieben, wie man Backups auflistet (*Abschnitt 19.4.1, „Backups anzeigen“*) und wiederherstellt (*Abschnitt 19.4.2, „Wiederherstellen“*). Ebenso wie beim Dialog „Edit Backup Parameter“ können diese Aktionen für eine Backup-Anwendung oder im Backup-Manager durchgeführt werden: So listet die Aktion List Backups im „Backup Application“-Kontext nur die Backups der jeweiligen Anwendung auf, während im „Backup Manager“-Kontext sämtliche Backups **aller** Backup-Anwendungen aufgelistet werden.

19.4.1 Backups anzeigen

Backups können wie folgt angezeigt werden: für alle verwalteten und registrierten Anwendungen oder nur für eine bestimmte Anwendung.

- Um die Backups **aller** registrierten und verwalteten Anwendungen anzuzeigen, müssen Sie entweder den Menübefehl **List Backups...** im Kontextmenü des **Backup-Managers** wählen oder die Position **Server->Administration->Backup-Manager** im Hauptmenü.

- Um die Backups **einer Anwendung** aufzulisten, müssen Sie den Menübefehl **List Backups...** der **entsprechenden Anwendung** wählen.

In beiden Fällen wird ein Info-Browser (*Bild 36*) mit einer Liste aller verfügbaren Backup-Einträge geöffnet. Im Kontext einer **Backup-Anwendung** erscheinen im oberen Fensterbereich zusätzlich der Name der Anwendung und der Pfad des zugehörigen Backup-Verzeichnisses.

Der Info-Browser zeigt folgende Informationen:

- **Applikation:** Der Name der registrierten Backup-Anwendung. [Diese Spalte ist nur im Backup-Manager-Kontext verfügbar.]
- **Status:** Der Status einer Backup- oder Restore-Operation. Werden gerade Daten wiederhergestellt, erscheint hier „Restore active“ (*Restore aktiv*). Ist die Restore- bzw. Backup-Operation bereits abgeschlossen, erscheint „Finished“ (beendet). Der Status „Corrupt“ (*Fehler*) signalisiert, dass das zugehörige Backup nicht vollständig oder nicht lesbar ist.
- **Zeit (generiert):** Ein Zeitstempel, der den Generierungszeitpunkt für diesen Backup-Eintrag dokumentiert und Informationen zur Backup-Operation enthält. Ein Backup(-Eintrag) wird manuell oder im Rahmen des automatischen Backup-Betriebs generiert.
- **Anzahl Dateien:** Die Anzahl der (Daten)Dateien, die für diese Anwendung gesichert werden bzw. wurden.
- **Gesamtgröße (Kb):** Die Gesamt-Speicherkapazität (in Kilobytes), die für die Sicherung aller (Daten)Dateien benötigt wird.
- **Übertragungszeit:** Die Ausführungszeit für die jeweilige Backup-Operation.
- **Letztes Wiederherstellungsdatum (generiert):** Das letzte Datum, an dem der Backup-Eintrag in einer Restore-Operation berücksichtigt wurde; siehe *Abschnitt 19.4.2, „Wiederherstellen“*.

Über die Schaltfläche **Aktualisieren** kann der Browser-Inhalt sowie der Status der Backup/Restore-Aktivitäten aktualisiert werden.

Die Schaltfläche **Wiederherstellen...** aktiviert die Restore-Operation(en). Weiterführende Informationen zur Wiederherstellungsfunktion finden Sie in *Abschnitt 19.4.2, „Wiederherstellen“*.

Wird der „List Backups Information“-Browser über eine **Backup-Anwendung** geöffnet, erscheinen im Browser-Fenster zusätzlich die Schaltflächen **Verzeichnis auswählen...** und **Standart-Verzeichnis setzen**. Über die Schaltfläche **Verzeichnis auswählen...** kann man in ein anderes Verzeichnis wechseln, um sich eine Liste aller Backup-Einträge dieses Verzeichnisses anzeigen zu lassen. Bei Aktivierung der Schaltfläche **Verzeichnis auswählen...** wird ein Dateiauswahl-Dialog (Remote File Chooser) geöffnet, in dem man zu einem anderen Verzeichnis des OpenScape FM-Server-Dateisystems wechseln kann. Nach Auswahl eines Verzeichnisses über den Remote File Chooser werden automatisch alle Backup-Einträge dieser Anwendung aufgelistet, die sich in dem gewählten Verzeichnis befinden. Bei Bedarf können aus diesem Verzeichnis heraus auch zuvor gesicherte Daten wiederhergestellt werden. Das Verzeichnis wird im List Backups Info Browser angezeigt, bis der Anwender wieder zum Standardverzeichnis wechselt. Um zum Standardverzeichnis zurückzukehren, d. h. dem Verzeichnis, das zuvor über die **Backup Parameters bearbeiten**-GUI vereinbart wurde (*Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*), müssen Sie auf die Schaltfläche **Standart-Verzeichnis setzen** klicken. Diese Schaltfläche ist nur verfügbar, wenn ein anderes Verzeichnis über die Schaltfläche **Verzeichnis auswählen...** gewählt wurde.

Hinweis:
Die Aktionen der Schaltflächen **Verzeichnis auswählen...** und **Standart-Verzeichnis setzen** haben keine Auswirkungen auf die Backup-Parameter der entsprechenden Anwendung.

19.4.2 Wiederherstellen

Der List Backups Info Browser enthält die Schaltfläche **Wiederherstellen...**. Über diese Schaltfläche können Restore-Operationen aktiviert werden.

Wird der List Backups Info Browser im **Backup-Manager**-Kontext geöffnet, kann eine Restore-Operation für mehrere Anwendungen gleichzeitig durchgeführt werden. Im Kontext einer **Backup-Anwendung** kann immer nur ein Backup wiederhergestellt werden.

Um ein Restore für eine Anwendung durchzuführen, braucht man nur einen Backup-Eintrag dieser Anwendung auszuwählen und anschließend die Schaltfläche **Wiederherstellen...** zu betätigen. In diesem Fall erscheint das Fenster „Restore Information“ mit einem Warnhinweis, der den Anwender darüber informiert, dass die Anwendung nach Abschluss der Restore-Operation möglicherweise neu gestartet werden muss. Bei Aktivierung der Schaltfläche **OK** wird mit der Wiederherstellung der Backup-Daten begonnen; soll dies nicht geschehen, müssen Sie die Schaltfläche **Abbrechen** anklicken.

Das erfolgreiche Einspielen von Sicherungen kann nur für Sicherungsdateien des aktuellen oder der unmittelbar vorherigen OpenScape FM Releases gewährleistet werden (also z.B. für OpenScape FM Release 4.3 für Sicherungsdateien aus Release 4.3 oder 4.2). Sollten ältere Sicherungsdateien nicht erfolgreich importiert werden können, sind evtl. ein oder mehrere Zwischenschritte über ältere OpenScape FM Server Releases notwendig.

Hinweis:
Wählt man im Backup-Manager-Kontext mehrere Backup-Einträge für ein und dieselbe Anwendung, erscheint im Message Log Window eine entsprechende Warnmeldung. Um diesen Fehler zu beheben, muss zunächst die Auswahl für alle ungültigen Backup-Einträge wieder aufgehoben werden.

Nach Bestätigung im Fenster „Restore Information“ ändert sich die Beschriftung des zugehörigen Anwendungssymbols wie in *Bild 36* gezeigt. Die Beschriftung des Symbols „Backup Application“ enthält nützliche Informationen (Transferstatistiken) wie die Anzahl der bereits wiederhergestellten Dateien sowie die bereits übermittelte Byte-Anzahl.

Hinweis:
Die Schaltfläche **Wiederherstellen...** ist nur verfügbar, wenn keine Backup- oder Restore-Operation für die Anwendung aktiv ist!

Wenn eine Restore-Anforderung von einer Anwendung abgelehnt wird, so wird dies vom Backup-Manager registriert und die Anforderung zu einem späteren Zeitpunkt (nach erneuter Registrierung der betreffenden Anwendung) wiederholt bzw. fortgesetzt.

Warnung:
Nach erfolgreicher Wiederherstellung der OpenScape FM-Datenbank wird der OpenScape FM-Server automatisch mit den wiederhergestellten OpenScape FM Desktop-Datenbankdateien über den Startup Manager neu gestartet (siehe *Abschnitt 4.1, „Server-Start“*).

Wird der List Backups Info Browser im Kontext einer **Backup-Anwendung** geöffnet, erscheinen im Browser-Fenster zusätzlich die Schaltflächen **Verzeichnis auswählen...** und **Standart-Verzeichnis setzen**. Über die Schaltfläche **Verzeichnis auswählen...** kann ein anderes Verzeichnis für die nachfolgenden Restore-Operationen aufgerufen werden. Um das Verzeichnis auf den im Dialogfenster „Edit Backup Parameters“ vereinbarten Wert zurückzusetzen, muss auf die Schaltfläche **Standart-Verzeichnis setzen** geklickt werden.

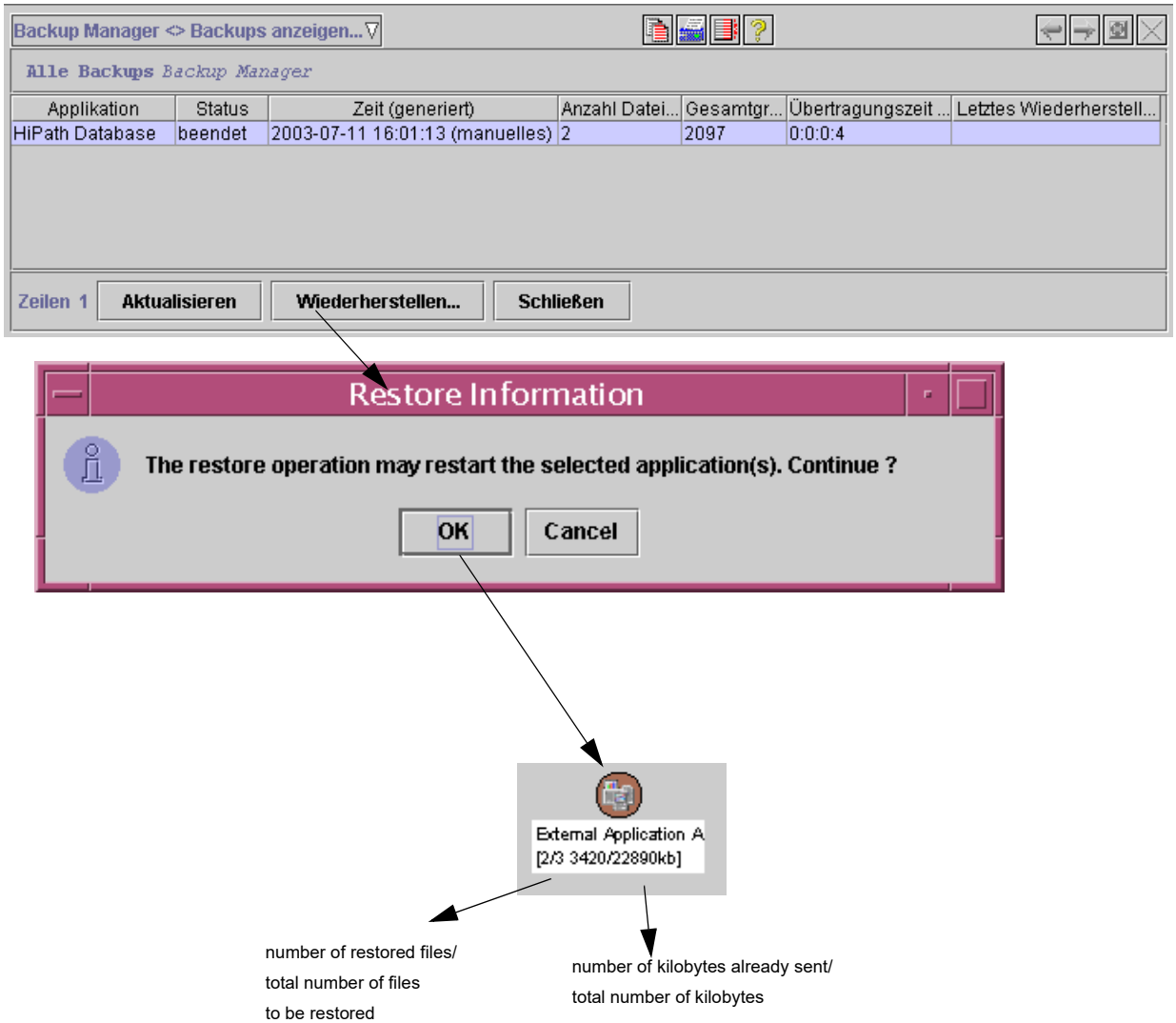


Bild 36 Backup-Anwendung: Liste der Backup- und Restore-Einträge

Um alte Daten wiederherzustellen, deren Backup nicht mit dem Backup-Manager erfolgte (d.h. mit einer älteren Version des OpenScape FM), müssen Sie den Server anhalten und die Datei `startRestore.exe` (Windows) bzw. `startRestore` (Unix) ausführen. Diese befindet sich im Installationsverzeichnis. Wählen Sie dann die „Base“-Datei aus, von der Sie die Daten wiederherstellen möchten. Es können nur Dateien des Typs „base“ ausgewählt werden! Anschließend wird die wiederhergestellte Datenbank aktiviert und der Server gestartet. Die alte Datenbank wird unter „database_old“ gespeichert.
Da der Server bereits läuft, können Sie die Clients später starten und die Arbeit mit den wiederhergestellten Daten aufnehmen.

19.5 Verwaltung aktivieren/deaktivieren

Über den Menüeintrag **Bearbeiten->Nicht Verwalten** kann eine Backup-Anwendung komfortabel aus dem Backup-Prozess ausgegliedert werden. Eine nicht verwaltete Backup-Anwendung wird angezeigt (siehe *Abschnitt 19.7, „Anwendungsstatus“*) und es sind keine spezifischen Menübefehle mehr verfügbar.

Für eine nicht verwaltete Backup-Anwendung kann über den Menübefehl **Bearbeiten->Verwalten** wieder den Status „*Verwaltet*“ vereinbart werden. Das Backup-Zielverzeichnis „Backup auf:“ aus *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“* wird in diesem Fall nach vorhandenen Backup-Einträgen durchsucht, und der Status der Backup-Anwendung(en) wird umgehend neu ermittelt.

Wichtige Information:
Für den Fall, dass eine Backup-Anwendung beschäftigt ist, wird die aktive Backup-Operation abgebrochen.

19.6 Abbruch

Ist eine Backup- oder Restore-Operation aktiv, so kann diese Operation über den Menübefehl **Abbrechen** vorzeitig beendet werden. Der Symbolstatus für die Anwendung wechselt in diesem Fall zu „Normal“, und die Transferstatistiken in der Symbolbeschriftung werden ausgeblendet.

19.7 Anwendungsstatus

Das Erscheinungsbild des Symbols „Backup Application“ hängt von der Art und dem Status der zugehörigen Anwendung ab. Der Anwendungsstatus wird durch bestimmte Anzeigefarben signalisiert. Tritt ein Fehler auf, beginnt das Symbol zu blinken; der Administrator wird auf diese Weise darauf hingewiesen, dass ein neues Ereignis eingetreten ist.

Es gibt insgesamt sieben verschiedene Zustände einer Backup-Anwendung:

Nicht verwaltet → hellbraun
Diese Anwendung ist zwar noch in der Datenbank registriert, aber es sind keine Backup- oder Restore-Operationen verfügbar. Wird die Verwaltung der Backup-Anwendung anwenderseitig (d. h. manuell) deaktiviert, erhält die Anwendung diesen Status.

Test → lachsrot
Der Status „Test“ signalisiert, dass gerade eine Backup-Operation für die Anwendung aktiv ist. Beginnt das Symbol in diesem Status zu blinken, bedeutet dies, dass eine Backup-Operation von der Backup-Anwendung abgelehnt wurde. Das zugehörige Ereignis im Ereignis-Browser zeigt in diesem Fall die Anzahl der Ablehnungen für diese Anwendung.

Deaktiviert → dunkelbraun
Der Status „Deaktiviert“ besagt, dass die Registrierung einer Backup-Anwendung manuell aufgehoben wurde. Weder Backup- noch Restore-Operationen sind möglich.

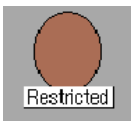
	Eingeschränkt → braun Der Status „Eingerschränkt“ signalisiert, dass eine Restore-Operation für die Anwendung aktiv ist. Beginnt das Symbol in diesem Status zu blinken, bedeutet dies, dass eine Restore-Operation von der Backup-Anwendung abgelehnt wurde. Bei der nächsten Registrierung der Anwendung „erinnert“ sich der Backup-Manager daran, dass der Backup-Eintrag abgelehnt wurde und startet automatisch die Wiederherstellung der zugehörigen Daten.
	Normal → grün Die Backup-Anwendung befindet sich im normalen Betriebszustand und ist für Backup- bzw. Restore-Operationen bereit.
	Schwerwiegend → orange Die letzte Backup- oder Restore-Operation ist fehlgeschlagen und wurde aufgrund eines E/A-Fehlers bzw. aufgrund von Netzwerkproblemen unterbrochen. Beginnt das Symbol in diesem Zustand zu blinken, so bedeutet dies, dass diese Anwendung nicht über die erforderliche Zugriffsberechtigung für das Backup-Zielverzeichnis verfügt (siehe *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*).
	Kritisch → rot Die Backup-Anwendung reagiert nicht mehr. Beginnt das Symbol in diesem Zustand zu blinken, weiß der Anwender, dass die Backup-Anwendung nicht reagiert und somit nicht mehr verfügbar ist. Dieser Status wird nur signalisiert, wenn die Anzahl der Wiederholungsversuche (siehe *Abschnitt 19.2, „Bearbeiten von Backup-Parametern“*) überschritten wird.

Tabelle 4 *Status von Backup-Anwendungen*

19.8 Löschen einer Backup-Anwendung

Wird eine Backup-Anwendung nicht mehr benötigt, kann sie über den Menübefehl **Bearbeiten**-> **Objekt Löschen** aus der Submap des Backup-Managers gelöscht werden.

Warnung:
Wenn Sie eine Backup-Anwendung aus der Submap des Backup-Managers löschen, werden gleichzeitig alle zugehörigen Backup-Einträge im hierfür angelegten Backup-Verzeichnis gelöscht.

Um den „Backup Manager“-Dienst wieder nutzen zu können, muss die Anwendung wieder mit dem Backup-Manager verknüpft werden.

Hinweis:
Wenn Sie das Objekt „OpenScape FM Database“ aus der Submap des Backup-Managers löschen, werden ebenfalls alle Backups gelöscht; nach einem Neustart des OpenScape FM-Servers wird dieses Objekt jedoch automatisch wieder registriert.

19.9 Protokollieren von Backup-Operationen

Sämtliche Backup-Operationen werden in einem speziellen „Aktivitätenprotokoll“ – dem OpenScape FM Activity Log – protokolliert. Eventuelle Fehler werden hierbei in einem Fehlerprotokoll (Error Log) festgehalten. Weiterführende Informationen zu der Protokollkomponente finden Sie in *Kapitel 18, „Protokollierung“*.
Prokolloperationen werden über das „Backup/Admin“-Konto ausgeführt – die zugehörigen Einträge der Protokolldatei können somit unter „backupAdmin“ in der entsprechenden „Gruppe“ der Protokolldateien abgerufen werden.

20 Zeitpläne

Zeitpläne, auch Zeitfilter genannt, sind Kalender-basierte Objekte zur Definition von Terminen und Zeitintervallen. Sie werden im OpenScape FM zu verschiedenen Zwecken eingesetzt, zum Beispiel:

- **Mobile Alarm Reaction (MAR):** Definition von Zeitintervallen, in denen Reaktionen ausgelöst werden sollen, z.B. Email während der Arbeitszeit und SMS außerhalb der Arbeitszeit
- **Ereignis-Browser:** Filtern der Anzeige, um nur Ereignisse während eines bestimmten Zeitintervalls anzuzeigen
- **Report Manager:** Automatische Generierung von Reports zu bestimmten Terminen
- **Event Correlation Engine (ECE):** Zeitabhängige Filterung von Ereignissen
- **Event Correlation Engine (ECE):** Ablaufplan für Wartungsfenster

20.1 Konfiguration

Der Konfigurationsdialog für einen Zeitplan kann überall dort aufgerufen werden, wo Zeitpläne eingesetzt werden, z.B. im MAR oder im Report Center. Eine zentrale Übersicht aller definierten Zeitpläne erlaubt der Hauptmenüpunkt **Server->Zeitplaner...**.

Der Dialog zur Konfiguration eines Zeitplans orientiert sich an einer Kalenderdarstellung und beinhaltet fünf verschiedene Sichten: Jahr, Monat, Woche, Tag und Liste. Alle Sichten stellen die für den aktuell angezeigten Zeitraum (z.B. aktueller Monat) definierten Termine dar. Eine Ausnahme bildet die Listendarstellung: Dieser bietet eine Übersicht aller Termine des Zeitplans unabhängig eines betrachteten Zeitintervalls.

20.1.1 Einfacher Termin

Ein einfacher Termin oder ein einfaches Zeitintervall kann in einer der Ansichten Jahr, Monat, Woche oder Tag durch einen Klick mit der rechten Maustaste hinzugefügt oder editiert werden. Über die Auswahl von **Termin hinzufügen** oder **Bearbeiten** aus dem Kontextmenü öffnet sich ein Dialog zur Konfiguration der folgenden Parameter:

- **Beschreibung**
  Ein beliebiger Beschreibungstext für den Termin bzw. das Zeitintervall
- **Von**
  Der Startzeitpunkt des Termins oder des Zeitintervalls im Format "`TT.MM.JJJJ`"
- **Bis**
  Der Endzeitpunkt des Termins oder des Zeitintervalls im Format "`TT.MM.JJJJ`"

Die Definition eines einfachen Termins ist hiermit abgeschlossen. Für die restlichen Parameter können die Standardwerte beibehalten werden. Weitergehende Konfigurationsmöglichkeiten werden im folgenden beschrieben.

