A MITEL
PRODUCT
GUIDE

Mitel OpenScape Fault Management

Mitel OpenScape Fault Management V13 Event Gateway

Bedienungsanleitung
10/2025

A31003-F30D0-U104-01-0019

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

Inhalt

1 Vorwort

1.1 Zweck

Dieses Handbuch ist eine Einführung in die Verwendung des Event Gateway Plugins für OpenScape FM. Grundlegendes Wissen über Netzwerk-Management und über das OpenScape FM werden vorausgesetzt. Mehr zu Letzterem findet sich in der *OpenScape FM Desktop Bedienungsanleitung*. Zusätzlich sollte der Anwender zumindest Grundwissen über die Konfiguration von SNMP Trap Empfängern besitzen.

1.2 Zielgruppe

Dieses Handbuch richtet sich an den Anwender, der den Umgang mit dem Event Gateway Plugin für OpenScape FM kennenlernen möchte.

1.3 Aufbau des Handbuchs

Dieses Handbuch ist wie folgt organisiert:

- *Kapitel 1, „Vorwort“* erklärt die Struktur des Handbuchs.
- *Kapitel 2, „Einführung“* erklärt das grundlegende Konzept des Event Gateway Plugin für OpenScape FM.
- *Kapitel 3, „Erste Schritte“* beschreibt die Installation und den Start des Event Gateway Plugin für OpenScape FM.
- *Kapitel 4, „Allgemeine Konfiguration“* erklärt die grundlegenden Funktionen des Event Gateway Config Tools.
- *Kapitel 5, „Verbindungs-Parameter“* beschreibt die unterschiedlichen Verbindungs-Typen und wie sie konfiguriert werden können.
- *Kapitel 6, „Filter-Parameter“* beschreibt wie Filter für Quellen-Verbindungen definiert werden können.
- *Kapitel 7, „Trap-Weiterleitung“* zeigt wie ein Trap-Empfänger hinzugefügt werden kann.
- *Kapitel 8, „Logging/Troubleshooting“* gibt Hinweise zur Fehlersuche.
- *Kapitel 9, „Konfigurations-Beispiel“* enthält Beispiele wie das Event Gateway Plugin für verschiedene Ziele konfiguriert werden kann.
- *Anhang A, „System-Voraussetzungen“* enthält die Hardware- und Software-Voraussetzungen für das Event Gateway Plugin.
- *Anhang B, „SNMP Trap MIB Definition“* enthält die SNMP Trap MIB Definition für Traps, die durch den Trap Forwarder versendet werden.
- *Anhang C, „Variablen“* beschreibt die Variablen, die in den verschiedenen Konfigurations-Schritten verwendet werden können.

- *Anhang D, „Glossar“* enthält ein Glossar mit einigen im Handbuch verwendeten Ausdrücken.

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.

Beispiel: **Save**.

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: *OpenScape FM Desktop Bedienungsanleitung.*

Kursiv gedruckte Schrift dient auch der Betonung.

Beispiel: *Alle* Anwender sind davon betroffen.

2 Einführung

Das OpenScape Fault Management (OpenScape FM) sammelt und repräsentiert die Ereignisse aller unterstützten HiPath/OpenScape Technologien (z.B. HiPath 3000, HiPath 4000, OpenScape Voice, HiPath MIB). Diese und andere Ereignisse werden im OpenScape FM Ereignis-Browser gesammelt. Wurde das konfigurierte Maximum an Ereignissen durch das OpenScape FM gesammelt, so werden die ältesten gespeicherten Ereignisse durch die neu ankommenden Ereignisse überschrieben. Um die Ereignis-Daten durch andere Werkzeuge zu erhalten oder zu bearbeiten, können die Daten mit Hilfe des Event Gateway für OpenScape FM als SNMP Traps an diese weitergeleitet werden.

Um sicherzustellen, dass nur die Ereignisse weiter geleitet werden, die für die Ziel-Applikation relevant sind, existiert ein zweistufiger Filter-Mechanismus. Dieser Mechanismus reduziert die Zahl der durch das Event Gateway bereit gestellten Ereignisse.