20.1.2 Serien von Terminen bzw. Zeitintervallen

Serien von Terminen sind Termine, die sich in regelmäßigen Abständen wiederholen. Zur Konfiguration einer solchen Serie müssen die folgenden Parameter definiert werden:

- **Periode**
  Das Wiederholungsintervall der Terminserie: Tag, Woche, Monat, Jahr, Einmal (Standardwert für einfache Termine)
- **Wiederholungsende**
  Das Datum, an dem die Terminserie endet
- **Multiplikator**
  Der Multiplikator definiert die Lücke zwischen zwei aufeinanderfolgenden Wiederholungen. Beispielsweise erzeugt die Definition der Periode "Tag" und des Multiplikators "2" eine Terminserie, bei welcher der Termin alle zwei Tage wiederholt wird.

Zur besseren Orientierung innerhalb der Übersichten werden die zur gleichen Serie gehörenden Termine mit der gleichen Farbkodierung (Hintergrund- und Randfarbe) dargestellt.

20.1.3 Ausschließen einzelner Tage von einer Terminserie

Falls bestimmte Tage von einer Terminserie ausgeschlossen werden sollen, können diese als "Ausnahmen" definiert werden. Dies geschieht wie folgt:

- **Ausnahmen**
  Ein Ausnahmedatum kann im Format "`TT.MM.JJJJ`" eingegeben und zur Liste der Ausnahmen hinzugefügt werden. An diesen Tagen wird die Terminserie ausgesetzt. Es können beliebig viele Ausnahmen hinzugefügt werden.
- **Intervalltyp**
  Der Intervalltyp wird dazu verwendet, ein Zeitintervall als "In Betrieb" oder "Außer Betrieb" zu markieren. Diese Markierung wird von einigen Komponenten wie dem Report Manager verwendet, um zwischen verschiedenen Intervallen zu unterscheiden. Beispielsweise kann dadurch ein Bericht generiert werden, welcher nur die Ereignisse umfasst, die während der Betriebszeiten ("In Betrieb") aufgetreten sind.

Wenn sich Termine mit unterschiedlichen Intervalltypen überlappen, hat der Termin mit dem Intervalltyp "Außer Betrieb" Priorität. Beispiel: Ein Zeitintervall vom Typ "In Betrieb" ist definiert von 12:00 bis 14:00, ein anderes Zeitintervall vom Typ "Außer Betrieb" ist definiert von 13:00 bis 15:00. Ein Bericht basierend auf diesem Zeitplan und über Ereignisse, die während der Betriebszeiten aufgetreten sind, wird nur Ereignisse beinhalten, die zwischen 12:00 und 13:00 aufgetreten sind.

Hinweis:
Ein Zeitintervall von Typ "Außer Betrieb“, dass sich nicht mit einem Zeitintervall von Typ "In Betrieb" überschneidet, besitzt keinerlei Funktion.

20.2 Löschen

Termine können in den Ansichten Jahr, Monat, Woche oder Tag über einen rechten Mausklick auf den entsprechenden Termin und die Auswahl der gewünschten Löschfunktion gelöscht werden. Ist der Termin Teil einer Terminserie, so kann entweder die komplette Serie oder nur der einzelne Termin gelöscht werden.

Löschen

21 Startup Manager

Der OpenScape FM Startup Manager ist in der OpenScape FM-Installation enthalten.

Bei Windows-Systemen steht dieser Dienst unter dem Namen "`OpenScape FM Startup Service`" zur Verfügung und kann über den Windows Service Manager verwaltet bzw. gesteuert werden.

Bei Unix-Systemen handelt es sich hierbei um einen Dämon-Prozess, der über die Programmdateien `<OpenScape FM installation directory>/startStartupService` (Start) und `<OpenScape FM installation directory>/stopStartupService` (Stop) gestartet bzw. angehalten werden kann. Nach einem Neustart wird ein RC-Script mit dem Namen `S99OpenScape FM` aufgerufen, um einen automatischen Systemstart durchzuführen.

Über den Startup Manager kann der lokal installierte OpenScape FM-Server gestartet oder angehalten werden bzw. bei Bedarf ein Server-Neustart eingeleitet werden. Wird eine unerwartete Server-Terminierung erkannt, führt der Startup Manager automatisch eine bestimmte Anzahl von Neustartversuchen durch (standardmäßig zwei), um den OpenScape FM-Server neu hochzufahren. Bei Erreichen des Vorgabewerts für die Anzahl der automatischen Neustartversuche führt der Startup Manager keine weiteren Neustarts durch, bis der gesamte Startup Manager neu gestartet wird bzw. bis der Administrator den OpenScape FM-Server manuell wieder hochfährt.

Standardmäßig startet der Startup Manager den OpenScape FM-Server und Prozesse, die für das OpenScape FM benötigt werden (z.B. Tomcat, Java DB). Bei entsprechender Konfiguration können jedoch auch andere Dienste automatisch gestartet werden.

Wichtiger Hinweis:
Genau wie für den OpenScape FM-Server wird auch bei allen anderen automatisch gestarteten Diensten die Anzahl der Neustarts nach unerwarteter Beendung pro Dienst individuell gezählt. Wird die maximale Anzahl erlaubter Neustarts für *einen der Dienste* erreicht, wird der Startup Manager, und damit auch das OpenScape FM automatisch heruntergefahren, um einen inkonsistenten Gesamtsystemzustand zu vermeiden.

Wichtiger Hinweis:
Auch die Zähler der einzelnen überwachten Dienste werden nach einem erfolgreichen Neustart des Dienstes nicht zurückgesetzt. Die Rücksetzung erfolgt nur bei Neustart des Startup Managers.

Hinweis:
Die überwachten Dienste werden mit der Java-Option `ExitOnOutOfMemoryError` gestartet. Diese Option sollte im Regelfall einen Dienst beim ersten Auftreten eines OutOfMemory-Fehlers geordnet beenden, und so ein durch Speichermangel unkontrolliertes Verhalten verhindern.

Die Konfiguration des OpenScape FM Startup Managers wird im *Technician Guide* besprochen.

Die über den Startup Manager verwalteten Dienste lassen sich in drei Kategorien unterteilen, die sich durch die Art der Abwicklung unterscheiden: konform *(conform)*, nicht konform *(non conform)* und Dämonen *(daemons)*.

- **conform**: Diese Dienste unterstützen den OpenScape FM Startup Manager. Der Dienst wird bei jedem Anhalten oder Herunterfahren durch den OpenScape FM Startup Manager benachrichtigt. Konforme Dienste können den Startup Manager über Ihren aktuellen Status im Prozessablauf informieren. Abhängige Dienste werden gestartet, sobald die erforderlichen Dienste den Status „aktiv" *(running)* haben.

- **non conform**: Diese Dienste bieten keine Unterstützung für den OpenScape FM Startup Manager. Dienste dieser Kategorie werden beim Anhalten oder Herunterfahren des Servers automatisch deaktiviert bzw. abgebrochen. Es wird sofort bzw. nach einem vordefinierten Zeitüberlauf davon ausgegangen, dass der gestartete Dienst den Status „gestartet“ hat.
- **daemon**: Diese Dienste werden nur gestartet und nicht weiter berücksichtigt. Es wird sofort bzw. nach einem vordefinierten Zeitüberlauf davon ausgegangen, dass der gestartete Dienst den Status „gestartet“ hat. Stopp- und Neustart-Aktionen werden für diese Dienste nicht unterstützt.

Der Startup Manager bietet die Möglichkeit, Abhängigkeiten zwischen verschiedenen Diensten zu definieren. In diesem Fall werden alle Dienste, von denen ein bestimmter Dienst abhängig ist, zuerst gestartet. Wird ein Dienst mit abhängigen Diensten angehalten, werden zunächst diese abhängigen Dienste angehalten. Ausnahmen hiervon sind Dämon-Dienste sowie Dienste, die unerwartet beendet werden. In diesen Fällen werden die abhängigen Dienste nicht angehalten.

Der OpenScape FM Startup Manager kann über die OpenScape FM Bedienoberfläche überwacht werden (siehe *Abschnitt 21.1, „Bedienoberfläche“*).

21.1 Bedienoberfläche

Nach dem Start des OpenScape FM erscheint ein Startup Manager-Symbol in der Server-Submap (**Root->System->Server->Administration->Startup Manager**). Unter dem Startup Manager-Symbol befindet sich ein Symbol für den OpenScape FM-Dienst. Ist der Startup Manager für den Start anderer Dienste konfiguriert, sind auch Symbole für diese anderen Dienste verfügbar. Das Kontextmenü des Startup Manager-Symbols enthält die Option **Zeige Dienste...**, über die sich ein Browser mit den Eigenschaften aller Dienste öffnen lässt. Diese Menüposition ist auch im Hauptmenü unter **Server->Administration->Startup Manager->Zeige Dienste** in der Hauptmenüleiste zu finden.

Im List Services-Browser werden folgende Eigenschaften für Dienste angezeigt:

- **Dienst Name**:
  Der Name des jeweiligen Dienstes (dessen ID)
- **Status:**
  Der aktuelle Status des Dienstes (siehe *Abschnitt 21.2, „Dienst-Status“*)
- **Status Message:**
  Eine optionale Statusmeldung, die gegebenenfalls vom Dienst selbst bereitgestellt wird
  Nur die jeweils letzte Meldung ist hier zu sehen.
- **Laufzeit:**
  Die Laufzeit des jeweiligen Dienstes
- **Startup Typ:**
  Der Start-Typ des jeweiligen Dienstes.
- **Abhängigkeiten:**
  Abhängigkeiten zu anderen registrierten Diensten, die beim Starten/Anhalten des Dienstes zu berücksichtigen sind

Der List Services-Browser zeigt immer nur einen registrierten Prozess pro Zeile an. Über die Schaltflächen **Dienst starten**, **Dienst stoppen** und **Dienst neu starten** können Sie den gewählten Prozess starten, anhalten oder neu starten. Bei Betätigung der Schaltfläche **Aktualisieren** werden die Anzeigedaten aktualisiert.

Warnung:
Wird die Schaltfläche **Dienst stoppen** angeklickt, während der OpenScape FM-Prozess unterlegt ist, wird der OpenScape FM-Server, bei dem der Anwender angemeldet ist, angehalten, und alle Clients werden geschlossen. Das System sollte daher auf jeden Fall so konfiguriert werden, dass nicht jeder Anwender diesen Dialog aufrufen kann (siehe *Abschnitt 21.3, „Rechtekonfiguration“*). Vergewissern Sie sich in jedem Fall, dass Sie den Server, bei dem Sie derzeit angemeldet sind, wirklich anhalten möchten.

Die Symbole der Dienste verfügen über ein Kontextmenü mit folgenden Menüpositionen:

- **Properties...**
  Öffnet ein Browser-Fenster mit den Eigenschaften des gewählten Dienstes.
- **Stop Service**
  [Nur verfügbar, wenn der Dienst den Status „aktiv“ *(running)* hat.]
- **Restart Service.**
  [Nur verfügbar, wenn der Dienst den Status „aktiv“ *(running)* hat.]
- **Start Service**
  [Nur verfügbar, wenn der Dienst den Status „beendet“ *(terminated)* hat.]

21.2 Dienst-Status

Folgende Dienstzustände sind möglich:

Dringlichkeit	Status	Beschreibung
	Wird gestartet *(starting)*	Der Startup Manager versucht gerade, den Dienst zu starten.
	Keine Startmeldung *(no start message)*	Der Dienst hat innerhalb des vorgegebenen Zeitlimits keine Startmeldung übermittelt [nur konforme Dienste]. Weitere Informationen zu den Zeitüberlauf-Werten finden Sie im *Technician Guide*
	Aktiv *(running)*	Der Dienst wurde erfolgreich gestartet und ist jetzt aktiv [nur konforme Prozesse].
	Gestartet *(started)*	Der Dienst wurde gestartet [nicht konforme Dienste und Dämon-Dienste].
	Wird heruntergefahren *(shutting down)*	Der Dienst wird heruntergefahren.
	Angehalten *(stopped)*	Der Dienst meldet, dass er angehalten wurde [nur konforme Dienste].

Tabelle 5 Dienst-Status

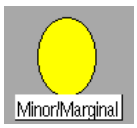
Dringlichkeit	Status	Beschreibung
	Beendet *(terminated)*	Der Dienst ist nicht mehr aktiv.
	Nie aktiv *(never run)*	Der Dienst konnte nicht gestartet werden, da Probleme bei der Befehlsausführung bzw. in der Konfigurationsdatei aufgetreten sind.
	Ungeklärte Abhängigkeiten *(unresolved dependencies)*	Konfigurierte Abhängigkeiten konnten nicht geklärt werden.

Tabelle 5 Dienst-Status

21.3 Rechtekonfiguration

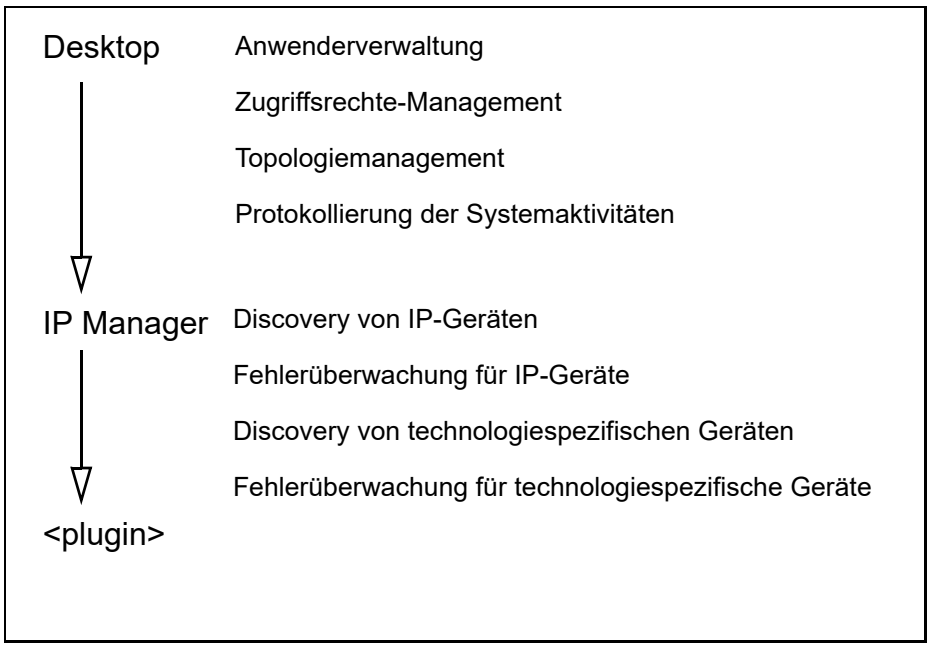
Der Startup Manager ist ein leistungsstarkes Tool. Es sollte daher sichergestellt werden, dass nicht jedem Anwender ein umfassender Zugang zur Bedienoberfläche des Startup Managers möglich ist. Um die Funktionalität der Bedienoberfläche einzuschränken, können bei Bedarf entsprechende Zugriffsrechte für den Startup Manager vereinbart werden (weitere Informationen hierzu finden Sie in *Kapitel 15, „Zugriffsrechte“*). Der Startup Manager unterstützt zwei vordefinierte zusammengesetzte Rechte:

- **Base->Startup Administrator** gestattet es einem Anwender, den Dienst, für den dieses Zugriffsrecht vereinbart wurde, anzuhalten und (neu) zu starten.
- **Base->Startup Operator** gestattet nur die Einsicht der dienstespezifischen Eigenschaften.

22 Plugin-Module

22.1 Plugin-Module und ihr Zusammenwirken

Bislang haben Sie den OpenScape FM Desktop lizenziert, und möglicherweise einige Plugin-Module initialisiert. Damit lässt sich jedoch kein umfassendes Netzwerkmanagement erreichen. Daher geben wir Ihnen vor der detaillierten Betrachtung der Desktop-Funktionen einen Überblick über die verschiedenen Module des OpenScape FM und deren Zusammenwirken.



Der Desktop bietet die Bedienoberfläche für Ihr Netzwerkmanagement. Der Desktop bildet außerdem die Grundlage für verschiedene Plugin-Module zur Anwenderverwaltung, zur Kontrolle der Zugriffsrechte und zur Anzeige der Netzwerktopologie.

Die Initialisierung des IP Manager Plugins erfolgt automatisch während des Initialisierungsprozesses. Der IP Manager erfüllt mehrere Aufgaben: er führt die IP-Discovery aus, welches die Grundlage für das gesamte Netzwerkmanagement bildet, und er kann die IP-Geräte auf Fehler überwachen.

Jedes **Plugin** erfüllt ebenfalls mehrere Aufgaben:

- Es bietet die Funktionen zum Zugriff auf technologiespezifische Informationen (d. h. Auslesen der entsprechenden MIB oder Abwickeln der spezifischen Anforderungen/Antworten in HTTP/XML).
- Es umfasst die Funktionen zur Discovery von für die Umgebung des <Plugin-Typs> spezifischen Geräten.
- Es verarbeitet die Fehlerinformationen der jeweiligen Geräte.

Plugin-Module

Plugin-Module und ihr Zusammenwirken

23 Fehlerbeseitigung

Falls bei der Arbeit mit OpenScape FM einmal Probleme auftreten sollten, haben Sie mehrere Möglichkeiten festzustellen, um was für eine Art von Fehler es sich handelt:

23.1 Protokolldateien

Startup Manager:
Das Verzeichnis `<OpenScape FM Installation directory>/startup/log` enthält eine Protokolldatei für jeden überwachten Dienst. Für OpenScape FM hat diese Datei den Namen `OpenScapeDesktop.log`.

Server:
In den Dateien server.log und java.log sind Protokolle des Servers gespeichert. Sie können diese Dateien selbst analysieren oder an einen OpenScape FM-Spezialisten weiterreichen, um die Ursachen von Fehlern festzustellen.

Die maximale Größe der Logdateien kann über den Hauptmenüeintrag **Server->Administration->Server-Eigenschaften** auf der Seite **Start Agrumente des Server Prozesses** konfiguriert werden (siehe *Abschnitt 6.2*).

In der Datei `trap.log` sind alle ankommenden SNMP-Traps an den Standard-Port 162 aufgelistet.

Die Log-Dateien können im Client über den Hauptmenüeintrag **Server->Administration->Debug-Optionen** betrachtet werden. Dazu muss auf der Debug-Seite über das unter befindliche Menü eine Logdatei ausgewählt und die Schaltfläche **Logdatei anzeigen** angeklickt werden.

Client:
Die erste Zeile des Meldungsprotokolls *Abschnitt 5.10, „Meldungsprotokoll“* zeigt an, wo die Protokolldatei für den Client gespeichert ist.

23.2 Log- und Debug-Konfiguration

Um eine einfache Konfiguration von Logging- und Debug-Optionen zur Verfügung zu stellen, bietet das OpenScape FM ein Log- und Debug-Konfigurationswerkzug an. Dieses Werkzeug dient dazu, für jedes einzelne initialisierte Plugin serverseitige Debug- und Log-Ausgaben ein- und auszuschalten. Hier können auch die vom Produkt-Support zur Fehler-Diagnose benötigten Dateien automatisiert in einer Archiv-Datei zusammengefasst werden.

Das Fenster des Log- und Debug-Konfigurationswerkzeug kann über den Menü-Befehl **Server->Administration->Debug-Optionen...**, der sich in der Hauptmenüleiste des OpenScape FM Clients befindet, geöffnet werden.

Die Spalte **Kategorie** enthält alle initialisierten Plugins. Die Spalten **Logging** und **Debugging** zeigen den aktuellen Log- und Debug-Status an. Ist ein Statusfeld aktiviert ist die jeweilige Option für dieses Plugin eingeschaltet.

Um die Debug-Option einzuschalten, sollte eines oder auch mehrere Plugins aus der Liste ausgewählt werden und rechts von der Liste das Statusfeld **Debugging** ausgewählt werden. Anschließend sollte das Auswahlfeld  gedrückt werden. Sobald das Auswahlfeld  gedrückt wurde, wird die Änderung angezeigt:

- in der Spalte **Debugging** ist das entsprechende Statusfeld aktiviert.
- von diesem Zeitpunkt an werden detaillierte Debug-Informationen in die Server-Logdatei geschrieben.

Um erweiterte Logging-Informationen in der Server-Logdatei zu erhalten, müssen die gleichen Anweisungen wie für das Debugging durchgeführt werden, jedoch muss das Statusfeld **Logging** anstatt **Debugging** ausgewählt werden.

Der Dialog unterstützt die Mehrfachselektion, daher kann in einem Schritt eine (oder beide) Option(en) für mehrere ausgewählte Plugins aktiviert werden. Wenn eine Option für alle Plugins aktiviert werden soll, müssen alle angezeigten Plugins ausgewählt und das entsprechende Statusfeld eingeschaltet werden.

Die Log- und Debug-Optionen sind unabhängig voneinander, aus diesem Grund kann zur gleichen Zeit sowohl die Logging- **als auch** die Debugging-Option eingeschaltet sein.

Die Schaltfläche **Logdatei anzeigen** öffnet einen Informations-Browser, in dem die Server-Logdatei angezeigt wird. Hier können sie die Datei aktualisieren (**Aktualisieren**) und das Fenster wieder schließen (**Schließen**).

Die Schaltfläche **SNMP-Trap-Tool herunterladen** öffnet das Test-Trap-Tool (siehe *Abschnitt 23.6*).

Die Schaltfläche **Schließen** schließt das Fenster des Log- und Debug-Konfigurationswerkzeugs.

Mit Hilfe der Schaltfläche **Diagnose-Informationen erstellen** kann automatisiert eine Logging-Archiv-Datei erstellt werden, welche die gesammelten Daten, die für eine Diagnose benötigt werden, zusammenfasst.