- Der erste Mechanismus filtert die Ereignisse, die in das Event Gateway kommen. Er basiert auf dem modularen und stark konfigurierbaren Rechte-System des OpenScape FM. Das Event Gateway verbindet sich mit dem OpenScape FM als ein spezifischer Anwender, und es werden nur die Ereignisse übertragen, die von diesem Anwender gesehen werden können. Z.B. kann das Event Gateway so konfiguriert werden, dass es sich mit einem Anwender zum OpenScape FM verbindet, der nur die OpenScape FM Rechte für Systeme in einer bestimmten Region besitzt. Es werden dann nur Ereignisse, die diese Systeme betreffen, im Event Gateway sichtbar.
- Der zweite Mechanismus filtert die ausgehenden Ereignisse. Nur Ereignisse, die den im Event Gateway definierten Filter-Parametern entsprechen, werden weitergeleitet. Für diese Filterung kann eine Kombination von Status, Kategorie, Klasse, OpenScape FM Tenant Domänen und Ereignis-Attributen abgefragt werden.

Die Kombination beider Mechanismen erlaubt eine große Flexibilität bei der Erstellung von Filtern.

In diesem Handbuch steht:
HiPath 4000: für HiPath 4000 oder OpenScape 4000,
HiPath 3000: für HiPath 3000 oder OpenScape Business.

2.1 Übersicht über die Event Gateway Konfiguration

Die Event Gateway Konfiguration setzt sich aus drei Punkten zusammen:

1. Konfiguration der Eingangs-Verbindung
2. Erstellung eines Filters für die Eingangs-Verbindung (optional)
3. Erstellung einer Ziel-Konfiguration

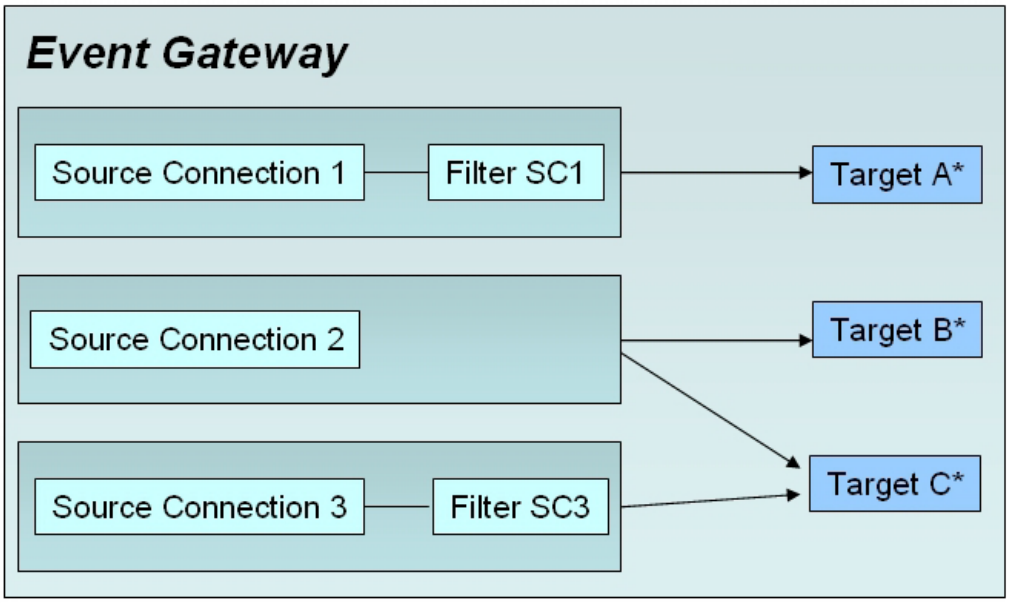

Bild 1 Übersicht über die Event Gateway Komponenten

Bei der Konfiguration der Eingangs-Verbindung wird festgelegt, welche Ereignisse durch das Event Gateway gesammelt werden. Der OpenScape FM Server, der Verbindungstyp, und die Login-Informationen, die das Event Gateway verwendet, um sich mit dem OpenScape FM zu verbinden, werden hier festgelegt. Mit dem Verbindungstyp wird die Quelle angegeben: Dies kann ein OpenScape FM Ereignis-Browser oder eine ECE-Konfiguration sein. Das ECE-Plugin muss ggfls. zuerst installiert werden, und es muss eine gültige ECE-Lizenz vorliegen. Die Login-Informationen bestimmen den Anwender, mit dem sich das Event Gateway mit dem OpenScape FM Server verbindet. Die diesem Anwender zugewiesenen Rechte bestimmen, welche Ereignisse im Event Gateway gesehen werden können. Mehr dazu findet sich in *Kapitel 5, „Verbindungs-Parameter“*.

Für jede Eingangs-Verbindung kann ein Filter definiert werden. Dieser Filter besteht aus einem oder mehreren Filter-Ausdrücken. Die Verwendung eines Filters erlaubt es, die Anzahl der ausgehenden Ereignisse zu begrenzen. Ist kein Filter definiert, so werden alle Ereignisse, die das erste Filter-Level passieren weiter geleitet. *Kapitel 6, „Filter-Parameter“* zeigt, wie Filter für eine Eingangs-Verbindung konfiguriert werden können.

Mittels des Trap Forwarder Moduls können OpenScape FM Ereignisse in SNMP-Traps verwandelt werden. Diese Traps werden an ein oder mehrere SNMP-Trapziele weitergeleitet (forwarded), um sie z.B. einem Umbrella Management System zu Verfügung zu stellen. Da der Trap Forwarder, falls nicht anders gewünscht, ein einheitliches Trap-Format für alle ausgehenden Traps verwendet (siehe *Anhang B, „SNMP Trap MIB Definition“*), muss vom Trap-Empfänger nur ein SNMP-Trapformat erkannt werden können. Selbst wenn neue OpenScape FM Ereignis-Typen im OpenScape FM hinzugefügt werden, so treffen auch diese automatisch auf der Empfänger-Seite ein, falls sie den Filter-Kriterien genügen. Die Trap-Ziele weiter geleiteter OpenScape FM Ereignisse werden zentral im Event Gateway Configuration Tool konfiguriert. Die Original-System senden ihre Traps weiterhin nur an den OpenScape FM Server. Mehr über die Konfiguration von Trap-Zielen findet sich in *Kapitel 7, „Trap-Weiterleitung“*.
Zusätzlich erlaubt das Trap Forwarder Modul die Erstellung/Verwendung von Anwender spezifischen Trap-Formaten, um dem Anwender ein Maximum an Flexibilität der Trap-Strukturen bereit zu stellen. Im Falle spezifischer Trap-Formate kann zusätzliche Konfiguration auf der Empfänger-Seite notwendig sein.

3 Erste Schritte

3.1 Installation

Während der Installation des OpenScape FM wird das Event Gateway Plugin automatisch installiert. Im Rahmen der Installation des Event Gateway wird der Dienst „OpenScape Event Gateway“ angelegt und gestartet. Das Event Gateway Plugin liefert die notwendige Oberfläche für die Konfiguration des Event Gateway.

3.1.1 Event Gateway Plugin Installation

Das Event Gateway Plugin ist Bestandteil der OpenScape FM Installation. Es muss nach der Installation lediglich als Plugin initialisiert werden (**Server->Plugins->Initialisiere Event Gateway Plugin**).

3.1.2 Event Gateway Dienst Installation

Während der Installation des OpenScape FM wird das Event Gateway Plugin automatisch installiert. Im Rahmen der Installation wird der Dienst „OpenScape FM Event Gateway“ eingerichtet und gestartet. Im OpenScape FM stellt das Plugin die notwendige Oberfläche bereit, um das Event Gateway konfigurieren zu können.

3.2 Lizenzierung

Um das Trap Forwarder Modul zu betreiben, muss im OpenScape FM eine Lizenz für das Event Gateway installiert worden sein. Ohne eine gültige Lizenz wird das Event Gateway Plugin, und damit der Trap Forwarder, nicht gestartet.

Eine Lizenz für die Weiterleitung von Ereignissen vom OpenScape FM Server und an bis zu zwei Trap-Ziele ist bereits in der Grund-Lizenz des Fault-Management enthalten.