In dem durch die Schaltfläche geöffneten Fenster kann eine Fehlerbeschreibung eingegeben werden. Außerdem kann ausgewählt werden, ob der aktuelle Thread-Status, ein aktueller Speicher-Dump und/oder alle Datenbank-Dateien des Server Prozesses dem Archiv hinzugefügt werden sollen. Zusätzlich kann festgelegt werden, ob das zu erstellende Archiv verschlüsselt mit einem Passwort gesichert werden soll. Wird die Schaltfläche **OK** betätigt, wird die Archiv-Datei erstellt, und der Anwender wird durch einen Datei-Browser dazu aufgefordert einen Speicherort und -namen auszuwählen.

Mit Hilfe der Skript-Datei `diagnose.bat` (für Windows-Systeme) oder `diagnose.sh` (für Linux-Systeme) kann die Erstellung einer Logging-Archiv-Datei alternativ angestoßen werden. Diese befinden sich unterhalb des OpenScape FM Installationsverzeichnisses im Ordner `diagnose` und müssen mit Administrator-Rechten gestartet werden.

Die Logging-Archiv-Dateien können, abhängig von der Auswahl der Parameter, ebenfalls Datenbank-, Heap- und Thread-Dumps erzeugen bzw. archivieren. Der Inhalt einer im gleichen Verzeichnis befindlichen Datei mit dem Namen `description.txt` kann dem Archiv zusätzlich als Problem-Beschreibungs-Datei hinzugefügt werden.

Die Skript-Dateien können, im Gegensatz zum zuvor beschriebenen Verfahren, auch verwendet werden, wenn der OpenScape FM Prozess gestoppt wurde.

Die Debug/Log-Konfiguration wird persistent abgespeichert und bleibt auch nach Server-Neustarts bestehen. Daher ist es möglich Debug-Informationen sowohl während der Server-Startup Phase als auch während der Laufzeit zu erhalten.

Das Einschalten der Debug- und Log-Optionen kann Performance-Einbußen verursachen. Eingeschaltete Debug- und Log-Optionen müssen manuell wieder ausgeschaltet werden.

Die geschrieben Debug-Information sind nicht für die Analyse durch den Anwender gedacht. Die Ausgaben enthalten technische Informationen über interne Server-Funktionen und werden vom Third-Level-Support und Entwicklungsteam für Debugging-Zwecke genutzt.

23.3 Server Informationen

Für den Fall das Probleme mit dem OpenScape FM Server auftreten, und der Third-Level-Support eingeschaltet werden muss, sind zusätzliche Informationen über den Server notwendig. Für diesen Zweck bietet der OpenScape FM Desktop, für Anwender mit Administrator Rechten, einen Info-Browser an, der die relevanten Informationen anzeigt. Dieser Info-Browser kann über den Menübefehl **Server->Administration->Server Eigenschaften** geöffnet werden. Er befindet sich auf der Seite **Info**.

23.4 Browser-Konfiguration

Wenn Ihr Web-Browser den Client nicht laden kann, überprüfen Sie Ihre Browser-Konfiguration. Möglicherweise sind die Proxy-Einstellungen nicht korrekt. Befinden sich Client und Server in gleichen Netzwerk, ist normalerweise kein Proxy erforderlich. Sie können in diesem Fall folgende Einstellung wählen: „no proxy for...“ <Server-IP-Adresse>.

23.5 Namens- und Adressauflösung

Wenn keine Client/Server-Verbindung zu Stande kommt, liegt möglicherweise ein allgemeines Problem mit der Namensauflösung innerhalb Ihres Netzwerks vor. Ist der DNS richtig konfiguriert? Wenn Sie die DNS-Funktion nicht nutzen, müssen Sie die Hosts-Dateien aller angeschlossenen Systeme „manuell“ aktualisieren.

Ein weiteres Problem kann auftreten, wenn Sie den Microsoft Internet Explorer verwenden: haben Sie die Adresse des OpenScape FM-Servers mit dem korrekten IP-Port, jedoch ohne Schrägstrich eingegeben, kann das Applet möglicherweise nicht geladen werden. Verwenden Sie daher die folgende URL:
http://<Name oder IP-Adresse des Servers>:3043/

23.6 Test-Trap-Tool

Um akute Probleme zeitnah melden zu können, wertet das OpenScape FM eingehenden SNMP-Traps aus. Gehen diese verloren, werden Probleme häufig erst zu einem späteren Zeitpunkt durch aktives Polling des OpenScape FM erkannt.

Besteht die Vermutung, dass die Auswertung von Traps durch das OpenScape FM gestört sein könnte, kann dies mit Hilfe des zum OpenScape FM Umfang gehörenden **Test-Trap-Tools** überprüft werden. Das Tool kann ebenfalls dazu verwendet werden, um die konfigurierten Reaktionen des OpenScape FM auf bestimmte Traps (z. B. im MAR-Umfeld) zu kontrollieren.

Tool-Installation:

Bevor das Tool eingesetzt werden kann, muss es zunächst auf dem lokalen Rechner eingerichtet werden.

Dies geschieht über ein Download, der über die Debug-Optionen-Seite (Hauptmenü-Eintrag **Server->Administration->Debug-Optionen**) mittels der Schaltfläche **SNMP-Trap-Tool herunterladen** angestoßen werden kann.

Die Schaltfläche öffnet einen Datei-Browser, in dem der Ablageort und der **Dateiname** des ZIP-Archives, welches das Test-Trap-Tool enthält, festgelegt werden kann. Die Schaltfläche **Speichern** stößt den Download an.

Nach erfolgreichem Download muss das ZIP-Archiv entpackt werden.

Tool-Ausführung:

Liegt das entpackte Verzeichnis des Tools vor, kann das Tool durch den Aufruf von `snmpTrapTool.bat` (Windows) oder `snmpTrapTool.sh` (Linux) aus dem Verzeichnis heraus gestartet werden.

Der Start des Tools öffnet ein Fenster, in dem ein **Trap Type** ausgewählt, unter **Trap Configuration** konfiguriert und schließlich mit **Send Trap** versendet werden kann.

Für alle Traps, die versendet werden sollen, muss eine Quelle und ein Ziel angegeben werden.

Dabei ist die Quelle (**From**) der IP-Knoten, für den ein Problem erzeugt werden soll. Das Ziel (**To**) ist der OpenScape FM-Server, der den Trap auswerten soll, zusammen mit dem **Port** auf dem der OpenScape FM-Server die Traps erwartet (Default: `162`).

Es können drei grundlegende Trap-Typen ausgewählt werden:

- **Link Down** und **Link Down SPAM**: Dies ist ein generischer Link-Down-Trap für die angegebene Quelle. Wird die SPAM-Variante gewählt, kann zusätzlich ausgewählt werden, wie oft (**Amount**) der Trap in kurzer Folge hintereinander versendet werden soll.
- **Link Up** und **Link Up SPAM**: Dies ist der passende Link-Up-Trap zur erstgenannten Auswahl.
- **OS4K**: Dies generiert einen *VIP PHONE failure* Alarm-Trap. Die Priorität (**Priority**) legt den Status des Alarms fest. Dabei steht `1` für *Minor*, `2` für *Critical* und `3` für *Warning*. Der **Status** legt fest, ob es sich um einen On- (`0`) oder Off-Alarm (`1`) handelt.

Die Schaltfläche **Send Trap** versendet den konfigurierten Trap an das ausgewählte Ziel und den ausgewählten Port.

Die Schaltfläche **Exit** beendet das Tool.

24 Datenbankdateien

Dauerhafte Informationen werden in Datenbankdateien im Verzeichnis `<Standardinstallationsverzeichnis>\server\database` (Windows) oder `<Standardinstallationsverzeichnis>/server/database` (Unix) gespeichert. Es liegen drei Dateien vor:

```
server.db.base
server.db.base.old
server.db.base.delta
```

OpenScape FM speichert alle Änderungen am System im Arbeitsspeicher und schreibt diese Änderungen in regelmäßigen Abständen in die Datei `server.db.base.delta`. Wenn die Größe der Delta-Datei einen bestimmten Grenzwert erreicht, werden die gesamten Informationen aus dem Arbeitsspeicher in die Datei `server.db.base` geschrieben.

Wichtiger Hinweis:
Vor einem externen Backup dieser Datenbankdateien muss der OpenScape FM-Server angehalten werden. Um die Dateien bei laufendem Server zu sichern, verwenden Sie den Backup-Mechanismus des OpenScape FM, siehe *Kapitel 19, „Backup und Wiederherstellung“*.

24.1 Zurücksetzten der Datenbank

Um alle Informationen, die in der OpenScape FM-Datenbank gesichert sind, zu löschen, muss die Datei `deleteFmDatabase` (Windows) bzw. `deleteFmDatabase.sh` (Unix) ausgeführt werden. Diese ausführbare Datei stoppt den OpenScape FM-Server, setzt die Datenbank zurück und startet den Server wieder. Anschließend muss das Passwort für root neu gesetzt werden.

25 NAT-Umgebung

Die Kommunikation zwischen dem OpenScape FM Server und dem OpenScape FM Client erfolgt durch die Benutzung des „Remote Method Invocation“ (RMI) Protokoll. RMI erlaubt das Ausführen von Methoden auf anderen Systemen. Beispeilsweise benutzt der Client einen RMI-Aufruf um eine bestimmte Operation auszuführen, die an einem spezifischen Menübefehl gebunden ist (z.B. IP-Knoten: **IP->Status aktualisieren**). Um solch einen Aufruf durchführen zu können, fordert der Client eine so genannte „Remote-Referenz“ des Objektes an, für den ein RMI-Aufruf gestartet werden soll. Diese Remote-Referenz beinhaltet die IP-Adresse des Servers zu dem das Objekt gehört. Im Falle einer NAT-Umgebung ist diese IP-Adresse nicht die IP-Adresse, unter der der Server dem Client bekannt ist. Das notwendige Mapping muss vom Client durchgeführt werden, um die IP-Adresse zu benutzen, unter der der Server dem Client bekannt ist.

Der OpenScape FM Server und Client benutzt einen speziellen Mechanismus, um eine NAT-Umgebung zu bemerken. Falls notwendig wandelt der Client die IP-Adresse um, um eine funktionierende RMI-Kommunikation gewährleisten zu können.

Der selbe Mechanismus wird auch verwendet, um ein ähnliches Problem zu lösen, das auftritt, wenn der Server zu mehreren Netzwerken gehört.

Falls der OpenScape FM Client erkannt hat, dass die IP-Adresse der „Remote-Referenz“ umgewandelt werden muss, wird dies angezeigt. In der oberen linke Ecke der Client GUI wird die Toolbar durch zusätzliche Informationen ergänzt:

- **NAT:** Die Toolbar wird durch den Begriff „NAT“ gefolgt von der reelen IP-Adresse erweitert.
- **Server mit mehreren Netzwerkkarten:** Die Toolbar wird durch den Begriff „MHH“ gefolgt von der IP-Adresse, die für die RMI-Kommunikation verwendet wird, ergänzt.

26 HTTPS und Zertifikate

26.1 Was ist HTTPS?

Beim HTTPS (HyperText Transfer Protocol Secure) handelt es sich um ein Verfahren zur Verschlüsselung und Authentifizierung der Kommunikation zwischen Webservern und -Browsern im World Wide Web. Technisch betrachtet definiert HTTPS eine zusätzliche Schicht zwischen HTTP und TCP.

Die Kommunikation zwischen Web-Server und -Browsern erfolgt nach dem in *Kapitel 27, „SSL-Verschlüsselung“* beschriebenen SSL-Verfahren.

26.2 HTTPS im OpenScape FM

Das HTTPS-Verfahren wird standardmäßig für die Kommunikation zwischen den OpenScape FM Clients und dem OpenScape FM Server verwendet. Optional kann auch in den HTTP-Modus gewechselt werden.

Die Aktivierung bzw. Deaktivierung des HTTPS-Modus für den Web-Server des OpenScape FM erfolgt im Client über ein Fenster, das durch den Aufruf des Hauptmenü-Eintrages **Server->Administration->Server Eigenschaften...** geöffnet wird. Die HTTPS-Konfiguration findet sich auf dem Reiter **SSL-Zertifikat**.

Die Seite **Allgemein** dient dazu festzulegen, welche Art der Kommunikation verwendet werden soll:

- Wird ein Haken vor den Eintrag **HTTPS Aktivieren** gesetzt, so wird der interne HTTP-Server des OpenScape FM auf HTTPS umgeschaltet.
- Wird ein Haken vor den Eintrag **RMI über SSL Aktivieren** gesetzt, so werden für die RMI-Kommunikation ebenfalls SSL-Sockets verwendet (siehe *Kapitel 27, „SSL-Verschlüsselung“*).

Wird der Verbindungsmodus umkonfiguriert, so erfolgt ein automatischer Neustart des OpenScape FM Servers.

Wurde eine HTTP-Verbindung konfiguriert, so können die Web-Clients wie bisher gestartet werden. Lediglich der Beginn der Aufruf-URL ändert sich nun von `https://` in `http://`.

Das OpenScape FM nutzt für die sichere Kommunikation Zertifikate für vier verschiedene Aufgaben:

1. Für die WebServer-Kommunikation zur Landing Page über Port `3043`.
2. Für die RMI-Kommunikation zwischen Server und Client (ebenfalls über Port `3043`).
3. Für die WebServer-Kommunikation zum Web Client und zum Performance Management Client über Port `3080`.
4. Für die Kommunikation mit IP-Knoten/Objekten im OpenScape FM.

Für die ersten drei Aufgaben verwendet das OpenScape FM standardmäßig selbst signierte Zertifikate. D. h. die für den Einsatz von HTTPS zwingend erforderlichen Zertifikate werden durch den OpenScape FM Server selbst erzeugt. Dies hat den Vorteil, dass die Zertifikate auch nach einer Umkonfiguration sofort zu Verfügung stehen, da sie nicht erst durch eine externe Zertifizierungsstelle bestätigt werden müssen. Damit verbundene Gebühren entfallen ebenfalls.

Allerdings haben sie den Nachteil, dass sie von Web-Browsern nicht als vertrauenswürdig eingestuft werden.

Hinweis:
Wenn die Startseite des OpenScape FM über HTTPS im Web-Browser geladen wird, wird eine Warnung ausgegeben, dass es sich **NICHT** um ein Sicherheitszertifikat handelt, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.

Wie stattdessen Benutzer definierte Zertifikate verwendet werden können, wird im folgenden Abschnitt beschrieben (siehe *Abschnitt 26.3*).

Wird für eine Verbindung ein selbst signiertes Zertifikat durch ein Benutzer definiertes ersetzt, so beendet dies für diese Verbindung den Selbst-Signierungs-Mechanismus.

Für die vierte Aufgabe, die Kommunikation mit IP-Knoten, werden Zertifikate verwendet, die vom jeweiligen IP-Knoten bereitgestellt werden. Normalerweise werden diese vom OpenScape FM automatisch während eines Status-Polls ermittelt (siehe *IP-Manager Bedienungsanleitung*). Die Zertifikate können aber auch über die Oberfläche des Clients unmittelbar geladen werden (siehe *Abschnitt 27.3*).

26.3 Erstellen und Importieren eines benutzerdefiniertes Zertifikats

Wird der interne Webserver des OpenScape FM im HTTPS Modus gestartet, generiert das OpenScape FM das dazu benötigte private/public Key Paar und erstellt außerdem ein selbstsigniertes Zertifikat für diese Schlüssel.

Dieses selbstsignierte Zertifikat des Webservers kann durch ein benutzerdefiniertes Zertifikat ersetzt werden, das von einer Certification Authority (CA) signiert wurde. Dies erhöht die Sicherheit, da neben der Verschlüsselung der Verbindung auch die Authentizität des Webservers von Beginn an garantiert ist und der Benutzer keine Warnungen des Browsers übergehen muss.

Wichtiger Hinweis:
Wird ein selbst signiertes Zertifikat durch ein Benutzer definiertes Zertifikat ersetzt, und läuft dieses ab, so wird es *nicht* automatisch durch ein neues selbst signiertes Zertifikat ersetzt/verlängert.

Die Beantragung, Erstellung und Importierung der Zertifikate wird durch die Oberfläche des OpenScape FM unterstützt (siehe *Abschnitt 26.3.1*). Die Einbindung der Zertifikate kann aber auch händisch erfolgen (siehe *Abschnitt 26.3.2*).

Die Liste aller dem OpenScape FM bekannten Zertifikate kann wie unter *Abschnitt 27.3* beschrieben eingesehen werden.

26.3.1 Erstellung der Zertifikate über die Benutzeroberfläche

Die Konfigurationsfenster zur Bearbeitung von Zertifikaten können über den Hauptmenü-Eintrag **Server->Administration->Server-Eigenschaften** geöffnet werden. Sie befinden sich auf der Seite **SSL-Zertifikat**.

Auf dieser Seite kann auf der Unterseite **Port 3043** das Zertifikat für die WebServer-Kommunikation zur Landing Page und für die RMI-Kommunikation zwischen Server und Client eingerichtet werden.

Auf der Unterseite **Port 3080** kann mit identischer Vorgehensweise das Zertifikat für die WebServer-Kommunikation zum Web Client und zum Performance Management Client eingerichtet werden.

Die Daten, die für die Erstellung eines selbstsignierten Zertifikats erforderlich sind, können im selben Konfigurationsfenster eingegeben werden
(Die in Klammern gesetzte Zeichenfolge entspricht den Distinguished Names (DN) im Zertifikat):

- Die Felder **Vollqualifizierter Domain-Name (CN)** und **Subjekt Alternative Bezeichnung (SAN)** dienen zur Eingabe der Host-Namen, für die das Zertifikat erstellt werden soll.
- Die Felder **Organisation (O)**, **Organisationseinheit (OU)**, **E-Mail-Adresse (EMAIL)**, **Land (C)**, **Lokation (L)** und **Staat (ST)** geben an, für wen das Zertifikat erstellt werden soll.
- Das Zertifikat wird Server seitig in einem Keystore abgelegt. Dieser Keystore ist mit einem Passwort geschützt. Das Passwort kann im Feld **Speicher-Passwort** festgelegt werden.
- Im Feld **Gültig (Tage)** wird die Gültigkeitsdauer des zu erstellenden Zertifikats festgelegt. Vor Ablauf der Frist wird durch den Server automatisch ein neues Zertifikat erstellt.

Wichtiger Hinweis:
Im Java-Client wird für den Keystore und für den Key immer das gleiche Passwort verwendet. Daher müssen das Keystore-Passwort und Key-Passwort immer gleich sein.

Im unteren Bereich kann dann, basierend auf diesen Daten, die jeweilige **Aktion** angestoßen werden.

Hier kann unter Anderem ein selbstsigniertes Zertifikat erstellt werden, die Daten für die Signierung durch eine Zertifizierungsstelle erzeugt werden, oder die Antwort der Zertifizierungsstelle dem Keystore hinzugefügt werden.

26.3.2 Manuelle Bearbeitung der Zertifikate

Um ein Zertifikat importieren zu können, muss zunächst ein benutzerdefiniertes Passwort für den vom Server generierten Key festgelegt werden. Das Passwort kann über den Hauptmenüdialog unter **Server->Administration->Server Eigenschaften** auf der Seite **SSL-Zertifikat** angegeben werden (siehe *Abschnitt 26.3.1*). Hier müssen die Unterseiten **Port 3043** (für die WebServer-Kommunikation zur Landing Page und für die RMI-Kommunikation zwischen Server und Client) oder **Port 3080** (für die WebServer-Kommunikation zum Web-Client und zum Performance Management Client) verwendet werden.

Das vom OpenScape FM-Server generierte private/public Key Paar ist für **Port 3043** unter dem Alias `internalwebserver` in der Datei
`<inst_dir>/server/database/trustedcerts.jks`
gespeichert, wobei `<inst_dir>` für das OpenScape FM-Installationsverzeichnis steht.

Für **Port 3080** wird der Alias `internaltomcatserver` in der Datei
`<inst_dir>/Wildfly/standalone/configuration/webappKeystore`
verwendet.

Bei diesen Dateien handelt es sich um einen *Java Key Store (JKS)*, in dem öffentliche und private Schlüssel und zugehörige Zertifikate passwortgeschützt verwaltet werden.

Um das selbstsignierte Zertifikat durch ein benutzerdefiniertes Zertifikat zu ersetzen, müssen für **Port 3043** folgende Schritte durchgeführt werden:

1. Wechseln in das OpenScape FM-Installationsverzeichnis und Erzeugen eines "Certificate Signing Request" für den generierten public key mit dem folgenden Befehl. Das verwendete Programm `keytool` gehört zum Installationsumfang *des Java Runtime Environment (JRE)*.

   ```
   keytool -certreq -alias internalwebserver -keystore keystore.jks -file csr.req
   ```

   Beim Ausführen des Befehls wird nach dem zuvor festgelegten Passwort für den Keystore gefragt. Das Schlüssel-Passwort (key password) und das Speicher-Passwort (store password) müssen identisch sein.

2. Das Kommando erzeugt eine Datei mit dem Namen `csr.req`, mit deren Hilfe ein neues Zertifikat erstellt werden kann. Diese Datei muss an die zuständige *Certificate Authority* gesendet werden.

3. Nach Erhalt des Zertifikates von der CA (z.B. `signed.cer`), kann es mit dem folgenden Befehl in den Keystore importiert werden. Der OpenScape FM Server muss vor dem Import gestoppt werden. Nach dem Import ist ein manueller Neustart des Servers notwendig.

   ```
   keytool -import -alias internalwebserver -keystore keystore.jks -file
   signed.cer
   ```

Für **Port 3080** muss der Alias durch `internaltomcatserver` ersetzt werden.

Beim Importieren des Zertifikats kann der folgende Fehler auftreten:

```
Keytool-Fehler: java.lang.Exception: Kette konnte nicht aus Antwort entnommen
werden.
```

In diesem Fall muss zunächst die gesamte Zertifikatskette in den Keystore importiert werden. Dazu muss der gleichen Befehl für alle Zertifikate der Kette ausgeführt werden, angefangen mit dem root-Zertifikat der CA:

```
keytool -import -alias root -keystore keystore.jks -file root.cer
```

Hinweis:
Wenn neben dem Zertifikat auch das generierte private/public Key Paar ersetzt werden soll, ist zu beachten, dass der neue Schlüssel die RSA-Verschlüsselung verwenden muss und unter dem Alias `internalwebserver` bzw. `internaltomcatserver` im Keystore gespeichert werden muss.