Da das Event Gateway ein Plugin im OpenScape FM ist, wird die Lizenz über den Standard-Lizenzierungs-Mechanismus des OpenScape FM geladen. Mehr dazu findet sich in der Bedienungsanleitung des OpenScape FM Desktop.

3.3 Starten/Stoppen des OpenScape FM Event Gateway Dienstes

Windows:

Auf Windows-Plattformen registriert sich des Event Gateway als System-Dienst. Um den OpenScape Event Gateway Dienst zu stoppen bzw. zu starten, kann die Dienste-Verwaltung verwendet werden.

Kann der Dienst nicht erfolgreich gestartet werden, finden sich in *Abschnitt 8.1, „Logging“* und *Abschnitt 8.2, „Troubleshooting“* möglicherweise Hinweise auf die Ursache.

Unix:

Während der Installation wird ein Start-Up-Script auf dem Betriebssystem spezifischen Start-Up-Verzeichnis eingerichtet. Ist eine gültige Lizenz verfügbar, wird der OpenScape FM Event Gateway Server bei einem Systemneustart automatisch gestartet.

Der OpenScape FM Event Gateway Server kann mit Hilfe von Skripten gestartet oder gestoppt werden. Sie heißen `startgw` und `stopgw` und befinden sich im Installations-Verzeichnis.

Nach dem Start des OpenScape FM Event Gateway läuft ein Prozess mit einem Namen wie "`/usr/bin/java -Djava.security.policy=/opt/OpenScapeEventGateway/server/conf`" auf der Maschine.

Tritt während des Starts eine Fehlermeldung auf, können *Abschnitt 8.1, „Logging“* und *Abschnitt 8.2, „Troubleshooting“* eventuell weiterhelfen.

4 Allgemeine Konfiguration

Für die Konfiguration des Gateway wird das Gateway Config Tool verwendet. Das Gateway Config Tool verbindet sich dazu mit einem laufenden OpenScape FM Event Gateway Server (siehe *Abschnitt 3.3, „Starten/Stoppen des OpenScape FM Event Gateway Dienstes“*). Läuft der OpenScape FM Event Gateway Service nicht, wird eine Warnmeldung angezeigt, und das Gateway Config Tool wird nicht gestartet. Das Config Tool muss nicht auf dem gleichen System laufen wie der OpenScape FM Event Gateway Server.

Das Config Tool wird durch die Auswahl des Menüeintrages **Konfigurieren** im Hauptmenü **Erweiterungen->Event Gateway** gestartet. Dies öffnet ein Login-Fenster in dem ein Host-System und ein Passwort eingegeben werden müssen. Das Host-Feld legt den Hostnamen des Systems fest, auf dem der Event Gateway Server konfiguriert werden soll. Das **Passwort**-Feld sichert den Zugriff auf die Gateway Konfiguration. Das Default-Passwort ist leer und muss beim ersten Login gefüllt werden. Es kann später auf der Karteikarte **Server-Eigenschaften** geändert werden.

Es existieren die folgenden Karteikarten:

- **Verbindungs-Parameter:**
  Definition der Quell-Verbindungen (siehe *Kapitel 5*).
- **Filter-Parameter:**
  Definition der Filter der Eingangsereignisse (siehe *Kapitel 6*).
- **Server-Eigenschaften:**
  Konfiguration des Event Gateway (siehe *Abschnitt 4.1*).
- **Trap Ziel Parameter:**
  Definition der Ziele und Daten für die Trap-Weiterleitung (siehe *Kapitel 7*).

4.1 Server Eigenschaften

Auf dieser Karteikarte wird das Login-Passwort für den OpenScape FM Event Gateway Server konfiguriert.

Die **Server Eigenschaften** Karteikarte des Gateway Config Tools zeigt die Felder an, die benötigt werden, um das Passwort zu verändern. Das aktuelle Passwort muss in das Feld **Passwort** eingegeben werden. Das neue Passwort in das Feld **Neues Passwort**. Zur Bestätigung muss es ein weiters Mal in das Feld **Neues Passwort wiederholen** eingegeben werden, um Tippfehler auszuschließen.