Weitere Informationen zum Java-Keytool finden sich unter:

```
http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html
```

27 SSL-Verschlüsselung

27.1 Was ist SSL?

Wenn Daten über ein Netzwerk übertragen werden, besteht die Gefahr, dass auch unbefugte Personen darauf zugreifen und diese Daten verändern können. Deshalb müssen vorab geeignete Maßnahmen ergriffen werden, um unbefugte Zugriffe zu verhindern und sicherzustellen, dass Daten während des Transports nicht manipuliert werden.

Im Internet werden Daten häufig mit Hilfe des SSL-Protokolls (Secure Socket Layer) verschlüsselt. Dieses ursprünglich von Netscape entwickelte Protokoll wird heute von den meisten Web-Browsern unterstützt. Basierend auf sicheren TCP-Sockets veranlasst dieses Protokoll zwei Vorgänge: Austausch des Secret Key (geheimer Schlüssel) und Verschlüsselung der Daten anhand dieses Schlüssels.

Eine SSL-Verbindung zwischen Client und Server wird mit einer als „SSL-Handshake" bezeichneten Verständigung eröffnet. Dabei sendet der Server zunächst einen Public Key (öffentlicher Schlüssel) an den Client, der damit einen generierten symmetrischen Session Key verschlüsselt. Dieser so genannte asymmetrische Verschlüsselungsmechanismus nimmt einige Zeit in Anspruch. Deshalb dauert zwar die erstmalige Herstellung einer Verbindung, nicht jedoch der nachfolgende Datentransfer länger als üblich (siehe *Abschnitt 27.2, „Verschlüsselung"*).

Nun verfügen Server und Client beide über einen Schlüssel, der dann für die Datenübertragung verwendet wird: Diese symmetrische Verschlüsselung dauert nicht länger als eine reguläre Verbindung.

Das SSL-Protokoll kommt auf TCP-Verbindungen zur Anwendung. Es ist also ein Protokoll der Anwendungsschicht, das zwischen die TCP-Schicht und das Protokoll für die Applikationsdaten eingefügt wird (siehe *Bild 37*).

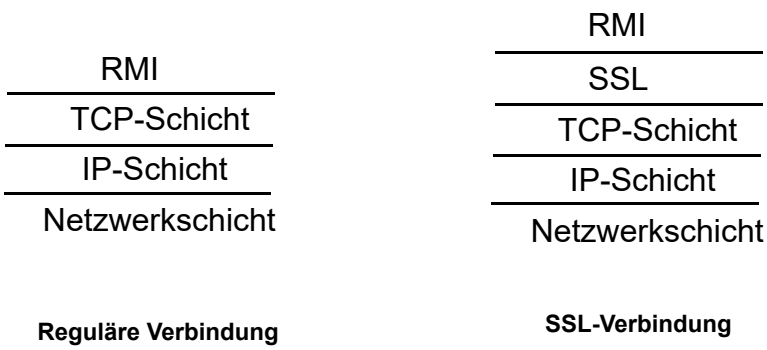


Bild 37 *Für den Datentransfer zwischen Server und Client in OpenScape FM benötigte Protokolle*

Eine SSL-Verbindung ist also eine sichere, verschlüsselte Verbindung für die Übertragung von Daten, die nur von dem SSL-Server und -Client gelesen werden können, die diese Verbindung eröffnet haben.

27.2 Verschlüsselung

Standardmäßig läuft der OpenScape FM-Server im SSL-Modus.

Über die Oberfläche des Clients kann dies umgestellt werden (siehe *Abschnitt 26.2, „HTTPS im OpenScape FM“*).

27.3 SSL Zertifikate

Die SSL Zertifikate können innerhalb des OpenScape FM über das Hauptmenü **Server->Administration->SSL Zertifikate** geladen und behandelt werden.

Behandlung bekannter Zertifikate:

Die Auswahl des Menüeintrags **Zertifikate anzeigen** führt zur Anzeige eines Fensters, das aus drei Seiten besteht, auf denen die aktuell dem OpenScape FM bekannten SSL Zertifikate behandelt werden:

- Die Seite **Nicht vertrauenswürdige Zertifikate** zeigt die Zertifikate an, die aktuell bekannt sind, denen aber nicht vertraut wird. Die unten befindlichen Schaltflächen können dazu verwendet werden, ein ausgewähltes Zertifikat aus dem OpenScape FM zu **Löschen**, oder um es in den **Vertrauen** Modus zu überführen.
- Die Seite **Vertrauenswürdige Zertifikate** die aktuell bekannten Zertifikate an, denen vertraut wird. Die unten befindlichen Schaltflächen können dazu verwendet werden, ein ausgewähltes Zertifikat aus dem OpenScape FM zu **Löschen**, oder um es in den **Nicht Vertrauen** Modus zu überführen.
- Die Seite **Gültigkeitsablauf** kann verwendet werden, um die Erstellung von Ereignissen zu konfigurieren, die erzeugt werden sollen, wenn die Gültigkeit eines vertrauenswürdigen Zertifikates bald abläuft.

  Jede Zeile innerhalb der Tabelle der Seite repräsentiert eine Regel um derartige Ereignisse zu erzeugen.

  Neue Regeln können erstellt, bestehende gelöscht, kopiert und die Reihenfolge der Regeln innerhalb der Tabelle verändert werden, indem Tabelleneinträge selektiert und die Schaltflächen unterhalb der Tabelle verwendet werden. Die Reihenfolge der Regeln hat *keine* Auswirkung auf deren Ausführung.

  Das **Netzwerk** und die **Maske** einer Regel definieren den IP-Bereich für den die Regel gültig ist. Bleiben diese Werte leer, gilt die Regel für alle IP-Knoten. Zertifikate werden gegen die IP-Adresse des Hosts getestet, zu dem sie gehören. Erzeugte Ablauf-Ereignisse werden ebenfalls diesem IP-Knoten zugewiesen.

  Der **Status** definiert den Status des Ereignisses, das als Ablaufwarnung erzeugt wird.

  Die **Ablaufzeit** legt fest wie lange vor dem Ende der Gültigkeit des Zertifikates das Ereignis erzeugt wird.

Laden neuer Zertifikate:

Der Menüeintrag **Zertifikate von Server importieren** kann verwendet werden, um weitere SSL Zertifikate zu importieren. Diese werden von dem Zertifikatserver geladen, der durch den angegebenen Hostnamen und Port identifiziert wird. Die geladenen Zertifikate werden als vertraute Zertifikate hinzugefügt.

28 Mobile Access

Mobile Access erlaubt den Zugriff auf wesentliche Management-Informationen des OpenScape FM mit Hilfe eines iOS or Android Telefons. Dies ist insbesondere für Service-Personal und für Rufbereitschaften hilfreich, da so ein einfacher Zugang zum OpenScape FM besteht, ohne die Notwendigkeit, sich im Büro aufhalten zu müssen.

Mobile Access erlaubt den Zugriff auf Ereignisse und das Betrachten von IP-Knoten über das OpenScape FM.

28.1 Technische Struktur

Der Mobile Client ist entsprechend der in *Bild 38* gezeigten Architektur implementiert.

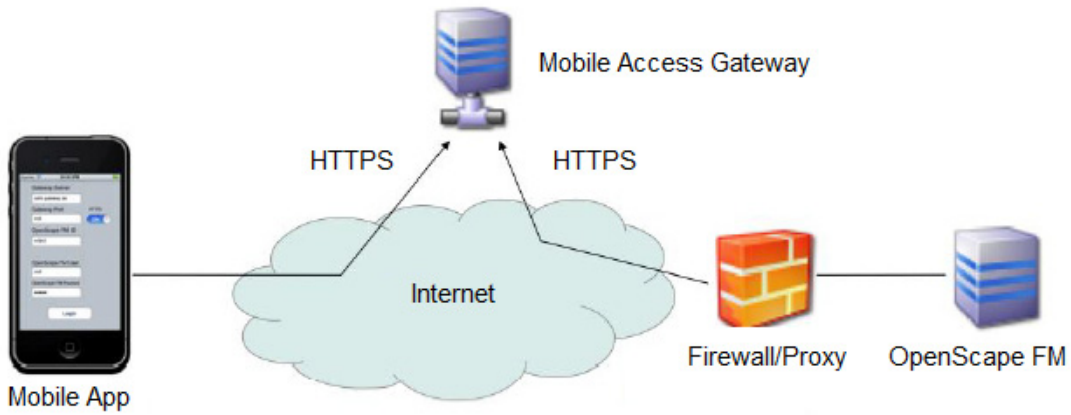


Bild 38 Technische Struktur

Der Mobile Client für iOS oder Android muss auf dem Telefon als App installiert werden (siehe *Abschnitt 28.4.1*). Die Telefon App richtet eine Verbindung zum gewünschten OpenScape FM Server ein, indem sie das Mobile Access Gateway verwendet. Das auf dem OpenScape FM Server installierte Mobile Access Gateway Plugin kommuniziert ebenfalls mit dem Mobile Access Gateway.

Dies bedeutet, dass die Kommunikation in Richtung des Mobile Access Gateways geschieht. Dies erlaubt die Verwendung sehr einfacher Firewall-Regeln.

Im Mobile Access Gateway werden beide Verbindungen zusammengeführt. Verbindungen, die durch einen Client angestoßen wurden, werden an die durch das Mobile Access Gateway Plugin auf einen OpenScape FM Server angestoßene Verbindung übergeben.

Falls der OpenScape FM Server direkt von der App erreicht werden kann, wird das Mobile Access Gateway nicht benötigt.

28.2 Mobile Access Gateway

Das Mobile Access Gateway ist dafür verantwortlich, die durch den Mobile Client erhaltenen Anfragen an den korrespondierenden OpenScape FM Server weiterzureichen. Es ist ebenfalls dafür zuständig, die Ergebnisdaten zu empfangen, und diese an den korrekten Client zu übermitteln. Wenn sich ein OpenScape FM das erste Mal mit dem Mobile Access Gateway verbindet, erhält dieses eine eindeutige ID. Der Mobile Client verwendet diese ID, um zu definieren, mit welchem OpenScape FM Server eine Verbindung eingerichtet werden soll.

Das Mobile Access Gateway wird nur benötigt, wenn mit den Mobile Client nicht direkt über das Netzwerk auf den OpenScape FM Server zugegriffen werden kann.

28.2.1 Mobile Access Gateway Installation

Das Mobile Access Gateway muss getrennt installiert werden. Dies geschieht durch das Ausführen der Datei `setup_mobilegw_osfm.exe` für Windows-Systeme oder `setup_mobilegw_osfm.sh` für Linux-Systeme, die sich auf dem Installationsmedium befindet.

Das Gateway installiert sich als ein Dienst mit der Bezeichnung ‚`OpenScape FM Mobile Access Gateway`‘.

Das Mobile Access Gateway muss auf einem System installiert werden, das sowohl vom Mobile Access Client wie auch vom OpenScape FM Server über HTTP/HTTPS erreicht werden kann.

Auf dem System muss ein Oracle Java installiert sein.

28.2.2 Mobile Access Gateway Konfiguration

Das Mobile Access Gateway wird durch die Anpassung der Datei `rserver.properties` konfiguriert. Diese befindet sich im Verzeichnis ‚`<installations-verzeichnis>/conf`‘.

Die Parameter ‘`httpport`‘ und ‚`httpsport`‘ in der Konfigurations-Datei definieren die Ports, die für HTTP- und HTTPS-Verbindungen benutzt werden sollen (z.B. `httpsport=443`). Diese Ports werden verwendet, um Anfragen vom Mobile Client und vom Mobile Access Gateway Plugin zu empfangen. Fehlt einer dieser Parameter, wird der entsprechende Dienst deaktiviert.

Der Parameter ‚`keystore`‘ definiert den Pfad zum Java Key Store (e.g. `keystore=conf/rsrv_keystore`). Existiert der Key Store nicht, wird er beim nächsten Start des Gateways erstellt.

Der Parameter ‚`keypasswd`‘ definiert das Passwort, mit dem auf den Key Store zugegriffen wird.

Der Parameter ‚`alias`‘ definiert das Zertifikat, das für den HTTPS-Zugang benutzt werden soll. Falls das Zertifikat nicht existiert, wird ein selbst-signiertes Zertifikat dieses Namens erzeugt.

Wird ein HTTPS-Zugang verwendet, muss für das Mobile Access Gateway die gleiche Java-Version verwendet werden wie für den OpenScape FM Server.

28.3 Mobile Access Gateway Plugin

Das OpenScape FM muss seine Daten dem Web-Client zu Verfügung stellen. Diese Aufgabe wird durch das Mobile Access Gateway Plugin verrichtet.

Das Mobile Access Gateway Plugin kommuniziert mit dem Mobile Access Gateway. Es erhält Anfragen, die vom Mobile-Client an das Mobile Access Gateway gesendet wurden, und arbeitet diese ab. Die Ergebnisse werden dann zurück an das Mobile Access Gateway gesendet, das sie an den Mobile Client übermittelt.

Wenn sich der OpenScape FM Server mit dem Mobile Access Gateway verbindet, registriert er sich mit einer ID. Diese ID wird vom Mobile Client verwendet, um eine Verbindung zum OpenScape FM zu etablieren.

Die ID und der allgemeine Status des Mobile Access Gateway können im OpenScape FM angezeigt werden, indem in einem OpenScape FM Client der Hauptmenü-Eintrag **Server->Administration->Mobile Access->Status** ausgewählt wird.

28.3.1 Mobile Access Gateway Plugin Installation

Das Mobile Access Gateway Plugin ist ein Plugin für das OpenScape FM. Es wird während des Installationsprozesses des OpenScape FM automatisch installiert.

Um es verwenden zu können, muss es durch Auswahl des Hauptmenü-Eintrages **Server->Plugins->Initialisiere Mobile Access Plugin** initialisiert werden.

28.3.2 Mobile Access Gateway Plugin Konfiguration

Wenn das Mobile Access Gateway Plugin aktiviert wurde, kann es mit dem Mobile Access Gateway verbunden werden.

Dies kann durch die Auswahl des Hauptmenü-Eintrages **Server->Administration->Mobile Access->Konfigurieren...** in einem OpenScape FM Client angestoßen werden.

Diese Aktion öffnet ein Fenster, in dem die Verbindungsdaten und der Verbindungstyp für das Mobile Access Gateway eingegeben werden können. Wurde eine Verbindung erfolgreich etabliert, wird die Verbindungs-ID im Feld **Server ID** angezeigt. Diese ID wird im Mobile Client benötigt, um das OpenScape FM zu identifizieren.

Die Schaltfläche **Aktivieren** oder **Deaktivieren** kann verwendet werden, um die Verbindung für Mobile Clients zu aktivieren oder zu deaktivieren.

Da die **Server ID** einen OpenScape FM identifiziert, wird sie nicht verändert wenn eine Verbindung deaktiviert/ aktiviert wird. Die Erzeugung einer neuen ID kann jedoch mit Hilfe der Schaltfläche **Löschen** erzwungen werden. Dies macht die alte ID ungültig. Eine neue ID wird bei der nächsten erfolgreichen Verbindung erzeugt.

28.3.3 Benutzersicht

Neben Ereignissen und IP-Knoten kann auch jedes andere Objekt, das im OpenScape FM angezeigt wird, auch im Mobile Client angezeigt werden. Die Objekte, die exportiert werden sollen, müssen im OpenScape FM konfiguriert werden.

Wenn im Mobile Client eine Objekt-Suche durchgeführt wird, und die Suchoption **Benutzersicht** das erste mal verwendet wird, wird ein Container-Objekt mit dem Label **Mobile Access** auf der Submap des Anwender-Symbols des entsprechenden Anwenders angelegt. Objekte, die in dieses Container-Objekt kopiert werden, können im Mobile Client betrachtet werden.

28.4 Mobile Client

Der Mobile Client ist eine App, die auf einem Apple oder Android Mobil-Telefon läuft. Es stellt eine Benutzeroberfläche bereit, um sich mit einem OpenScape FM Server zu verbinden, und um Ereignisse und IP-Knoten anzuzeigen.

Wird ein Mobile Client gestartet, verbindet er sich mit dem konfigurierten Mobile Access Gateway und führt ein Login auf dem ausgewählten OpenScape FM Server aus. Wurde der Login durchgeführt, ermittelt er Daten, indem er weitere Anfragen an das Mobile Access Gateway sendet.

Es ist frei konfigurierbar welches Mobile Access Gateway und welches OpenScape FM durch die App verwendet werden sollen.

28.4.1 Mobile Client Installation

Der Mobile Client für iOS muss vom Apples App-Store geladen und installiert werden.

Der Mobile Client für Android muss vom Google Play Store geladen und installiert werden.

28.4.2 Allgemeine Funktionen

Der Mobile Client zeigt die Objekte und Ereignisse an, die auf dem entsprechenden OpenScape FM Server gefunden werden.

Im Allgemeinen werden Objekte und Ereignisse in Form von Listen dargestellt. Dabei entspricht jeder Eintrag einem Objekt oder einem Ereignis.

Werden Listen-Einträge angetippt, werden nähere Details zum Eintrag angezeigt. Wird eine Pfeil-Schaltfläche, die sich an der rechten Seite befindet, angetippt, werden Daten, die sich auf den ausgewählten Eintrag beziehen, angezeigt.

Die einzelnen **Tabs** können geöffnet werden, indem die unten befindlichen Schaltflächen betätigt werden (iOS Version), oder über Menüeinträge, die von links in die Oberfläche gewischt werden (Android Version).

Die Schaltfläche in der rechten oberen Ecke, die einen kreisförmigen Pfeil darstellt, kann verwendet werden, um die angezeigten Daten zu aktualisieren.

Die Schaltfläche in der linken oberen Ecke, die den Namen der Liste anzeigt, kann verwendet werden, um auf die zuvor geöffnete Liste zu wechseln.

Die folgenden Kapitel beschreiben die Benutzeroberfläche des Mobile Client näher (die Bildschirmfotos entstammen aus der iOS Version).

28.4.3 Login

Wird die Mobile Client App gestartet, muss zunächst ein Login auf einem Mobile Access Gateway, der irgendwo läuft durchgeführt werden. Alternativ kann der Login auch auf einem OpenScape FM Server durchgeführt werden, der sich in einem lokal erreichbaren Netzwerk befindet.

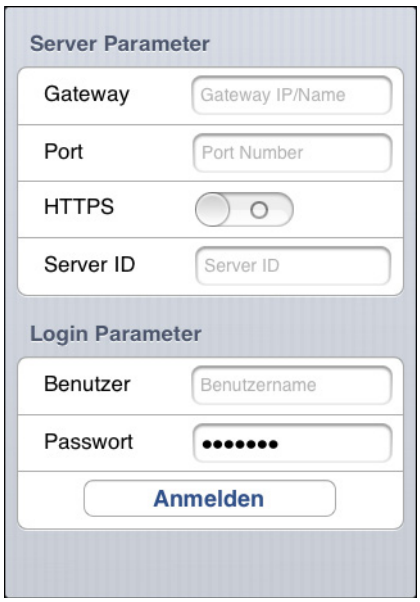


Bild 39 Login

Das Login-Fenster (siehe *Bild 39*) fragt die Verbindungs-Daten und -Methode ab. Soll eine Verbindung zu einem Mobile Access Gateway etabliert werden, muss die **Server ID** des gewünschten OpenScape FM eingegeben werden. Die **Server ID** kann in einem OpenScape FM Client über die Hauptmenü-Einträge **Server->Administration->Mobile Access->Status** oder **Server->Administration->Mobile Access->Konfigurieren** angezeigt werden.

Der **Anwender** und das entsprechende **Passwort** müssen einem Anwender im OpenScape FM entsprechen.

28.4.4 Übersicht

Der **Übersicht** Tab des Mobile Client kann verwendet werden, um einen ersten Eindruck über den Status der überwachten Objekte auf dem OpenScape FM Server zu gewinnen.

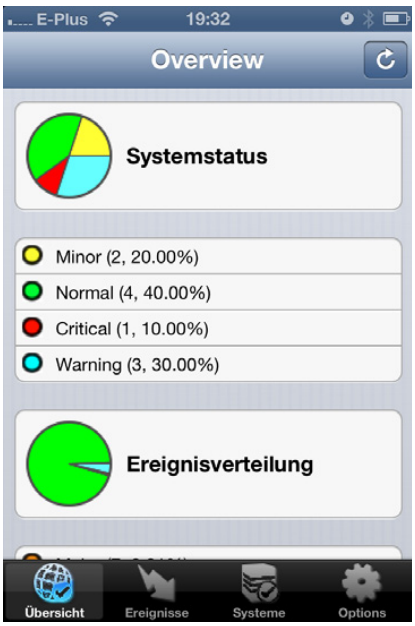


Bild 40 *Übersicht*

Der Tab (siehe *Bild 40*) liefert einen Überblick über die Verteilung des System-Status für die überwachten Objekte und den Ereignis-Status der aktuell unbestätigten Ereignisse. Dies erlaubt es einem Techniker auf den ersten Blick zu erkennen, ob Probleme vorliegen, denen Beachtung geschenkt werden muss.

Wird ein Statuseintrag berührt, öffnet sich eine Liste mit den unbestätigten und nicht korrelierten Ereignissen, die den entsprechenden Status besitzen.

28.4.5 Ereignisse

Der **Ereignisse** Tab des Client erlaubt den Zugriff auf die Ereignisse, die im Ereignis-Browser des OpenScape FM aufgelistet sind. Die Liste ist nach Datum sortiert. Dabei befindet sich das aktuellste Ereignis am Anfang der Liste.

28.4.5.1 Ereignis-Suche

Generell zeigt der **Ereignisse** Tab alle Ereignisse an, die im Ereignis-Browser des OpenScape FM angezeigt werden. Die Ereignisse werden in ‚Korrelierter Sicht' angezeigt (korrelierte Ereignisse werden in einer einzelnen Zeile zusammengefasst).

Um spezifische Ereignisse zu finden, können die folgenden Parameter ausgewählt werden, um die Anzeigeliste auf die Ereignisse zu beschränken für die alle ausgewählten Parameter zutreffen (siehe *Bild 41*).