Die Schaltfläche **OK** ändert das Passwort des Config Tools auf den Wert, der in die Felder **Neues Passwort** und **Neues Passwort wiederholen** eingetragen wurde, sofern die Werte identisch sind.

Zusätzlich kann festgelegt werden, ob der OpenScape FM Event Gateway Server Debug-Ausgaben in seiner Log-Datei erzeugen soll. Um die Debug-Ausgabe-Option zu aktivieren/deaktivieren, muss der Haken hinter **Server Debugging Ausgaben aktivieren** gesetzt bzw. entfernt werden, und die Schaltfläche **Ok** gedrückt werden. Es ist zu beachten, dass das Aktivieren der Debug-Ausgaben zu Performance-Einschränkungen führen kann.

Zusätzlich können in der Tabelle **System-Properties** weitere Eigenschaften definiert werden.

4.2 Standard-Schaltflächen

Einige Schaltflächen stellen grundlegende Funktionen bereit, die auf allen Karteikarten, mit Ausnahme der Server Eigenschaften, erscheinen. Diese werden in diesem Abschnitt beschrieben.

Die Schaltfläche **Erzeugen** kann verwendet werden, um zusätzliche Einträge in der links befindlichen Tabelle der Karteikarte vorzunehmen. Zum Beispiel kann sie verwendet werden, um zusätzliche Verbindungen innerhalb der Verbindungs-Parameter Karteikarte zu erzeugen. Im Falle von **Filter-Parametern** wird die Schaltfläche **Erzeugen** verwendet, um eine neue Filter-Ausdrucks-Zeile zu erzeugen.

Die Schaltfläche **Entfernen** entfernt die selektierten Einträge. Das Entfernen muss in einem Bestätigungsfenster bestätigt werden.

Die Schaltfläche **Speichern** speichert die veränderten Einstellungen ab. Die Schaltfläche ist nur aktiv, wenn mindestens eine Veränderung vorgenommen wurde.
Nach Betätigung der Schaltfläche **Speichern** verwendet der Gateway sofort die neue Konfiguration.

Die Schaltfläche **Beenden** verwirft alle gemachten Einstellungsänderungen, seitdem die **Speichern** Schaltfläche das letzte mal verwendet wurde. Das Verwerfen muss in einem Bestätigungsfenster bestätigt werden.

4.3 Makros für Enterprise spezifische SNMP-OIDs

Das Gateway bietet die Möglichkeit Makros für Enterprise spezifische SNMP OIDs (Enterprise OID) zu definieren. Die Makros können in einem Menü ausgewählt werden, um das Nachschlagen häufig benötigter OIDs unnötig zu machen und die Lesbarkeit der Konfiguration zu erhöhen. Das Menü wird durch einen Rechtsklick in einem Feld angeboten, in das Enterprise OIDs eingegeben werden können (z.B. in Filter-Ausdrücken). Wird ein Makro ausgewählt, wird der Name des Makros im Config Tool angezeigt. Intern wird aber die definierte Enterprise OID verwendet.

Die Makros werden in der Datei `enterprises.properties` im Installationsverzeichnis des Gateway Servers gesammelt:
`<Gateway installation directory>/server/resources/macros`.

Um einen neuen Makro-Eintrag zu definieren, muss eine neue Zeile in der `enterprises.properties` Datei hinzugefügt werden. Zunächst muss der Name des Makros eingegeben werden. Dieser Name wird im Menü angezeigt. Diesem muss ein Gleichheitszeichen (=) folgen, und diesem die Enterprise OID, welche durch das Makro interpretiert werden soll. Nach dem Speichern der Datei, muss der OpenScape FM Event Gateway Server durchgestartet werden, um die neuen Makros zu aktivieren. Es ist zu beachten, dass bei einer Update-Installation des OpenScape FM Event Gateway Servers alle Änderungen in der `enterprises.properties` verloren gehen. Vor einem OpenScape FM Event Gateway Server Update sollte also ein Backup dieser Datei durchgeführt werden.
Die folgenden Zeilen enthalten Beispiele zur Definition von Makros:

```
HiPath4000MajorAlarmOn=1.3.6.1.4.1.231.7.2.1.21.2.2.30
HiPath4000MajorAlarmOff=1.3.6.1.4.1.231.7.2.1.21.2.2.31
```