Bild 41 Ereignis-Suche

- **Von Datum**, **Bis Datum**: Es werden nur die Ereignisse angezeigt, die im gewählten Zeitintervall aufgetreten sind.
- **Text**: Der eingegebene Text muss Bestandteil des **Ursprungs**, der **Kategorie** oder der **Beschreibung** sein.
- **Status**: Das Ereignis muss einen der ausgewählten Status-Werte haben.

28.4.5.2 Ereignis-Browser

Der **Ereignis-Browser** (siehe *Bild 42*) zeigt alle Ereignisse an, die den ausgewählten Suchkriterien entsprechen (siehe *Abschnitt 28.4.5.1, „Ereignis-Suche“*). Wurde keine Suche spezifiziert, werden alle Ereignisse angezeigt. Die Schaltfläche **Suchen** in der linken oberen Ecke öffnet die Ereignissuche-Sicht.

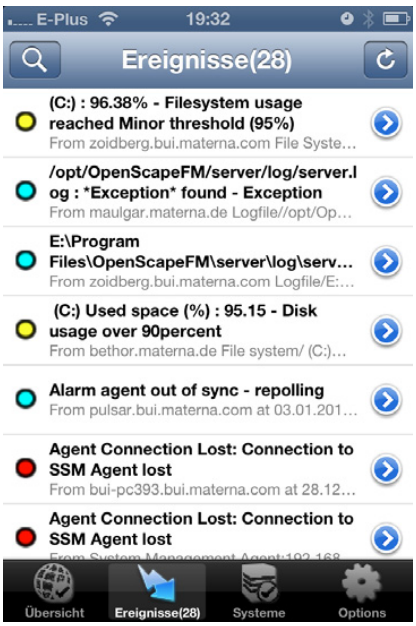


Bild 42 Ereignis-Browser

Wird ein Ereignis gedrückt, öffnet sich die Ereignis-Detailansicht (siehe *Abschnitt 28.4.5.3, „Ereignis-Details“*).

Existieren für ein Ereignis korrelierte Ereignisse, so wird auf der rechten Seite des Ereignisses eine Pfeil-Schaltfläche angezeigt. Wird diese ausgewählt, öffnet sich eine neue Ereignis-Liste, die nur die korrelierten Ereignisse enthält.

28.4.5.3 Ereignis-Details

Der Ereignis-Detailsansicht öffnet sich, wenn ein Ereignis im Ereignis-Browser gedrückt wird. Sie zeigt detaillierte Informationen über das ausgewählte Ereignis an. Die Bestätigen-Schaltfläche kann verwendet werden, um das Ereignis im OpenScape FM zu bestätigen. Existieren untergeordnete Ereignisse, so werden diese ebenfalls bestätigt.

28.4.6 IP-Knoten- und Objekt-Browser

Der Tab **Knoten** erlaubt den Zugriff auf IP-Knoten und Objekte, die durch den OpenScape FM Server verwaltet werden. Er enthält Listen von IP-Knoten oder von Objekten, die sich auf der Submap ‚Mobile Access‘ des Anwenders befinden, und erlaubt die Navigation durch den Objekt-Baum.

28.4.6.1 Knoten-Suche

Generell zeigt der **Knoten** Tab alle IP-Knoten an, die im OpenScape FM angezeigt werden.

Um spezifische Knoten zu finden, können die folgenden Parameter ausgewählt werden, um die Anzeigeliste auf die Knoten zu beschränken für die alle ausgewählten Parameter zutreffen.

- **Text**: Der eingegeben Text muss Bestandteil des **Knoten-Bezeichner**s, des **Hostnamen** oder der **IP-Adresse** sein.
- **Status**: Der Knoten muss einen der ausgewählten Status-Werte haben.

In der Knoten-Suche kann die Sicht auf ‚**Benutzersicht**' umgestellt werden. Ist dies der Fall, so wird die im Plugin ausgewählte Objektliste im Browser dargestellt. (siehe *Abschnitt 28.4.6.2, „Knoten-Browser"*). Dies sind die Objekte, die im OpenScape FM in den ‚Mobile Access' Container auf der Submap des Anwenders kopiert wurden.

Hierarchische Suche kann nur dann ausgewählt werden, wenn ‚Benutzersicht' aktiviert wurde. Ist sie ausgewählt, wird in den Objekt-Bäumen unterhalb des ‚Mobile Access' Containers eine Tiefensuche ausgeführt. Ist sie nicht ausgewählt, beschränkt sich die Suche auf die unmittelbaren Kind-Objekte des ‚Mobile Access' Containers.

28.4.6.2 Knoten-Browser

Der **Knoten-Browser** (siehe *Bild 43*) zeigt alle Knoten an, die den ausgewählten Such-Kriterien entsprechen (siehe *Abschnitt 28.4.6.1, „Knoten-Suche"*). Wurde keine Suche spezifiziert, werden alle Knoten angezeigt. Die Schaltfläche **Suchen** in der linken oberen Ecke öffnet die Knoten-Suche-Sicht.

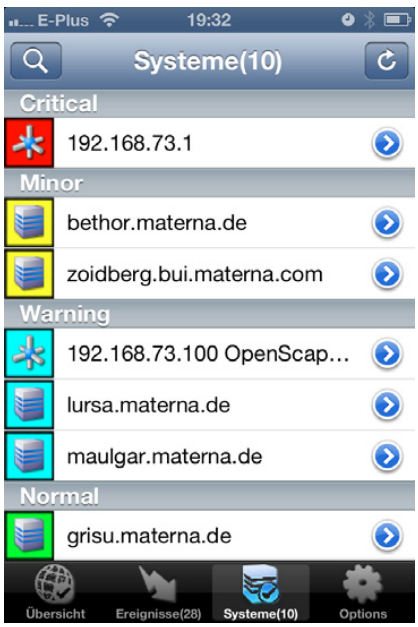


Bild 43 Knoten-Browser

Wird ein Knoten gedrückt, öffnet sich die Objekt-Detailansicht für den aktuellen IP-Knoten (siehe *Abschnitt 28.4.6.4, „Objekt-Details"*).

Wird die **Pfeil-Schaltfläche** auf der rechten Seite des Knotens ausgewählt, öffnet sich eine Objekt-Liste (siehe *Abschnitt 28.4.6.3, „Objekt-Browser"*), welche die Objekte enthält, die sich auf der Submap des IP-Knotens befinden.

28.4.6.3 Objekt-Browser

Der **Objekt-Browser** enthält die Objekte einer ausgewählten Submap.

Besitzt ein Objekt Kind-Objekte, so kann der Pfeil-Schaltfläche auf der rechten Seite des Objektes gedrückt werden, um einen Objekt-Browser zu öffnen. Der Browser enthält die Kind-Objekte des ausgewählten Objektes.

Die Schaltfläche **Zurück** in der oberen linken Ecke des Objekt-Browsers öffnet die vorherige Sicht (im Allgemeinen den Objekt-Browser mit den Objekten der Submap des Eltern-Objektes).

Diese beiden letztgenannten Funktionen erlauben die Navigation durch den Objekt-Baum des OpenScape FM.

Das Drücken eines Objektes öffnet den Objekt-Detail-Browser (siehe *Abschnitt 28.4.6.4, „Objekt-Details“*) für das ausgewählte Objekt.

28.4.6.4 Objekt-Details

Der Objekt-Details-Dialog öffnet sich, wenn ein IP-Knoten im Knoten-Browser oder ein Objekt im Objekt-Browser gedrückt wird. Der Dialog zeigt detaillierte Informationen über das ausgewählte Objekt an. Die angezeigte Information kann sich in Abhängigkeit vom Typ des ausgewählten Objektes unterscheiden.

28.4.7 Optionen

Der **Optionen** Tab kann verwendet werden, um sich abzumelden, oder um die gespeicherten HTTPS-Zertifikate anzuzeigen oder zu löschen.

29 String-Formatierungssprache

Die String-Formatierungssprache kann in unterschiedlichsten Plugins verwendet werden, um Ausgaben flexibel in Bezug auf die Eingabe-Variablen zu generieren.

Dieses Kapitel beschreibt die einzelnen Strukturen dieser Sprache im Detail.

29.1 Die Sprache in BNF Notation:

29.1.1 Tokens:

```
<DEFAULT> TOKEN: {
<ESCAPE: "\\" ["{","}","$",",","\\","n","t"]>
| <NESCAPE: "\\" ~["{","}","$",",","\\","n","t"]>
| <TEXT: (~["{","}","$",",","\\"])+>
}
```

29.1.2 NON-Terminals

Tabelle 6 NON-Terminals

Input	:==	StartPhrase <EOF>
Escape	:==	(<ESCAPE>)
Text	:==	(<TEXT> | <NESCAPE>)
Word	:==	Escape | Text
Get	:==	(("$get{" \| "${") Phrase "}")
GSet	:==	"$gset{" Phrase "," Phrase "}"
Set	:==	"$set{" Phrase ("," Phrase |) "}"
If	:==	"$if{" Phrase "," Phrase ("," Phrase)? "}"
Switch	:==	"$switch{" Phrase ("," ("{" Phrase "," Phrase "}"))* "}"
Match	:==	"$match{" Phrase "," Phrase "," Phrase "}"
Split	:==	"$split{" Phrase "," Phrase "," Phrase "}"
Length	:==	"$length{" Phrase "}"
SubString	:==	"$substring{" Phrase "," Phrase ("," Phrase)? "}"
IndexOf	:==	"$indexof{" Phrase "," Phrase ("," Phrase)? "}"
LastIndexOf	:==	"$lastindexof{" Phrase "," Phrase ("," Phrase)? "}"
ReplaceFirst	:==	"$replacefirst{" Phrase "," Phrase "," Phrase "}"
ReplaceAll	:==	"$replaceall{" Phrase "," Phrase "," Phrase "}"
Range	:==	"$range{" Phrase "," Phrase ("," Phrase)? "}"
Array	:==	"$array{" Phrase ("," Phrase)* "}"
Add	:==	("$+{" \| "$add{") Phrase "," Phrase "}"
Sub	:==	("$-{" \| "$sub{") Phrase "," Phrase "}"
Mul	:==	("$*{" \| "$mul{") Phrase "," Phrase "}"
Div	:==	("$/{" \| "$div{") Phrase "," Phrase "}"
Mod	:==	("$%{" \| "$mod{") Phrase "," Phrase "}"
Math	:==	(Add | Sub | Mul | Div | Mod)

Tabelle 6 NON-Terminals

Bool	:==	`( Or | And | Matches | NotMatches | Equals | NotEquals | Less | LessEquals | Greater | GreaterEquals | Not )`
Matches	:==	`( "$~{" ) Phrase "," Phrase "}"`
NotMatches	:==	`( "$!~{" ) Phrase "," Phrase "}"`
Or	:==	`( "$||{" ) Phrase "," Phrase "}"`
And	:==	`( "$&&{" ) Phrase "," Phrase "}"`
Equals	:==	`( "$=={" ) Phrase "," Phrase "}"`
NotEquals	:==	`( "$!={" ) Phrase "," Phrase "}"`
Less	:==	`( "$<{" ) Phrase "," Phrase "}"`
LessEquals	:==	`( "$<={" ) Phrase "," Phrase "}"`
Greater	:==	`( "$>{" ) Phrase "," Phrase "}"`
GreaterEquals	:==	`( "$>={" ) Phrase "," Phrase "}"`
Not	:==	`( "$!{" ) Phrase "}"`
FormatDate	:==	`"$formatdate{" Phrase "," Phrase ( "," Phrase ( "," Phrase)? )? "}"`
Parsedate	:==	`"$parsedate{" Phrase "," Phrase ( "," Phrase ( "," Phrase )? )? "}"`
LogError	:==	`"$logError{" Phrase ( "," Phrase )* "}"`
LogWarn	:==	`"$logWarn{" Phrase ( "," Phrase )* "}"`
LogInfo	:==	`"$logInfo{" Phrase ( "," Phrase )* "}"`
StartPhrase	:==	`( Word | Get | Set | GSet | Script | Switch | If | Bool | Match | Split | Length | IndexOf | LastIndexOf | ReplaceFirst | ReplaceAll | Range | Array | SubString | Math | FormatDate | ParseDate | "," | "$" )*`
Phrase	:==	`( Word | Get | Set | GSet | Script | Switch | If | Bool | Match | Split | Length | IndexOf | LastIndexOf | ReplaceFirst | ReplaceAll | Range | Array | SubString | Math | FormatDate | ParseDate | "{" Phrase "}" )+`

29.2 Die Funktionalität der unterschiedlichen Kommandos

29.2.1 Das Get Kommando

`$get{ Phrase`$_{in}$` } or ${ Phrase`$_{in}$` }`

Gibt den Wert der Variablen zurück, deren Name dem Rückgabewert von `Phase`$_{in}$ entspricht.

29.2.2 Das GSet Kommando

$gset{ $Phrase_{var}$, $Phrase_{value}$ }

Das GSet Kommando setzt global den Wert der Variablen mit dem durch $Phrase_{var}$ definierten Namen auf den durch $Phrase_{value}$ generierten Wert.

29.2.3 Das Set Kommando

$set{ $Phrase_{var}$, $Phrase_{value}$ }

Das Set Kommando arbeitet wie das zuvor beschriebene GSet Kommando. Allerdings wird die Variable nur lokal definiert, um in einem eingeschlossenen Unter-Kommando (durch {}) eingeschlossen) verwendet zu werden.

Das Kommando kann auch ohne den zweiten Parameter verwendet werden:

$set{ $Phrase_{var}$ }

In diesem Fall wird die Variable mit dem durch $Phrase_{var}$ definierten Namen nicht auf einen Wert gesetzt, sondern sie wird entfernt.

29.2.4 Das Switch Kommando

$switch{ $Phrase_{in}$ <,{ $Phrase_{1A}$, $Phrase_{1B}$ } >
<, { $Phrase_{2A}$, $Phrase_{2B}$ } >
...
< , { $Phrase_{NA}$, $Phrase_{NB}$ } > }

Das Switch Kommando liefert $Phrase_{xB}$ zurück, falls die Eingabe $Phrase_{in}$ dem regulären Ausdruck $Phrase_{xA}$ entspricht (x ist dabei zwischen 1 und N).

Zum Beispiel liefert die Phrase

```
$switch{${severity},{Warning,Medium},{Minor,Medium},
{Major,Medium},{Critical,High},{.*,Low}}
```

das Ergebnis ’Medium’ falls die Variable ’severity’ den Wert ’Warning’, ’Minor’ oder ’Major’ enthält. Sie liefert das Ergebnis ’High’ falls die Variable ’severity’ den Wert ’Critical’ enthält. Sie liefert den Wert ’Low’ in allen anderen Fällen.

29.2.5 Das Match Kommando

$match{ $Phrase_{in}$, $Phrase_{expr}$, $Phrase_{array}$ }

Das Kommando parst das Ergebnis von $Phrase_{in}$ mit einem Perl ähnlichen regulären Ausdruck, der sich durch $Phrase_{expr}$ ergibt. Der reguläre Ausdruck darf eine beliebige Anzahl von Unter-Ausdrücken, die in runde Klammern eingeschlossen sind, enthalten. Jeder Unter-Ausdruck, der erfolgreich geparst werden kann, kopiert seinen Inhalt in ein neues Mitglied des Arrays mit dem Namen, der durch $Phrase_{array}$ festgelegt wird.

Z.B. liefert das Kommando

```
$match{ abcdefghijk , .*(c).*(f.*i).* , testarray }
```

das Array 'testarray', das aus den zwei Einträgen 'c' und 'fghi' besteht. Soll auf den Eintrag 'c' zugegriffen werden, muss `testarray[0]` verwendet werden.

29.2.6 Das Split Kommando

$split{ Phrase_{in} , Phrase_{splitter} , Phrase_{array} }$

Dieses Kommando durchsucht den durch $Phrase_{in}$ generierten String nach Vorkommen des Substrings, der durch $Phrase_{splitter}$ festgelegt wird. Diese Vorkommen werden aus $Phrase_{in}$ entfernt, und die verbleibenden Segmente werden in ein Array gefüllt, dessen Name sich durch $Phrase_{array}$ ergibt.

Das Kommando

```
$split{ abxcdxef , x , testarray }
```

generiert z.B. das Array 'testarray', das aus den drei Einträgen 'ab', 'cd' und 'ef' besteht. Um auf den Eintrag 'ab'b

von testarray zuzugreifen, muss `testarray[0]` verwendet werden.

29.2.7 Das Length Kommando

$length{ Phrase_{in} }$

Liefert die Länge in Zeichen der Ausgabe von $Phrase_{in}$.

29.2.8 Das Substring Kommando

$substring{ Phrase_{in} , Phrase_{start} }$

$substring{ Phrase_{in} , Phrase_{start} , Phrase_{end} }$

Dieses Kommando liefert einen Teilstring, der durch $Phrase_{in}$ generiert wird, zurück.

Im ersten Fall besteht der zurück gelieferte Teil aus dem Rest des Strings beginnend mit der Position $Phrase_{start}$ (wobei $Phrase_{start}$ einen Integer-Wert liefern muss).

Im zweiten Fall besteht der zurück gelieferte Teil aus dem Substring beginnend an Position $Phrase_{start}$ und endend an Position $Phrase_{end}$ (wobei $Phrase_{start}$ und $Phrase_{end}$ Integer-Werte liefern müssen.

29.2.9 Das Indexof Kommando

$indexof{ $Phrase_{in}$, $Phrase_{match}$ }

$indexof{ $Phrase_{in}$, $Phrase_{match}$, $Phrase_{pos}$ }

Im ersten Fall liefert das Kommando die Position des ersten Auftretens des Ergebnisses von $Phrase_{match}$ im Ergebnis von $Phrase_{match}$.

Im zweiten Fall beginnt die Substring-Suche an der Position, die durch $Phrase_{pos}$ definiert wird (dies muss ein Integer-Wert sein). Mögliche Treffer, die weiter links auftreten werden ignoriert.

29.2.10 Das Lastindexof Kommando

$lastindexof{ $Phrase_{in}$, $Phrase_{match}$ }

$lastindexof{ $Phrase_{in}$, $Phrase_{match}$, $Phrase_{pos}$ }

Entspricht dem Indexof Kommando. In diesem Fall werden die am weitesten rechts gefundenen Treffer ausgewertet.

29.2.11 Das Replaceall Kommando

$replaceall{ $Phrase_{in}$, $Phrase_{old}$, $Phrase_{new}$ }

Dieses Kommando liefert den String, der durch $Phrase_{in}$ bestimmt wird, und in dem alle Vorkommen des Teilstrings $Phrase_{old}$ durch den durch $Phrase_{new}$ generierten String ersetzt wurden.

29.2.12 Das Replacefirst Kommando

$replacefirst{ $Phrase_{in}$, $Phrase_{old}$, $Phrase_{new}$ }

Entspricht dem Replaceall Kommando. Jedoch wird in diesem Fall nur das erste (am weitesten links befindliche) Auftreten von $Phrase_{old}$ durch $Phrase_{new}$ ersetzt. Weitere Vorkommen werden unverändert übernommen.

29.2.13 Das Range Kommando

"$range{" $Phrase_{StartValue}$ "," $Phrase_{EndValue}$ ("," $Phrase_{Increment}$)? "}"

Dieses Kommando liefert eine Sequenz von Werten indem es eine klassische For-Schleife simuliert.

Die gelieferten Werte beginnen mit $Phrase_{StartValue}$ und es wird so lange $Phrase_{Increment}$ addiert bis $Phrase_{EndValue}$ mit dem nächsten Schritt überschritten würde. Wird $Phrase_{Increment}$ nicht angegeben, so wird es auf 1 gesetzt.

Wichtiger Hinweis:
Das Kommando überprüft nicht, ob durch die Definition eine sehr große oder sogar unendliche Sequenz entsteht.

Beispiel:

`$range{0,10,2}`

Diese Kommando liefert {0, 2, 4, 6, 8, 10}. Also die Sequenz, welche die Zahlen von 0 bis 10 in 2er-Schritten enthält.

29.2.14 Das Array Kommando

`"$array{" Phrase`$_1$` ( "," Phrase`$_n$` )* "}"`

Dieses Kommando liefert die aufgeführten Werte als Sequenz. Es kann dabei eine beliebige Anzahl von Werten angegeben werden.

Beispiel:

`$array{a,1,b,2}`

Erzeugt wird eine Sequenz aus `"a"`, `"1"`, `"b"` und `"2"`.

29.2.15 Die Math Kommandos

`(Add | Sub | Mul | Div | Mod )`

Die Math Kommandos liefern den Wert einer mathematischen Operation.

29.2.15.1 Add Operation

Die Add Operation addiert zwei gegebene Parameter.

Beispiel:

`$+{2,3}` oder `$add{2,3}` ergeben den Wert 5

29.2.15.2 Sub Operation

Die Sub Operation subtrahiert zwei gegebene Parameter.

Beispiel:

`$-{5,3}` oder `$sub{5,3}` ergeben der Wert 2.

29.2.15.3 Mul Operation

Die Mul Operation multipliziert zwei gegebene Parameter.

Beispiel:

`$*{2,3}` oder `$mul{2,3}` liefert den Wert 6.

29.2.15.4 Div Operation

Die Div Operation dividiert zwei gegebene Parameter.

Beispiel:

`$/{6,3}` oder `$mul{6,3}` liefert den Wert 2.

29.2.15.5 Mod Operation

Die Mod Operation liefert den Rest der Division zweier gegebener Parameter.

Beispiel:

`$%{7,3}` oder `$mod{7,3}` liefert den Wert 1.

29.2.16 Das If Kommando

`"$if{" Phrase`$_{Bool}$ `"," Phrase`$_{if}$ `( "," Phrase`$_{else}$ `)? "}"`

Dieses Kommando kann verwendet werden, um Entscheidungen zu treffen. Der erste Parameter ist ein boolescher Ausdruck. Ist dieser wahr, wird der zweite Parameter ausgeführt. Ist er falsch, wird der dritte Parameter ausgeführt, sofern ein dritter Parameter angegeben wurde.

Beispiel:

`$if{$~{${severity},Critical},Important,Unimportant}`

Falls die Severity des Ereignisses Critical ist, wird die Ausgabe 'Important' geliefert. Ansonsten ist die Ausgabe „Unimportant“.

29.2.17 Die Bool Kommandos

`( Or | And | Matches | NotMatches | Equals | NotEquals | Less | LessEquals | Greater | GreaterEquals | Not )`

Die Bool Kommandos können verwendet werden, um boolsche Operation auszuführen. Die folgenden Operationen sind möglich:

29.2.17.1 Or Operation

`( "$||{" ) Phrase`$_1$ `"," Phrase`$_2$ `"}"`

Diese Operation liefert true, falls mindestens einer der beiden Ausdrücke wahr liefert, false ansonsten.

29.2.17.2 And Operation

`( "$&&{" ) Phrase`$_1$ `"," Phrase`$_2$`"}"`

Diese Operation liefert true, falls beide Ausdrücke wahr liefern, false ansonsten.

29.2.17.3 Matches Operation

`( "$~{" ) Phrase`$_{string}$ `"," Phrase`$_{reg}$ `"}"`

Diese Operation vergleicht, ob der erste Parameter dem gegebenen regulären Ausdruck in Phrase$_{reg}$ entspricht. Dabei ist die Operation „greedy“. Dies bedeutet, dass der Vergleich mit den kompletten Ausdrücken durchgeführt wird.

Hinweis:
Um reguläre Ausdrücke auszuwerten, wird die Java-Klasse `jave.util.reges.Pattern` verwendet. Da reguläre Ausdrücke ein mächtiges Instrument darstellen, kann hier keine vollständige Erklärung geliefert werden. Mehr dazu findet sich in der entsprechenden Java-Dokumentation.

Beispiel:
`$~{"It is Critical","Critical"}` gibt false zurück.

`$~{"It is Critical",".*Critical.*"}` gibt true zurück.

29.2.17.4 NotMatches Operation

`( "$!~{" ) Phrase "," Phrase "}"`

Diese Operation vergleicht, ob der erste Parameter dem gegebenen regulären Ausdruck in Phrase$_{reg}$ nicht entspricht. Dabei ist die Operation „greedy“. Dies bedeutet, dass der Vergleich mit den kompletten Ausdrücken durchgeführt wird.

Beispiel:
`$!~{"It is Critical","Critical"}` gibt true zurück.

`$!~{"It is Critical",".*Critical.*"}` gibt false zurück.

29.2.17.5 Equals Operation

`( "$=={" ) Phrase "," Phrase "}"`

Diese Operation vergleicht, ob die gegebenen Parameter gleich sind. In diesem Fall wird true zurück gegeben, false ansonsten.

29.2.17.6 NotEquals Operation

```
( "$!={" ) Phrase "," Phrase "}"
```

Diese Operation vergleicht, ob die gegebenen Parameter verschieden sind. In diesem Fall wird true zurück gegeben, false ansonsten.

29.2.17.7 Less Operation

```
( "$<{" ) Phrase "," Phrase "}"
```

Diese Operation überprüft, ob der erste Ausdruck kleiner als der Zweite ist.

29.2.17.8 LessEquals Operation

```
( "$<={" ) Phrase "," Phrase "}"
```

Diese Operation überprüft, ob der erste Ausdruck kleiner oder gleich dem zweiten Ausdruck ist.

29.2.18 Das FormatDate Kommando

```
$formatdate{<date in milli seconds>, <format of the output date>[, locale, [country]]
```

Das FormatDate Kommando gibt ein Datum zurück. Die folgende Tabelle enthält die möglichen Formate. .

Tabelle 7 Datums- und Zeit-Muster in der Java Classe SimpleDateFormat

Symbol	Datums- oder Zeit-Komponente	Präsentation	Beispiele
G	Era Designator	Text	AD
y	Jahr	Jahr	1996; 96
M	Monat des Jahres	Monat	July; Jul; 07
w	Woche des Jahres	Zahl	27
W	Woche des Monats	Zahl	2
D	Tag des Jahres	Zahl	189
d	Tag des Monats	Zahl	10
F	Tag der Woche im Monat	Zahl	2

Tabelle 7 Datums- und Zeit-Muster in der Java Classe SimpleDateFormat

Symbol	Datums- oder Zeit-Komponente	Präsentation	Beispiele
E	Tag der Woche	Text	Tuesday; Tue
a	AM/PM Marker	Text	PM
H	Stunde des Tages (0-23)	Zahl	0
k	Stunde des Tages (1-24)	Zahl	24
K	Stunde in AM/PM (0-11)	Zahl	0
h	Stunde in AM/PM (1-12)	Zahl	12
m	Minute der Stunde	Zahl	30
s	Sekunde der Minute	Zahl	55
S	Milli-Sekunde	Zahl	978
z	Zeitzone	Allgemeine Zeitzone	Pacific Standard Time; PST; GMT-08:00
Z	Zeitzone	RFC 822 Zeitzone	-0800

Beispiele:

`$formatdate{1258626787000,dd.MM.yyyy}` liefert ein Datum wie `19.11.2009`.

`$formatdate{1258626787000,dd. MMMM yyyy,en}` liefert ein Datum wie `19. November 2009`.

29.2.19 Das ParseDate Kommando

`$parsedate{{<date>, <format of the given date>[, locale, [country]]`

Das ParseDate Kommando parst ein gegebenes Datum und liefert das Datum als die Zahl der Milli-Sekunden seit Mitternacht des 1.1.1970 zurück. Der Format-Parameter beschreibt das Format des gegebenen Datums. Siehe Tabelle 7 auf Seite 167 für mögliche Format-Optionen.

Beispiele:

`$parsedate{19.11.2009,dd.MM.yyyy}` liefert ein Datum wie z.B. `1258626787000`.

`$parsedate{19. November 2009,dd. MMMM yyyy,en}` liefert ein Datum wie z.B. `1258626787000` aus einem anderen gegebenen Datumsformat.

29.2.20 Das LogError LogWarn und LogInfo Kommando

```
$_logError{ Phrase1 <, Phrase2>
                     ...
                    <, PhraseN> }

$_logWarn{ Phrase1 <, Phrase2>
                     ...
                    <, PhraseN> }

$_logInfo{ Phrase1 <, Phrase2>
                     ...
                    <, PhraseN> }
```

Die _logError-, _logWarn- und _logInfo-Kommandos können verwendet werden, um der Logdatei `server.log` Informationen hinzuzufügen. Abhängig vom verwendeten Kommando werden die Komma separierten Phrasen als Fehler, Warnung oder Information hinzugefügt.

A Die Rechte des Basis-Moduls

Die Zugriffsrechte des Basis-Moduls sind in die allgemeine Rechte-Verwaltung eingegliedert (*siehe Kapitel 15, „Funktionen der einzelnen Rechte“*).

Die Beschreibung der einzelnen Rechte erfolgt in Form eines Tool-Tipps für das jeweils zugehörige Rechte-Symbol (Baum oder Submap).

Die Namen der Rechte des Basis-Moduls beginnen mit der Kennzeichnung *Base*.

B Anforderungen an die Hardware- und Software-Umgebung

Die Hardware- und Software-Voraussetzungen für OpenScape FM Server und Clients finden sich in den Unify Release-Nodes für OpenScape FM.

Virtualisierung:
Es ist erlaubt das OpenScape FM auf einem virtuellen System zu installieren, das auf einem VMware vCenter läuft.

Wichtiger Hinweis:
Der OpenScape FM Support deckt keine Probleme ab, die sich aus der Interaktion des Gast-Betriebssystems und dem hypervisor ergeben, oder die einer der beiden Komponenten zugeordnet werden können.
Andere Probleme, die in der Konstellation eines OpenScape FM auftreten, das auf einem virtuellen System in einem VMware vCenter läuft, werden wie üblich über den normalen Support-Prozess behandelt.

C Installationsprozess

Dieser Teil des Handbuches beschreibt die Installation des OpenScape FM. Für den Betrieb benötigte zusätzliche Software wie Betriebssystem oder Datenbank werden als vorhanden und installiert voraus gesetzt.

Eine detaillierte Beschreibung der Installation findet sich in der separaten *Installationsanleitung* der Unify Software and Solutions GmbH & Co. KG.

Während der Installation kann einer von drei Installationsumfängen ausgewählt werden:

- Die vollständige OpenScape FM Installation ist der Normalfall und installiert alle Komponenten.
- OpenScape Business / HiPath 3000 installiert nur das System Management und das OpenScape Business / HiPath 3000 Plugin.

C.1 Einsatz von MySQL

Kommt für OpenScape FM das Performance Management Plugin in Verbindung mit MySQL zum Einsatz, sollten die folgenden Schritte berücksichtigt werden:

1. **Installation des Datenbank-Treibers** (dieser Punkt kann übersprungen werden, falls **MySQL 5.5** verwendet wird)

   Der in der OpenScape FM Installation enthaltene Datenbank-Treiber (JDBC Treiber von MariaDB) unterstützt ausschließlich MySQL 5.5. Wird eine andere MySQL Version verwendet, muss der entsprechende MySQL Treiber manuell installiert werden. Dies kann wie folgt geschehen:

   a) Öffnen der Download-Seite `http://dev.mysql.com/downloads`

   b) Auswahl des Links `MySQL Connectors`

   c) Auswahl des Links `Connector/J`

   d) Im Auswahlmenü **Select Platform** dem Eintrag `Platform Independent` auswählen

   e) Download des Archivs (Verfügbar als `zip` oder `tar`)

   f) Entpacken des Archivs und Auffinden des Treibers. Sein Name hat etwa die folgende Form: `mysql-connector-java-X.X.XX-bin.jar`. Dabei steht `X.X.XX` für die Nummer der Version

   g) Stoppen des OpenScape FM Server-Prozesses

   h) Kopieren der Treiber-Datei `mysql-connector-java-X.X.XX-bin.jar` in das Verzeichnis `<OPENSCAPE FM INSTALL>/server/lib/external`

   i) **Löschen** der Datei `<OPENSCAPE FM INSTALL>/server/lib/external/mariadb-java-client.jar`. **Dieser Schritt ist wichtig**, da andernfalls die Datenbank-Verbindung eventuell nicht korrekt arbeitet.

   j) Starten des OpenScape FM Server-Prozesses

2. Vorbereitung der Datenbank

Das Performance Management Plugin benötigt eine zuvor definierte Datenbank. Um eine Datenbank in MySQL einzurichten, können die folgenden Schritte ausgeführt werden:

a) Verbinden mit dem lokalen MySQL Datenbak-Server durch den Aufruf des `mysql` Kommandozeilen-Tools. Wird das Tool nicht gefunden, wurde evtl. das `mysql-client` Paket nicht installiert. Der Client fragt nach dem Passwort für "`root`" falls er wie unten stehend aufgerufen wird. Dabei handelt es sich **nicht** um den Unix-root Anwender, sondern um den MySQL Datenbank-Administrator. Das Passwort muss bekannt sein. Gewöhnlich wird es während der Installation des MySQL Servers festgelegt.

Kommando: `mysql -u root -p`

b) Erzeugung einer Datenbank mit einem frei gewählten Namen. Der gleiche Name muss in der Oberfläche des OpenScape FM über den Hauptmenüeintrag **Erweiterungen->Performance Management->Datenbankverbindung auswählen oder erzeugen** konfiguriert werden.

Kommando: `create database pm_database;`

c) Verlassen des Kommandozeilen-Tools

Kommando: `exit;`

C.2 Linux

Einzelheiten zu den Anforderungen an das Betriebssystem und die JVM können *Anhang B, „Anforderungen an die Hardware- und Software-Umgebung“* entnommen werden.

Um OpenScape FM unter Linux zu installieren, muss das Skript `openscapefm.bin` vom Installationsmedium ausgeführt werden:

```
sh /setup_osfm.sh
```

Der Installationsprozess wird über eine Befehlszeilenschnittstelle geleitet. Hinsichtlich der durchzuführenden Schritte ist diese Schnittstelle sehr stark an den Windows-Client angelehnt. Daher werden wir die Einzelheiten der Installation anhand des Prozesses auf einem Windows-System beschreiben.

Das Standardinstallationsverzeichnis auf Linux-Systemen ist `/opt/OpenScapeFM` .

C.3 Windows

Die Installation wird mit Aufruf der Datei `setup_osfm.exe` auf dem Installationsmedium angestoßen. Dies startet den Installer, welcher die Installation durchführt.

Der Installer sucht zunächst nach installierten virtuellen Maschinen für Java(TM) und benutzt die erforderliche Version. Ist keine virtuelle Maschine vorhanden, wird die Installation von OpenScape FM abgebrochen.

Es erscheint eine Begrüßungsnachricht, die Installationsdateien werden extrahiert und die graphische Installationsoberfläche wird angezeigt, über welche die Installation konfiguriert werden kann. Über die Schaltfläche **Weiter** kann jeweils zum nächsten Schritt fortgefahren werden. Die Schaltfläche **Abbrechen** kann jederzeit verwendet werden, um die die Installation abzubrechen.

Um die Konfiguration beginnen zu können, müssen zunächst die Lizenzvereinbarungen akzeptiert werden.

Ist dies geschehen, kann ausgewählt werden, welche Komponenten installiert werden sollen.

Es kann entweder eine vollständige OpenScape FM Installation oder eine OpenScape Business Installation durchgeführt werden.

Im folgenden Fenster kann das Installationsverzeichnis festgelegt werden. Vom System wird hier bei einer ersten Installation das Standard-Installationsverzeichnis `C:\Program Files\OpenScapeFM` vorgeschlagen. Wurde vorher bereits eine Installation durchgeführt, so wird das Verzeichnis der durchgeführten Installation angezeigt. Über die Schaltfläche **Auswählen...** kann hier bei Bedarf auch ein beliebiges anderes Verzeichnis ausgewählt werden.

Bei der Installation wird abgefragt auf welchem System/Port der Customer License Agent läuft. Beim ersten Verbindungsaufbau, falls noch keine Produktlizenz eingespielt wurde, wird eine Demo-Lizenz eingerichtet, die die Benutzung der Software für 90 Tage erlaubt. Lizenzen müssen über die Mechanismen des CLA eingespielt werden. Der Menüpunkt **Server->Administration->Lizenz Manager->Lizenzdatei laden...** dient nur dazu Lizenzen für das HiPath QM und UM einzuspielen, die weiterhin vom OpenScape FM verwaltet werden.

Nach einer Bestätigung des Installationsverzeichnisses wird die eigentliche Installation angestoßen.

Soll der OpenScape FM andere Hosts über WMI überwachen, kann bei der Installation ein Konto für diese Funktion eingetragen werden. Dieses Konto muss der lokalen Gruppe *Administrator* angehören und die Windows-Sicherheitsrichtlinie '*Anmeldung als Dienst*' haben. Für dieses Konto müssen die **Domäne**, der **Dienst Benutzer** und das **Passwort** angegeben werden.

In dem Fenster wird nun der Fortschritt der Installation angezeigt, bzw. diese, falls erfolgreich, mit einem grünen Haken-Symbol bestätigt.

Wurden der OpenScape FM Server bzw. das Event Gateway installiert, werden diese automatisch durch den Dienst OpenScape FM Startup Service bzw. den Dienst Event Gateway gestartet.

Über einen Web-Browser oder einen eigenständigen Client kann jetzt eine Verbindung zum Server hergestellt werden, indem die URL `https://localhost:3043` aufgerufen wird.

C.4 Installationsparameter

Die in diesem Abschnitt beschriebenen Parameter können dem Installationsaufruf hinzugefügt werden, um die Installation zu modifizieren. Die Parameter gelten sowohl für die Linux- wie auch die Windows-Installation.

- `-console`
  Dieser Parameter bewirkt, dass die Installation nicht mit der Installationsoberfläche durchgeführt wird, sondern innerhalb eines Konsolen-Fensters. Es können die gleichen Einstellungen vorgenommen werden, wie in der graphischen Oberfläche.

- `-silent`
  Dieser Parameter bewirkt, dass die Installation vollständig im Verborgenen durchgeführt wird. D.h. es wird während der Installation weder die Installationsoberfläche noch eine Konsole geöffnet. Die Installation erfolgt in das Installationsverzeichnis, das für das jeweilige Betriebssystem vorgesehen ist.
- `-Dnobackup=true`
  Die Installation wird ohne zuvoriges Backup der bestehenden OpenScape FM Installation durchgeführt.
- `-Dcreatebackup=true`
  Die Installation wird mit zuvorigem Backup der bestehenden OpenScape FM Installation durchgeführt.
- `-Dserver=true`
  Wird die Installation im Verborgenen ausgeführt, kann dieser Parameter verwendet werden, um eine vollständige Installation des OpenScape FM durchzuführen.
- `-Dserver_osbiz=true`
  Wird die Installation im Verborgenen ausgeführt, kann dieser Parameter verwendet werden, um die Installationsoption "OpenScape Business" auszuwählen.
- `-Dtarget.directory="<installation_dir>"`
  Dieser Parameter bewirkt, dass als Installationsverzeichnis der statt `<installation_dir>` angegebene Pfad verwendet wird. Ist bereits ein OpenScape FM installiert, wird dieser Parameter ignoriert und das vorhandene Installationsverzeichnis verwendet.

Ein mögliches Kommando wäre unter Linux z.B.:

```
sh setup_osfm.sh -Dtarget.directory=/opt/OpenScapeFM_Test -silent
```

C.5 Deinstallation

- Bei einem Linux-System kann dazu der folgende Befehl aufgerufen werden:
- `/<OpenScape FM installation directory>/uninstall.sh`
- Bei einem Windows-System kann OpenScape FM über den Eintrag “Software” in der Systemsteuerung deinstalliert werden. Nach Auswahl von “OpenScape FM” in der Applikationsliste muss lediglich die Schaltfläche “Hinzufügen/Entfernen” betätigt werden. Anschließend sind die Anweisungen im Dialogfeld zu befolgen.

Existiert zum Zeitpunkt der Deinstallation ein registriertes Tray Bar Symbol (siehe *Kapitel 9, „Anzeige von Tray Bar Symbolen“*), wird dieses nicht automatisch deinstalliert. Die Deinstallation des Symbols muss über die Auswahl der Menüeintrages **Deinstallieren...** aus dem Kontextmenü des Tray Bar Symbols manuell durchgeführt werden.

D Systemkonfiguration

D.1 Initialisierung von Plugins

Nach erfolgreich abgeschlossener Installation (siehe *Anhang C, „Installationsprozess“*) kann mit der Konfiguration des OpenScape FM fortgefahren werden.

Nachdem ein Client gestartet wurde (siehe *Abschnitt 4.2, „Starten des Clients“*) können die zusätzlich benötigten Plugins initialisiert werden. Dies geschieht durch die Auswahl der entsprechenden Einträge im Menü **Server->Plugins**.

Die Plugins IP Manager, System Management, Layer 2 Manager, Control Center, Performance Management und Enterprise MIB werden während der Installation automatisch initialisiert.

Wurde die OpenScape Business Version installiert, so sind nur die Plugins IP Manager, System Management und OpenScape Business verfügbar. Diese werden während des Installation automatisch initialisiert.

D.2 Ändern der Java Version

Das OpenScape FM ist in Java implementiert. Zum Laufen des OpenScape FM Server und Clients wird deshalb auf dem jeweiligen Rechner ein Java-Runtime-Environment (JRE) oder ein Java-Development-Kit (JDK) benötigt. Der Client wird als Java-Applet gestartet und verwendet das in den Systemeinstellungen definierte JRE. Der OpenScape FM Server verwendet das JRE/JDK, das bei der Installation ausgewählt wurde. Wird dieses JRE/JDK deinstalliert, wird beim Neustart des OpenScape FM Servers automatisch die aktuellste installierte JRE/JDK-Variante einer benötigten Version gesucht und verwendet. Soll eine andere JRE/JDK-Version vom OpenScape FM Server verwendet werden, so kann diese Version dem OpenScape FM Server auch manuell bekannt gemacht werden. Hierzu wird für Windows das Programm `ServerProperties.exe` und für Linux das Script `serverProperties` verwendet. Dieses Programm findet sich direkt im Installationsverzeichnis des OpenScape FM.

Die Variable JAVA_HOME sollte so definiert werden, dass sie auf das oberste Verzeichnis der JDK-Installation zeigt.

Windows:
Durch Doppelklick auf die `ServerProperties.exe` startet das Programm. Dieses bietet einen Datei-Browser über dem das neue JAVA-HOME Verzeichnis ausgewählt und über die Schaltfläche **Auswählen** zugeordnet werden kann. Über die Schaltfläche **Aktualisieren** wird der aktuelle Ordner aktualisiert. Die Schaltfläche **Beenden** schließt das Programm und ändert nichts an den Einstellungen.

Linux:
Durch Aufruf des Befehls `serverProperties` öffnet sich eine grafische Oberfläche äquivalent zu der unter Windows. Ist es nicht möglich eine grafische Oberfläche zu starten, wird ein Kommandozeilen-Tool gestartet. Hier muss der Pfad zum JAVA-HOME manuell eingegeben und mit der Eingabetaste bestätigt werden.

Nach dem Ändern des Pfades muss sowohl unter Windows als auch unter Linux der Startup Service neugestartet werden, um die gewünschte Konfiguration zu übernehmen.

E Lizenzierung

E.1 Allgemeines

Der Einsatz des OpenScape FM Desktop sowie der zugehörigen Plugins unterliegt gewissen Lizenzauflagen, die für die einzelnen Leistungsmerkmale verwaltet werden. Eine Lizenz ermöglicht die Nutzung eines bestimmten **Leistungsmerkmals** von OpenScape FM Desktop und Fault Management.

Im Anschluss an die OpenScape FM-Installation wird, bei der ersten Verbindung mit dem Customer License Agent, zunächst eine Demo-Lizenz für 90 Tage generiert. Diese Lizenz umfasst Einträge für den OpenScape FM DT sowie die vereinbarten Fault Management (FM)-Leistungsmerkmale. Nach Ablauf der Demo-Laufzeit werden die Fault Management Funktionen automatisch deaktiviert. Ein sinnvolles Arbeiten mit dem OpenScape FM ist nicht mehr möglich.