5 Verbindungs-Parameter

Auf der Karteikarte **Verbindungs-Parameter** kann die Verbindung zwischen dem Gateway und einer Quelle (ein OpenScape FM Server) eingerichtet werden. Verbindungen werden benötigt, um die Ereignisse aus dem OpenScape FMzu erhalten.

Es wird ein Login-Parameter und ein Verbindungstyp zum Quell OpenScape FM Server definiert.

Die Zugriffsrechte des Anwenders, der für die Verbindung des Gateway ausgewählt wurde, bestimmen die Ereignisse, die vom Gateway gesehen werden. Auf diese Weise kann das hoch konfigurierbare modulare Zugriffsrechte-System des OpenScape FM verwendet werden, um die empfangenen Ereignisse sinnvoll zu beschränken. So kann zum Beispiel ein OpenScape FM Anwender erstellt werden, der nur spezifische Rechte für ein bestimmtes System besitzt. Ein Gateway, das diesen Anwender zur Verbindung verwendet, erhält dann nur Ereignisse für dieses System.

Eine differenziertere Methode des Filterns stellt die Verwendung der Event Correlation Engine dar. Die ECE kann so konfiguriert werden, dass Ereignisse gefiltert werden können, bevor sie an das Gateway gesendet werden.

Für jede konfigurierte Verbindung kann zusätzlich ein Filter des Gateway selbst verwendet werden. Nur Ereignisse, die diesen Filter passieren, werden weiter geleitet. Mehr über Filter findet sich in *Kapitel 6, „Filter-Parameter“*.

Die **Verbindungs-Parameter** Karteikarte besteht aus zwei Teilen: Die linke Seite enthält eine Liste der konfigurierten Verbindungen. Die rechte Seite zeigt die konfigurierten Werte für jeweils ein Element dieser Liste an.

- **Verbindungs-Name**: Hier sollte ein sprechender Name, der die Verbindung beschreibt, eingegeben werden. Dieser Name wird in anderen Karteikarten verwendet, um die Verbindung auszuwählen.
- **Host-Name**: Der Server-Name kann entweder ein Host-Name oder die IP-Adresse eines OpenScape FM Servers sein.
- Das Feld **Verbindung** wird verwendet um den Verbindungs-Typ zu definieren. Der Verbindungs-Typ bestimmt, wie das Gateway sich mit dem Quell-Server verbindet. Dies kann eine der folgenden Methoden sein:
  - **PSAccount** bedeutet, dass sich das Gateway als ein definierte Anwender auf dem OpenScape FM Server anmeldet. Das Gateway erhält alle Ereignisse aus dem Ereignis-Browser des OpenScape FM, auf die der Anwender Zugriff hat.
  - **MegEceConnector** bedeutet ebenfalls, dass sich das Gateway als ein definierter Anwender auf dem OpenScape FM anmeldet. Aber das Gateway erhält nur die Ereignisse, die für den Anwender verfügbar sind und die durch einen korrespondierenden MegEceConnector-Knoten im OpenScape FM geroutet wurden. Mehr über die Konfiguration der ECE-Verbindung findet sich in *Abschnitt 5.1*. Mehr über das ECE selbst findet sich in der separaten Event Correlation Engine Bedienungsanleitung.
- **Benutzer:** Der Anwender-Name, der vom Gateway verwendet wird, um sich auf dem OpenScape FM Server anzumelden.
- **Passwort/Passwort erneut eingeben:** Das Passwort des zuvor angegebenen Anwenders.
- **RMI Port**: Der Server-Port über den die Kommunikation stattfinden soll. Der Standard-Wert ist 3042.

5.1 MEG-ECE Verbindung

Wurde ein **MegEceConnector** für eine Verbindung konfiguriert (siehe oben), so werden nur die Ereignisse durch das Gateway behandelt, die durch den zugehörigen MegEceConnector-Knoten auf der ECE Submap geleitet wurden.