Es empfiehlt sich daher, rechtzeitig eine gültige OpenScape FM Desktop Lizenz zu installieren.

OpenScape FM-Plugins kombinieren unterschiedliche HiPath-Technologien (HiPath 3000/5000, HiPath 4000 etc.) zu OpenScape FM Desktop und Fault Management. Einige Plugins können wahlweise im Desktop- oder Fault Management-Modus betrieben werden. Wenn die Plugins im Desktop-Modus betrieben werden, können alle zugehörigen Systeme der Technologien erkannt und in Submaps angeordnet werden. Eingeschränkte Systeminformationen können abgefragt und anwendungsspezifische Funktionen aufgerufen werden. Im Fault Management-Modus unterstützen die Systeme zusätzlich eine grafische Fehlerstatus-Anzeige sowie den Zugriff auf verschiedene technologiespezifische Fehlerinformationen.

Die Lizenzierung von OpenScape Fault Management basiert auf Ports für bestimmte Technologieebenen (siehe Anhang E.4, „Technologieebenen und Ports“).

Ein OpenScape FM DT kann mehrere aktivierte Plugins enthalten, die entweder im FM-Modus oder im DT-Modus betrieben werden. Sollen die FM-tauglichen Plugins im FM-Modus betrieben werden, wird eine spezielle Lizenz benötigt (Leistungsmerkmal OpenScapeFaultManagement). Die Installation dieser Lizenz aktiviert die FM-Funktionen der Plugins.

Um die OpenScape FM Desktop und IP Manager Funktionen aktivieren zu können, muss eine OpenScape FM Desktop- und eine IP Manager-Lizenz aktiviert werden.

E.2 Lizenz-Management

Das von der Unify GmbH & Co. KG entwickelte License Management System (LM) ist ein Werkzeug um Lizenzen zu verwalten. Um konkurierende Lizenzierungs-Mechanismen zu vermeiden ist das OpenScape FM in der Lage, das LM zu verwenden. Dies macht es möglich, ein integriertes Lizenz-Management für das komplette OpenScape FM Umfeld zu verwenden. Im Folgenden wird davon ausgegangen, dass dem Leser das Lizenzierungs-Verfahren bekannt ist. Mehr dazu findet sich in der entsprechenden Dokumentation.

Das LM erlaubt die Verwendung von ’floating’ Lizenzen. Floating Lizenzen sind nicht an ein definiertes System gebunden. Sie begrenzen lediglich die Anzahl der OpenScape FM Server, die gleichzeitig laufen dürfen. Dies erlaubt den effizienten Einsatz weniger Lizenzen, da diese im Netzwerk geteilt werden können. Lizenz-Administratoren können festlegen, wer die lizenzierten Applikationen verwenden darf, und auf welchen Systemen sie verfügbar sein sollen.

Floating Lizenzen sind ausschließlich an den Customer License Agent (CLA) gebunden, der diese Linzenzen bereitstellt, jedoch nicht an den OpenScape FM Server, der eine Lizenz beantragt.

E.2.1 Lizensierungs-Voraussetzungen

Eine generierte Lizenz muss auf dem CLA initialisiert und aktiv sein. Ansonsten ist es dem MSMC FM nicht möglich Lizenzen anzufordern.

Das OpenScape FM arbeitet wie ein sogenannter Customer License Client (CLC). Das OpenScape FM fordert OpenScape FM spezifische Lizenzen (licenses features) vom CLS unter Verwendung des CLA an. Damit der OpenScape FM Server starten kann, müssen alle angeforderten OpenScape FM Lizenz-Features vorhanden sein.

Der OpenScape FM Server und der CLA können auf den gleichen oder auf unterschiedlichen Systemen betrieben werden.

E.2.2 Lizenz-Datei und -Konfiguration

Das OpenScape FM verwendet eine Lizenz-Datei, die die Verbindungsdaten zum Customer License Agent (CLA). enthält. Diese Daten werden bei der Installation erfasst, und die Datei wird automatisch erstellt.

Die Verbindungsdaten zum CLA können auch aus dem OpenScape FM heraus konfiguriert werden. Durch Auswahl des Hauptmenü-Eintrages **Server->Administration-> License Manager-> Customer License Agent (CLA)...** kann ein Konfigurations-Fenster geöffnet werden.

Innerhalb des Konfigurations-Fensters können die folgenden Daten konfiguriert werden:

CLA IP Adresse/Hostname:
Die IP Adresse oder der Hostname des CLA.

CLA Port:
Der Port, der für die Verbindung zum CLA verwendet werden soll. Der Standard-Port ist 61740.

Verbindungs Timeout (ms) und Anzahl Verbindungsversuche:
Wird eine Anforderung an den CLA gesendet, so muss dieser innerhalb der Timeout-Intervalls antworten. Ist dies nicht der Fall, wird eine erneute Anfrage gestartet. Wird die Anzahl der definierten Versuche erreicht, ohne dass eine Antwort erfolgt ist, wird ein Fehler generiert, der die ’verlorene Verbindung’ anzeigt.

Wird die Schaltfläche **OK** gedrückt, wird eine Lizenzdatei mit den eingegebenen Daten erzeugt. Diese Datei überschreibt die existierende OpenScape FM Lizenzdatei.

Wichtiger Hinweis:
Wird eine ungültige Verbindung eingegeben, oder ist keine Lizenz auf dem CLA verfügbar, so kann die Lizenz nicht mehr überprüft werden. In diesem Fall wird der OpenScape FM Server gestoppt.

E.2.3 Lizenz-Überprüfung

Alle lizenzierten Features werden automatisch einmal täglich überprüft. Außerdem können Lizenz-Überprüfungen manuell durch den Anwender angestoßen werden, indem die Lizenz-Informationen von Lizenz-Manager abgerufen werden. Die kann durch die Auswahl des Eintrages **Server->Administration->Lizenz Manager->Lizenz Informationen** aus dem Hauptmenü angestoßen werden.

Wird eine solche Überprüfung angestoßen, so werden die entsprechenden Features vom CLA abgefragt. Dies beinhaltet den aktuellen Status (verfügbar, nicht verfügbar, wartend), die verbleibende Zeit und die verbleibenden Anzahlen.

Die benötigte Anzahl an Lizenzen für ein Feature und für einen OpenScape FM Server ist stets 1. Ist eine größere Anzahl lizenziert, bedeutet dies, dass mehr als ein OpenScape FM Server gleichzeitig Lizenzen vom gleichen CLA zugewiesen bekommt.

Lizenz-Fehler werden im OpenScape FM abgebildet und im Ereignis-Browser dargestellt.

E.3 Installieren einer Lizenzdatei

Für fast alle Plugins und Funktionen erfolgt die Lizenzierung über den zuvor beschriebenen CLA,

Eine Ausnahme bilden das HiPath User Management (HPUM) und das HiPath Quality Management (HPQM). Diese werden über einen internen Lizenzierungs-Mechanismus aktiviert. Dazu muss eine passende Lizenzdatei geladen werden.

Es gibt zwei Verfahren für die Installation einer Lizenzdatei. Die Datei kann über den OpenScape FM Client (Anhang E.3.1, „Eingabe einer Lizenzdatei über den Client“) oder ein Standalone-Programm (Anhang E.3.2, „Eingabe einer Lizenzdatei über ein Standalone-Programm“) installiert werden.

E.3.1 Eingabe einer Lizenzdatei über den Client

Für dieses Verfahren muss zunächst der Client gestartet und ordnungsgemäß beim Desktop angemeldet werden. Dazu muss der OpenScape FM-Server laufen. Über die Menüposition **Server->Administration->License Manager->Lizenzdatei laden...** im Hauptmenü wird ein Dateiauswahl-Dialog gestartet, in dem die zu installierende Lizenzdatei gewählt werden kann.

Wichtiger Hinweis:
Ist das Lizenzmerkmal des OpenScape FM Desktop abgelaufen (Server wurde automatisch angehalten) und eine neue Lizenz soll integriert werden, muss das Standalone-Programm verwendet werden. Siehe auch Abschnitt E.3.2, „Eingabe einer Lizenzdatei über ein Standalone-Programm“.

Hinweis:
Kann nicht für das Laden von CLA-Lizenzen verwendet werden.

E.3.2 Eingabe einer Lizenzdatei über ein Standalone-Programm

Im Installationsverzeichnis des **MSMC FM** befindet sich das Programm `installLicenseFile.exe` (Windows) oder `installLicenseFile` (Unix). Dieses Programm ermöglicht die Auswahl einer Lizenzdatei und wickelt den weiteren Installationsverlauf ab. Eine gültige Lizenz muss installiert werden, wenn der OpenScape FM DT-Server nicht aktiv ist oder aufgrund einer fehlenden Lizenz nicht gestartet werden kann.

Hinweis:
Kann nicht für das Laden von CLA-Lizenzen verwendet werden.

E.3.3 Auswirkungen auf vorhandene Lizenzen

Wird eine neue Lizenz eingespielt, wird damit die alte Lizenz überschrieben.

E.4 Technologieebenen und Ports

Für das OpenScape Fault Management erfolgt die Lizenzierung anhand von Technologieebenen und Ports. Darüber hinaus stellt OpenScape FM die kumulative Portanzahl nach Technologietyp bereit.

Die Begriffe Technologietyp und Technologieebene werden wie folgt verwendet:

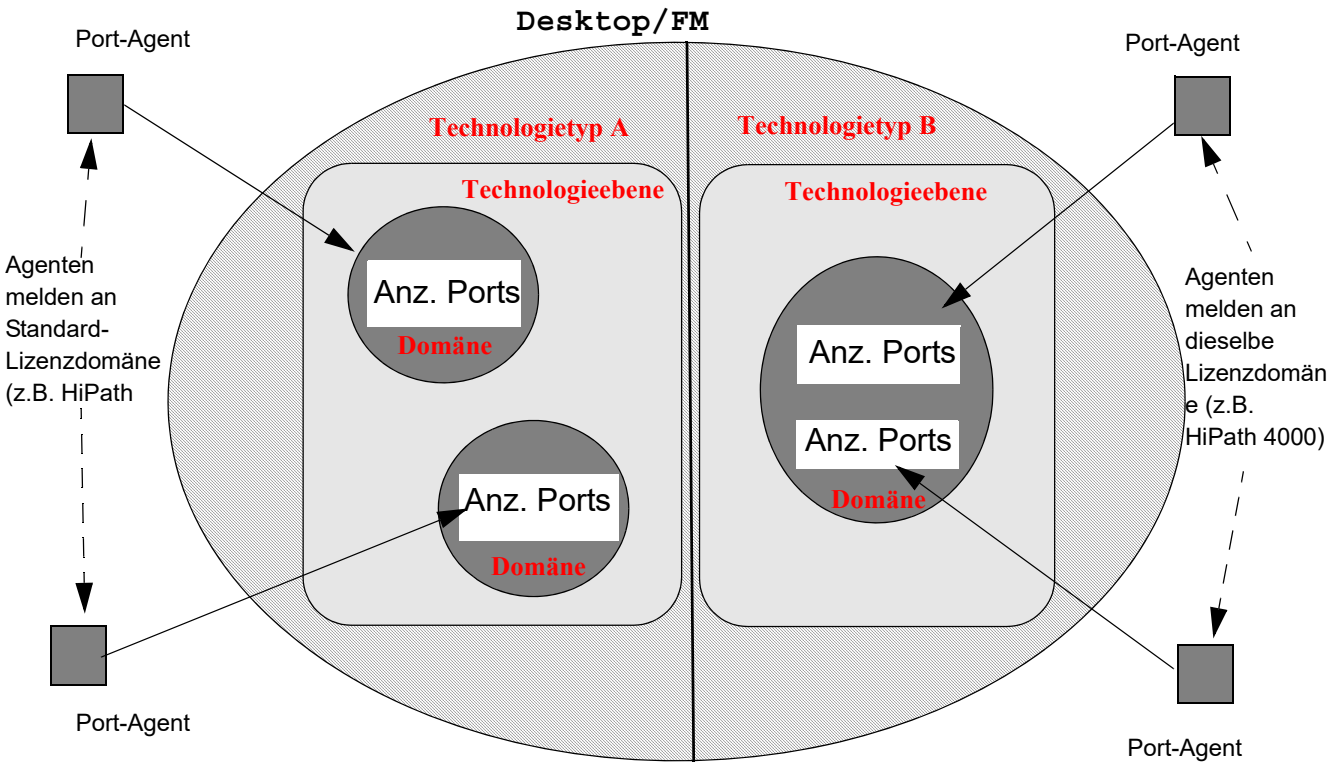
- **Technologietyp**
  ermöglicht die Unterscheidung zwischen Knoten/Geräten unterschiedlicher Systemfamilien, die per Desktop und Fault Management verwaltet werden. Beispiele für Systemfamilien sind HiPath 3000/5000 und HiPath 4000.
- **Technologieebene**
  ermöglicht die Gruppierung eines vordefinierten Bereichs von Versionen innerhalb eines bestimmten Technologietyps zu einer gemeinsamen Ebene/Gruppe. Eigenständige Versionen können auf diese Weise ein und derselben Technologieebene zugewiesen werden. Neue Versionen eines Technologietyps (z.B. HiPath 4000-Systeme) haben eine höhere Technolgoieebene als ältere Systeme (z.B. Hicom 300) desselben Technologietyps.
- **Port**
  Ein „physischer“ Port gehört zu einem bestimmten Technologietyp und einer Technologieebene dieses Typs. Es handelt sich hierbei um die Basiseinheit im Rahmen des Lizenzprüfungsprozesses.
- **Domäne**
  Wird verwendet, um eine doppelte Zahl von Ports in „Hot Standby“-Lösungen und in Assistant/Manager Szenarios zu vermeiden. Wenn zwei HiPath Port Agenten eine Portanzahl für die selbe Lizenzdomäne melden, wird diese nicht doppelt gezählt (siehe Abschnitt E.5, „Port-Manager“). Melden die Agenten eine

unterschiedliche Port-Anzahl, verwertet der Port Manager nur die höhere Port-Anzahl, die für eine bestimmte Lizenzdomäne gemeldet wird.

Der OpenScape FM DT enthält das Modul “Port Manager”, das für die Sammlung und Verarbeitung von Port-Lizenzdaten zuständig ist (siehe Anhang E.5, „Port-Manager“). Die Port-Lizenzdaten werden von den HiPath Port-Agenten abgerufen. Ein HiPath Port-Agent muss von jeder HiPath-Technologie unterstützt werden, die am Port-basierten Lizenzprozess beteiligt ist. Demzufolge müssen in HiPath-Umgebungen mit mehreren unterschiedlichen HiPath-Technologien die entsprechenden Port-Agenten aktiv sein, damit eine Lizenzprüfung möglich ist.
Auf der OpenScape FM DT-Bedienoberfläche wird ein HiPath Port-Agent durch ein Port Collector-Objekt dargestellt. Dieses Symbol befindet sich unterhalb des IP-Knotens, für den der zugehörige Port-Agent erkannt wurde. Ein Port Collector-Objekt unterstützt die Menüposition **Domain Ports**, über die ein Browser mit Informationen zu Domains, Ports, Technologie-Ebenen und Technologietypen geöffnet werden kann.

Jedes Plugin, das im FM-Modus arbeitet, prüft einmal täglich die aktuelle Anzahl der verwalteten Ports. Wird hierbei eine Überschreitung der lizenzierten Port-Anzahl erkannt, wird dies als Lizenzverletzung interpretiert. Eine solche Lizenzverletzung wird gemäß den in Anhang E.6, „Lizenz-Manager“ beschriebenen Regeln gehandhabt.

Das Konzept von OpenScape Desktop/FM im Hinblick auf Technologietypen, Technologieebenen, Ports und Domänen ist im folgdenden Bild dargestellt.



E.5 Port-Manager

Der HiPath Port-Manager fungiert als zentrale Informationsinstanz und Sammelstelle für alle Port-Lizenzdaten. Der Port-Manager erkennt die HiPath Port-Agenten und generiert für jeden erkannten Agenten ein Port Collector-Objekt. Port Collector-Objekte rufen die Port-Einträge (Technologietyp, Technologieebene, Port-Nummer und Domänenkennung) von den Port-Agenten ab und stellen diese Informationen für die Weiterbearbeitung durch den Port Manager zur Verfügung. Alle IP-Knoten, für die ein Port-Agent erkannt wurde, werden in der Submap unterhalb des Port-Managers dargestellt.

Darüber hinaus unterstützt der Port-Manager auch Lizenzdomänen. Eine Lizenzdomäne (Licence Domain) kommt in „Hot Standby“-Hardwarekonfigurationen und bei Assistant/Manager-Konfigurationen zum Einsatz, um eine Doppelzählung von lizenzierten Ports zu vermeiden. Eine Domäne ist durch die zugehörige Lizenzdomänenkennung eindeutig identifizierbar. Stimmen zwei erkannte Port-Einträge in den Werten Domänenkennung (Domain ID), Technologietyp (Technology Type) und Technologieebene (Technology Level) überein, wird die Port-Nummer nur einmalig für die zugehörige Lizenzdomäne berücksichtigt. Liefern zwei Port-Agenten eine unterschiedliche Port-Nummer für ein und dieselbe Domäne sowie Technologietyp und -ebene, berücksichtigt der Port-Manager die Information des Port-Agenten, der die höchste Port-Anzahl meldet.

Für den Fall, dass ein Port-Agent keine Domänenkennung für einen Port-Eintrag liefert, greift der Port-Manager auf die IP-Adresse des betreffenden Port-Agenten als Standard-Domänenkennung zurück.

Die Einrichtung einer Lizenzdomäne erfolgt durch den Lieferanten des HiPath-Geräts/-Systems.

Erkennt der Port-Manager, dass sich die Port-Informationen geändert haben, liest er sämtliche Port-Informationen neu ein.

Das Symbol des Port-Managers befindet sich auf der OpenScape FM DT-Bedienoberfläche unterhalb von

Root->System->Server

Das Port-Manager-Symbol stellt folgende Menüpositionen bereit:

Overall Port Sum...: Liefert die Port-Gesamtanzahl aller registrierten Ports – unabhängig vom Technologietyp oder der Technologieebene. Die Lizenzdomänen sind jedoch in dieser Kalkulation berücksichtigt.

Ports By Technology Type...: Liefert die Port-Gesamtanzahl aller Port Collectors, sortiert nach Technologietypen.

Ports By Level...: Liefert die Port-Gesamtanzahl aller Port Collectors, sortiert nach Technologietypen sowie den zugehörigen Technologieebenen.

Ports By Domain...: Liefert die Port-Gesamtanzahl aller Port Collectors, sortiert nach Technologietyp, Technologieebenen und Domänen. Um einen besseren Überblick zu erhalten, wird für die Standarddomänen die Einstellung “(IP-Adresse)“ vereinbart.

E.6 Lizenz-Manager

Eine spezifische Lizenzprüfung im Hinblick auf den Technologietyp und die Technologieebene werden in folgenden Abständen automatisch durchgeführt:

- Einmal täglich
- Bei jeder Eingabe einer Lizenzdatei und
- Jedes Mal, wenn der Server gestartet wird

Zusätzlich kann ein Anwender eine Lizenzüberprüfung veranlassen, indem er die Lizenzinformationen vom Lizenz-Manager abfragt (Abschnitt E.6.1).

Zunächst wird hierbei geprüft, ob eine Lizenz für das angeforderte Leistungsmerkmal verfügbar ist. „Verfügbar“ heißt in diesem Fall:

- Von CLA konnte die Lizenzdatei erfolgreich ausgecheckt werden.
- Das entsprechende Lizenzmerkmal ist durch die Lizenzdatei abgedeckt (nur für HPQM, HPUM).
- Der durch das Lizenzmerkmal definierte Zeitraum ist gültig.
- Die Lizenzinformationen sind intakt.
  (z.B. muss das Format der Attributzeichenfolge gültig sein und der „Digest“ muss der Lizenzzeichenfolge entsprechen).

Die Lizenzen werden, abhängig vom Lizenzmodus, gegen die IP-Adresse des OpenScape FM Servers oder gegen die MAC-Adresse der Netzwerkkarten, die vom OpenScape FM Server benutz werden, überprüft (nur für HPQM, HPUM).

Anschließend wird die Gültigkeit der Fault Management-Lizenzen für alle Plugins im Hinblick auf folgende Basisregeln geprüft:

- Es können freie Port-Lizenzen einer höheren Technologieebene genutzt werden, um fehlende Lizenzen für Ports einer niedrigeren Technologieebene zu ersetzen, und zwar unabhängig vom Technologietyp. Es ist jedoch nicht möglich, freie Port-Lizenzen einer niedrigeren Technologieebene für fehlende Port-Lizenzen einer höheren Technologieebene zu nutzen.

Beispiel:
Hicom 300- und HiPath 4000-Systeme gehören zum selben Technologietyp. Die Ports von Hicom 300-Systemen sind der Technologieebene “1” zugewiesen, die Ports von HiPath 4000-Systemen sind der Ebene “2” zugewiesen; beide haben denselben Technologietyp: “HiPath 4000”. Angenommen, OpenScape FM verfügt über 1000 Port-Lizenzen für HiPath 4000 Ebene 1 sowie 1000 Lizenzen für HiPath 4000 Ebene 2.

In diesem Fall ist folgende Port-Lizenzzuweisung gültig:

Ebene 1 - Hicom 300: 1500 Ports (Hinweis: 500 Lizenzports sind von Ebene 2-Ports zugewiesen)

Ebene 2 - HiPath 4000: 500 Ports

Der folgende Port-Lizenztransfer ist nicht möglich:

Ebene 1 - Hicom 300: 500 Ports (Hinweis: 500 Ports dieser Ebene werden nicht genutzt)

Ebene 2 - HiPath 4000: 1500 Ports (Hinweis: 500 Ports von Level >=2 werden benötigt)

Eine Lizenzverletzung wird erkannt, wenn die Anzahl der verwalteten Ports größer ist als die Anzahl der lizenzierten Ports. Die Reaktion auf eine solche Lizenzverletzung und die hiermit verbundene Fehlersituation wird in folgenden Abschnitten beschrieben:

- Abschnitt E.6.2, „Reaktion auf fehlende Lizenzen“
- Abschnitt E.6.4, „Reaktion auf Lizenzverletzungen für bestimmte Technologietypen“

E.6.1 Lizenzstatus prüfen

Ein Anwender kann den Lizenzstatus am OpenScape FM DT-Client über die Hauptmenüposition **Server->Administration->Lizenz Manager->Lizenz Information** auf der Seite **Lizenz-Status** prüfen. Das Öffnen des Dialogs startet eine Lizenzstatus-Überprüfung. Folgende Informationen werden in dem geöffneten Dialog angezeigt:

- **Feature:** Name des Leistungsmerkmals
- **Status:** Status des Lizenzmerkmals (siehe Tabelle 1)
- **Letzte Überprüfung:** Datum der letzten Lizenzprüfung
- **Start Datum:** Startdatum des Lizenzzeitraums
- **Ende Datum:** Ablaufdatum des Lizenzzeitraums
- **Lizenzierte Version:** Version des lizenzierten Plugins/der lizenzierten Applikation
- **Angeforderte Version:** Version des installierten Plugin/der installierten Applikation, für das/die eine Lizenz angefordert worden ist
- **Tage bis zum Ablauf:** Verbleibende Zeit (in Tagen) bis zum Ablauf der Lizenz
- **Toleranzzeit:** Gibt bei Registrieren einer Lizenzverletzung (Warnung) die Anzahl der verbleibenden Tage bis zur Meldung einer Lizenzverletzung (Fehler) an.
- **Attribute:** Enthält Leistungsmerkmal spezifische Informationen. Beispielsweise die Anzahl der lizenzierten Ports für eine bestimmte Technologieebene. Unterschiedliche Technologieebenen werden durch das Zeichen “|“ getrennt und die dedizierten Ports durch ein Semikolon “;“. Beispiel: Die Attribute “1;500|2;1200“ signalisieren, dass für die Technologieebene “1“ 500 Ports lizenziert sind und für die Technologieebene “2“ 1200 Ports.
- **Beschreibung:** Beschreibung der Lizenz

Für jedes geprüfte Lizenzmerkmal wird ein eigenes Objekt unterhalb des Lizenz-Managers generiert. Der Lizenz-Manager befindet sich in der Objekthierarchie an der Position **Root->System->Server->Administration->Lizenz Manager**. Das LM-Objekt verfügt über ein Kontextmenü mit der Menüposition **Information**. Über diese Position können dieselben Informationen abgerufen werden, die auch im Informationsbrowser “License Status“ erscheinen, allerdings nur für das jeweils gewählte Leistungsmerkmal. Jedes LM-Symbol hat einen bestimmten Status. Die (durch eine entsprechende Anzeigefarbe signalisierte) Dringlichkeit des Objektsstatus hängt vom Ergebnis der letzten Lizenzprüfung ab (einen Überblick über die verschiedenen Dringlichkeiten finden Sie in *Abschnitt 5.11, „Topologien im Submap/Info-Ansichtsbereich“*):

Lizenzstatus	Dringlichkeit	Beschreibung
Ok	NORMAL -> grün	Die Lizenz ist in Ordnung.
Feature Not Found	UNBEKANNT -> blau	Das angeforderte Lizenzmerkmal wurde in der Lizenzdatei nicht gefunden.
Expiration Warning 1	WARNUNG -> hellblau	Die Lizenz läuft in 60 bis 31 Tagen ab.
Expiration Warning 2	GERINGFÜGIG -> gelb	Die Lizenz läuft in 30 bis 21 Tagen ab.
Expiration Warning 3	SCHWERWIEGEND -> orange	Die Lizenz läuft in 20 bis 11 Tagen ab.
Expiration Warning 4	KRITISCH -> rot	Die Lizenz läuft in 10 bis 1 Tagen ab.
License Expired	DEAKTIVIERT -> dunkelbraun	Der Lizenzzeitraum für das Leistungsmerkmal ist abgelaufen.
License Not Started	DEAKTIVIERT -> dunkelbraun	Das Startdatum des Lizenzmerkmals ist noch nicht erreicht.
Digest Error	KRITISCH -> rot	Die Digest-Informationen stimmen nicht mit den Lizenzinformationen überein.
Host Error	KRITISCH -> rot	Das Leistungsmerkmal ist für diesen Host nicht lizenziert. (Nur bei IP-Adressen-basierter Lizenz)
MAC Error	KRITISCH -> rot	Das Leistungsmerkmal ist nicht für diesen Host lizenziert. (Nur bei MAC-Adressen-basierter Lizenz)
Info Error	KRITISCH -> rot	Die Info-Zeichenfolge liegt nicht im erwarteten Format vor.
Version Error	KRITISCH -> rot	Die angeforderte Lizenzversion entspricht nicht der lizenzierten Version. Dies ist der Fall, wenn die angeforderte Hauptversion in einer Lizenz größer ist als die Hauptversion der Lizenzinformationen.
Invalid Format Error	KRITISCH -> rot	Das Lizenzmerkmal hat ein ungültiges Format.
Violation Warning	GERINGFÜGIG -> gelb	Eine Verletzung des Lizenzmerkmals wurde erkannt. Das Lizenzmerkmal hat jetzt den Status “Lizenzverletzung (Warnung)” mit einer Nachfrist von 30 Tagen (siehe Anhang E.6.4, „Reaktion auf Lizenzverletzungen für bestimmte Technologietypen“).
Violation Error	SCHWERWIEGEND -> orange	Die Nachfrist für eine zuvor erkannte Lizenzverletzung ist abgelaufen; das Lizenzmerkmal hat jetzt den Status “Lizenzverletzung (Fehler)”. Siehe Anhang E.6.4, „Reaktion auf Lizenzverletzungen für bestimmte Technologietypen“.

Tabelle 1 Lizenzstatus – Zuordnung der Dringlichkeiten

Weiterführende Informationen zur aktuellen Lizenznutzung können über die Menüposition **Server->Administration->Lizenz Manager->Lizenz-Information** auf der Seite **Detail Information** abgerufen werden. Bei Aufruf dieses Befehls wird ein Browser mit folgenden Informationen aufgerufen:

- **Feature:** Name des Leistungsmerkmals
- **Technology Level:** Lizenzierte Technologieebene.
- **Number:** Anzahl der erfassten Einheiten (Units)
- **Max. Number:** Maximale Anzahl der lizenzierten Einheiten
- **Unit:** Lizenzierte Einheit (z.B. Ports, IP-Knoten oder EPM MIB-Objekte)
- **Check Ok:** Signalisiert, ob die Lizenzprüfung erfolgreich abgeschlossen wurde oder nicht
- **Technologieports:** Zeigt die kumulative Anzahl von Einheiten nach Technologietyp an.

E.6.2 Reaktion auf fehlende Lizenzen

Wenn beim Start des OpenScape FM DT das entsprechende Lizenzmerkmal nicht zugänglich oder gültig ist, treten folgende Einschränkungen in Kraft:

- **OpenScape FM DT:** Alle Fault Management Funktionen werden deaktiviert.
- **IP Manager:** Es können keine weiteren IP-Knoten hinzugefügt werden.
  - **Enterprise MIB:** Es ist nicht möglich weitere EPM Objekte hinzuzufügen, das EPM Hauptmenü, MIB Browser-spezifische Menüs/Funktionen und Schwellwert spezifische Menüs/Funktionen sind deaktiviert.
  - **MAR:** Die Funktionen des MAR-Plugins sind deaktiviert, aber zuvor definierte Reaktionen werden weiterhin ausgelöst.
- **HiPath 3000/5000 FM**, **HiPath 4000 FM**, **HiPath MIB FM**, **IP Manager FM, Enterprise MIB FM, OpenScape Voice:** Der Ereignis-Browser zeigt keine Fehlerereignisse an, der grafische Fehlerstatus (Symbolstatusfarbe) der Geräte/Knoten/Objekte wird deaktiviert und die Fault Management spezifischen Menüs des jeweiligen Plugins werden deaktiviert und die Fault Management spezifischen Objekte der jeweiligen Plugins werden gelöscht.
- **Sonstige Plugins:** Fehlt die Lizenz oder ist sie abgelaufen, kann das jeweilige Plugin nicht initialisiert werden bzw. die Funktionen stehen nicht länger zu Verfügung. Werden Parameter-Vorgaben überschritten, kann das Plugin während einer Kulanzfrist weiter betrieben werden. Liegt danach die Überschreitung weiterhin vor, wird das entsprechende Plugin deaktiviert.

Für den Fall, dass die Lizenzprüfung über einen Lizenz-Server erfolgt und dieser Server nicht erreichbar ist, kann der OpenScape FM Desktop noch für die Dauer von 30 Tagen genutzt werden. Nach Ablauf dieser Zeitspanne ist der OpenScape FM Desktop nicht mehr verfügbar, wenn der Lizenz-Server nicht neu gestartet wird. Kann beim erneuten Hochfahren des Lizenz-Servers die OpenScape FM Desktop-Lizenz (im Rahmen der Lizenzprüfung) nicht geprüft werden, wird der OpenScape FM Desktop angehalten.

E.6.3 Reaktion auf IP-Adressen- oder MAC-Adressen-Änderung

Abhängig vom Lizenztyp hat eine IP-Adressen- bzw. MAC-Adressen-Änderung verschiedenen Auswirkungen:

- **CLA:** Falls eine IP-Adresse bzw. MAC-Adresse für das Lizenzmerkmal gefunden wird, die nicht mit der IP-Adresse bzw. MAC-Adresse des Systems übereinstimmt, wird eine 30 Tage Nachfrist gestartet. Sobald diese Nachfrist abläuft, wird das entsprechende Leistungsmerkmal deaktiviert.
- **Interne:** Falls eine IP-Adresse bzw. MAC-Adresse für das Lizenzmerkmal gefunden wird, die nicht mit der IP-Adresse bzw. MAC-Adresse des Systems übereinstimmt, wird das Leistungsmerkmal sofort ausgeschaltet (nur für HPQM, HPUM).

E.6.4 Reaktion auf Lizenzverletzungen für bestimmte Technologietypen

HiPath 3000/5000 FM, **HiPath 4000 FM**, **HiPath MIB FM**, **IP Manager FM, OpenScape Voice:** Erkennt der MSMC Desktop, dass die Anzahl der aktiven Ports die Anzahl der lizenzierten Ports für eine bestimmte Technologieebene übersteigt (eine so genannte „Lizenzverletzung (Warnung))“, beginnt automatisch eine 30-tägige Nachfrist. Während der Nachfrist ist die Funktionalität des OpenScape FM-Systems nicht eingeschränkt. Während dieser Nachfrist wird täglich ein Warnereignis nach folgendem Muster generiert: “Anzahl der aktiven Ports übersteigt Anzahl der lizenzierten Ports”.
Bei Ablauf dieser Nachfrist („Lizenzverletzung (Fehler)“) werden sämtliche fehlerspezifischen Menüs des HiPath 3000/5000 FM, HiPath 4000 FM, HiPath MIB FM und des IP-Manager FM Plugins deaktiviert. Die fehlerspezifischen Ereignisse sowie der Fehlerstatus der zugehörigen Objekte werden jedoch nach wie vor angezeigt. Dieser Modus wird eingeschränkter FM-Modus bezeichnet. Das Fault Management wird also von einem Lizenzmerkmal aktiviert. Eine Lizenzverletzung hat Auswirkungen auf alle Plugins, die im Fault Management-Modus waren.

Wichtiger Hinweis:
Wird kein Port-Agent für ein HiPath 4000-System vorgefunden, werden die fehlerspezifischen Menüeinträge für die entsprechenden Objekte deaktiviert.
Ist ein Port-Agent für ein HiPath 4000-System länger als 7 Tage nicht zugänglich, werden die fehlerspezifischen Menüeinträge für die entsprechenden Objekte ebenfalls deaktiviert.

E.7 Lizenzmerkmal-Informationen im Logobereich

Einige Lizenzmerkmale stellen Informationen bereit, die im Logobereich des Clients angezeigt werden, wenn dieser mit dem Server verbunden wird. Auf diese Weise kann jeder Anwender genau sehen, wenn Funktionen lizenziert und aktiv sind. Sobald das Lizenzmerkmal abgelaufen ist, werden die Informationen nicht mehr angezeigt.

F Lizenzschlüssel

Um das OpenScape FM nutzen zu können, benötigen Sie eine gültige Lizenz. Wenn Sie versuchen das OpenScape FM ohne gültige Lizenz zu starten, startet es in diesem Fall nicht.

Um eine gültige Lizenz zu bekommen, wenden Sie sich bitte an Unify.

OpenScape FM Desktop und IP Manager werden jeweils mit einer Demo-Lizenz ausgeliefert; weiterführende Informationen zur Lizenzierung von OpenScape FM finden Sie in *Anhang E, „Lizenzierung“*.

G Server-Update

Falls OpenScape FM bereits installiert wurde und ein Upgrade auf eine neuere Version (inklusive des gebündelten Performance Management) durchgeführt werden soll, kann dazu einfach die neue Version in das bestehende OpenScape FM-Verzeichnis installiert werden.

Wichtiger Hinweis:
Ein Upgrade auf OpenScape FM V12 wird nur ausgehend von OpenScape FM V11 unterstützt. Upgrades von älteren Versionen müssen inkrementell durchgeführt werden.

Eine gültige Lizenz für die neue Produktversion muss über das CLA bereitgestellt bzw. installiert werden.

Plattform-Wechsel:

Falls OpenScape FM auf eine andere Plattform verschoben werden soll, beispielsweise von Windows 2000 auf ein UNIX System, oder auf ein neues System mit einer anderen IP-Adresse, kann dies ohne Datenverluste erreicht werden. Dazu kann OpenScape FM auf der neuen Plattform installiert und anschließend die alte OpenScape FM-Datenbank eingefügt werden. Es wird jedoch empfohlen, den neuen Server zuerst einzurichten und seine Funktion zu prüfen, bevor der alte Server entfernt wird.

Wichtiger Hinweis:
Das neue System sollte dem OpenScape FM unbekannt sein.
Mit anderen Worten: Das neue System sollte nicht bereits durch den alten Server überwacht worden sein.

Die folgenden Schritte sollten auf dem neuen Server durchgeführt werden:

- Installation des OpenScape FM auf der neuen Plattform gemäß Beschreibung in *Anhang C, „Installationsprozess“*.
- Anmeldung über den Client auf den OpenScape FM-Server.
- Initialisierung der benötigten Plugin-Module.
- Installieren der Lizenzdatei oder einer Verbindung zum CLA für den OpenScape FM Desktop sowie der erforderlichen Module.
- Stoppen des OpenScape FM-Servers.
- Ersetzen der Datenbankdateien in der neuen OpenScape FM-Installation:
  Entfernen der neu installierten Datenbankdateien und kopieren der bestehenden Datenbankdateien in das Datenbankverzeichnis.
  Windows: `<Standardinstallationsverzeichnis>\server\database`
  Unix: `<Standardinstallationsverzeichnis>/server/database`
- Starten des neuen Servers.
- Starten eines eigenständigen OpenScape FM-Client oder Anmeldung über Web Browser auf den OpenScape FM-Server.

G.1 Updates mittels Unify SWS Server

Um die OpenScape FM Software auf einem aktuellen Stand zu halten, enthält das OpenScape FM eine Software-Update-Funktion. Ist diese aktiviert, verwendet die Update-Funktion das Unify SWS um regelmäßig zu überprüfen, ob neue Loads oder Patches für das OpenScape FM oder die System Management Agenten (siehe *System Management Bedienungsanleitung*) verfügbar sind. Diese Überprüfung kann auch manuell angestoßen werden.

Entsprechend der Konfiguration der Update-Funktion können neue Loads oder Patches automatisch geladen und installiert werden.

Wichtiger Hinweis:
Um die Update-Funktion verwenden zu können, muss der OpenScape FM Server sich mit dem Internet und dem Unify SWS Server verbinden können. Um ein Update durchzuführen, muss das OpenScape FM auf dem Unify SWS registriert sein.

G.1.1 Update-Konfiguration

Die Konfigurationsseite der Software-Update-Funktion kann in der OpenScape FM Administrator Console über den Hauptmenü-Eintrag **Server->Administration->Server-Eigenschaften** geöffnet werden. Sie befindet sich auf der Seite **Update,** welche die folgenden Zeilen enthält:

- **Update-Server**
  Die Adresse des Unify SWS Update-Servers ist dem OpenScape FM bekannt. Ob und wann eine Verbindung zum Update-Server erfolgreich war, wird in dieser Zeile angezeigt. Die Schaltfläche **Proxy-Server konfigurieren** kann verwendet werden, um den Proxy-Server zu konfigurieren, über den das Unify SWS erreicht werden soll.
- **Registrierungsstatus**
  Ob und wann eine Registrierung auf dem Update-Server erfolgreich war, kann dieser Zeile entnommen werden. Die Schaltfläche **Registrieren** kann verwendet werden, um die Anmeldeparameter (**Login** und **Passwort**) zu definieren, die für die Registrierung verwendet werden.
- **Automatische Prüfung**
  Ist diese Zeile mit einem Haken versehen, überprüft die Update-Funktion, ob neue Loads oder Patches vorhanden sind. Die Zeile zeigt die verfügbare Load- oder Patch-Version an. Die Schaltfläche **Prüfen** kann verwendet werden, um manuell eine sofortige Überprüfung der verfügbaren Updates durchzuführen.
- **Prüfe alle**
  Diese Zeile wird verwendet, um das Zeitintervall festzulegen, in dem die automatischen Überprüfungen auf die Verfügbarkeit neuer Loads oder Patches durchgeführt werden. Beispielsweise können die Überprüfungen jedem Tag um 3 Uhr durchgeführt werden.
- **Automatisches Herunterladen**
  Ist diese Zeile mit einem Haken versehen und es wird ein neuer Load oder Patch erkannt, so wird für diesen Load oder Patch automatisch ein Download angestoßen. Die Zeile zeigt die Version des letzten geladenen Loads oder Patches an, und die Schaltfläche **Herunterladen** kann verwendet werden, um einen Download manuell anzustoßen.

- **Automatische Installation**
  Ist diese Zeile mit einem Haken versehen und ein neuer Load oder Patch wurde automatisch geladen, so wird dieser Load oder Patch automatisch installiert. Die Zeile zeigt den letzten Load oder Patch an, der zuletzt installiert wurde. Die Schaltfläche **Installieren** kann verwendet werden, um die Installation des letzten geladenen Loads oder Patches manuell zu starten.
- **Sicherung**
  Ist der Haken vor dieser Zeile gesetzt, so wird vor der Durchführung eines Updates der aktuelle Inhalt des OpenScape FM Installationsverzeichnisses (mit Ausnahme der Java DB) gesichert. Über das Eingabefeld und die Schaltfläche **Auswählen** kann der Ablageort und der Name des Ablagearchives ausgewählt werden.
- **Erforderlicher freier Plattenplatz für Update**
  In dieser Zeile kann angegeben werden, wieviel Plattenplatz mindestens auf der Installationspartition verfügbar sein muss, damit mit einem Update überhaupt begonnen wird. Hier sollte, insbesondere im Zusammenhang mit einer Sicherung, ein ausreichend großes Volumen angegeben werden.
  Wird eine Sicherung wegen mangelndem Platz abgebrochen, wird ein entsprechendes Ereignis im OpenScape FM angezeigt.

Enthält ein OpenScape FM Load oder Patch, der installiert wurde, Loads oder Patches für seine **System Management Agenten**, so können diese Agenten ebenfalls automatisch aktualisiert werden. Der *Interne System Management Agent* wird als Bestandteil des OpenScape FM immer aktualisiert. Die *Externen Agenten*, die aktualisiert werden sollen, müssen jedoch individuell konfiguriert werden.

Die Konfigurationsseite für Externe System Management Agenten kann über den Hauptmenüeintrag **System Management->Update** geöffnet werden.

Die Seite listet alle Externen System Management Agenten in separaten Tabellenzeilen auf, welche den **Servername**n, die **Server IP** und die aktuell installierte **Version** des jeweiligen Agenten anzeigen.

Die Haken in der Spalte **Automatisches Update** definieren, welche der Agenten automatisch aktualisiert werden sollen, falls ein neuer Agenten-Load oder Patch während der Installation des OpenScape FM Loads oder Patches gefunden wird.

Die unterhalb der Tabelle befindliche Schaltfläche **Update** kann verwendet werden, um den aktuellen Load oder Patch manuell auf den ausgewählten Agenten zu installieren.

G.1.2 Update-Ausführung

Das OpenScape FM verwendet den separaten Windows- oder Linux.-Dienst **OpenScape Update Service**, um neue Loads oder Patches zu installieren.

Dieser Dienst wird während der Installation des OpenScape FM registriert. Er wird durch das OpenScape FM gestartet, wenn ein neuer Load oder Patch installiert werden soll.

Der Update-Dienst führt ein vordefiniertes Kommando aus, welches die Optionen enthält, die Installation des Loads oder Patches still durchzuführen. Nach Beendigung der Installation wird der Update-Dienst beendet. Während der Installation des Loads oder Patches wird der OpenScape FM Startup Dienst gestoppt und neu gestartet.

Die System Management Agenten enthalten ebenfalls einen Update-Dienst.

Ist **Automatisches Update** für einen Externen System Management Agenten ausgewählt und es wurde ein neuer Load oder Patch geladen, so wird der Load oder Patch zum Agenten übertragen und er wird aufgefordert, die Installation dieses Loads oder Patches durchzuführen. Das Update des Agenten wird durchgeführt, indem der Update-Service des betroffenen Agenten gestartet wird.

Ist **Automatisches Update** für einen Externen System Management Agenten nicht ausgewählt, müssen Updates für diesen Agenten manuell angestoßen werden.

Für die Übertragung des neuen Loads oder Patches an einen Agenten werden die bereits bekannten/ verwendeten Ports des System Management Agenten verwendet. Es ist daher *nicht* notwendig, die Regeln der Firewall um zusätzliche Ports zu erweitern.

Stichwörter

R

S