Bevor eine MEG-ECE-Verbindung benutzt werden kann, muss das ECE Plugin initialisiert sein.

Ist im Gateway eine MegEceConnector Verbindung konfiguriert, erscheint im OpenScape FM ein MegEceConnector Symbol auf der ECE Submap. Der Bezeichner des Symbols enthält die IP-Adresse des OpenScape FM Event Gateway Servers und den OpenScape FM Anwender, den das Gateway verwendet, um sich mit dem OpenScape FM zu verbinden. Das Ereignisquelle-Symbol auf der ECE Submap repräsentiert die Quelle aller OpenScape FM Ereignisse, das Ereignis-Browser- Symbol alle Ereignisse des Ereignis-Browsers. Ist das Ereignis-Browser-Symbol direkt mit dem MegEceConnector Symbol verbunden, so werden alle Ereignisse aus dem Ereignis-Browser an das Gateway gesendet. Natürlich können ein oder mehrere Filter definiert und zwischen dem Ereignis-Browser-Symbol und dem MegEceConnector Symbol angeordnet werden. In diesem Fall werden nur die Ereignisse an das Gateway übermittelt, welche die definierten Filter passieren. Mehr über das Definieren von Filtern im ECE findet sich in der separaten Event Correlation Engine Bedienungsanleitung.

6 Filter-Parameter

Generell werden alle eingehenden Ereignisse einer Eingangs-Verbindung (OpenScape FM) an das definierte Ziel (Trap Target) weitergeleitet. Die Zahl der Ereignisse, die durch das Gateway weitergeleitet werden, kann mit zwei Methoden reduziert werden:

1. Durch die Auswahl eines Anwenders auf der Karte **Verbindungs-Parameter**, der nur über beschränkte Ereignis-Betrachten-Rechte verfügt. Z.B. ein Anwender, der nicht alle Ereignisse, sondern nur Ereignisse für bestimmte Systeme sehen darf.
2. Durch die Definition von Filter-Regeln für das Gateway auf der Karte **Filter-Parameter**.

In den meisten Fällen, ist es einfacher nur die zweite Option zu verwenden, und im OpenScape FM einen Anwender zu wählen, der alle Ereignisse sehen darf. Die Gateway Filter-Regeln, werden in diesem Kapitel beschrieben. Für jede Eingangs-Verbindung kann ein oder kein Filter definiert werden. Dieser kann aus einem oder mehreren Filter-Ausdrücken bestehen, die durch UND- oder ODER-Beziehungen verbunden werden können.
Jeder Filter-Ausdruck kann die folgenden Kriterien eines Ereignisses überprüfen:

- der Status,
- das Source-Objekt,
- die Klasse des Source-Objektes,
- die Tenant-Domäne des Source-Objektes
- und die unterschiedlichen Ereignis-Attribute, wie z.B. die Enterprise OID der Original-Traps.

Die verschiedenen Filter-Ausdrücke werden auf Gleichheit (`a=b`) überprüft. Für Filter-Ausdrücke, welche die Quelle, die Klasse oder die Tenant Domäne betreffen, kann ein regulärer Ausdruck für den Vergleich verwendet werden.

Hinweis:
Das Gateway verwendet die Java-Klasse `java.util.regex.Pattern`, um reguläre Ausdrücke auszuwerten. Da reguläre Ausdrücke ein mächtiges Werkzeug darstellen, kann dieses Handbuch keine vollständige Beschreibung liefern. Mehr dazu findet sich in der spezifischen Java-Dokumentation der entsprechenden Klasse.

Für Filter-Ausdrücke, die sich auf Ereignis-Attribute beziehen, kann zusätzlich aus verschiedenen Vergleichs-Operatoren ausgewählt werden. Eine Beschreibung der unterschiedlichen Funktionen der Formatierungssprache findet sich in der *OpenScape FM Desktop Bedienungsanleitung*. Ein einfacher Filter kann z.B. „Severity=Critical“ sein, es sind aber auch komplexe Filter möglich, welche die unterschiedlichen Funktionen der String Formatting Language in Kombination verwenden.

Die Filter-Ausdrücke werden auf der **Filter-Parameters** Karteikarte (*Bild 2*) konfiguriert. Die Karte besteht aus zwei Teilen: Die linke Seite besteht aus einer Liste, die alle konfigurierten Eingangs-Verbindungen enthält. Die rechte Seite enthält eine Tabelle, welche die konfigurierten Filter-Ausdrücke für die ausgewählte Verbindung enthält.

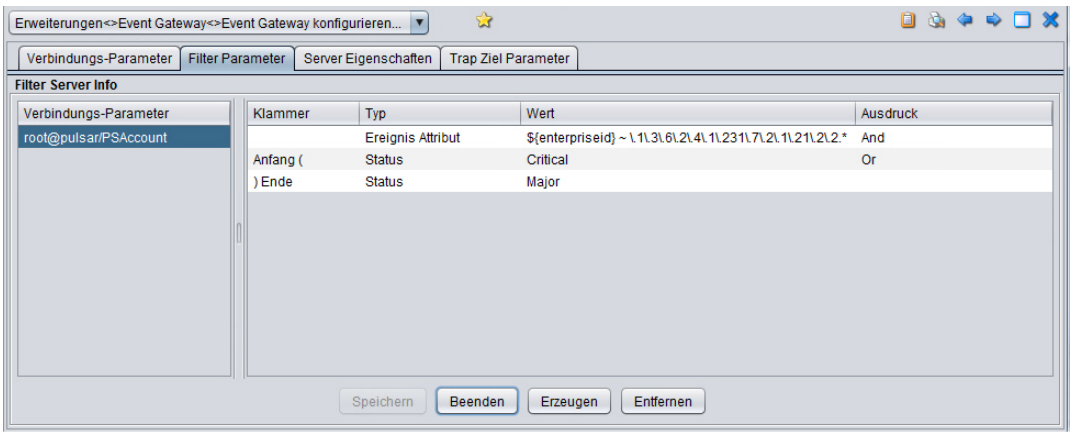

Bild 2 Config Tool: Filter-Parameter

Die Filter-Tabelle besteht aus vier Spalten: **Klammer**, **Typ**, **Wert** und **Ausdruck**.

Mit Hilfe der Spalte **Klammer** können Ausdrücke gruppiert werden. Alle Werte, die für eine spezifische Zeile möglich sind, können aus dem Kontextmenü der Spalte ausgewählt werden. Das Kontextmenü wird nur angezeigt, wenn mindestens zwei Filter-Ausdrücke definiert wurden. Verschachtelte Klammerungen sind nicht möglich.

Die Spalte Typ bietet die folgenden Filter-Typen an: „Kategorie“, „Status“, „Quelle“, „Quelle (Reg.-Exp.)“, „Klasse (Reg.-Exp.)“, „Tenant-Domäne (Reg.-Exp.)“ und „Ereignis-Attribut“.
In der Spalte **Wert** wird der Vergleichswert für den selektierten Typen spezifiziert. Die Spalte Wert bietet ein Kontextmenü an, um Vergleichswerte schnell auswählen zu können. Dabei ist der Inhalt des Kontextmenüs vom selektierten Typ abhängig.

Wurde für eine Verbindung mehr als ein Ausdruck definiert, so können sie mit einer ’UND’- oder ’ODER’-Beziehung in der **Ausdruck**-Spalte verbunden werden. Voreingestellt ist die ’UND’-Beziehung. Diese kann durch ein Anklicken des Feldes und durch die Auswahl einer anderen Beziehung verändert werden.

Die folgenden Filter-Typen sind möglich:

- **Kategorie:**
  Ein Kategorie-Filter überprüft, ob die Kategorie des Ereignisses mit der Kategorie übereinstimmt, die im Feld **Wert** spezifiziert wurde. Um einen Kategorie-Filter zu definieren, muß im Feld **Typ** der Wert ’Kategorie’ ausgewählt werden, und im Feld **Wert** die Ereignis-Kategorie, wie zum Beispiel:
  „User Events“: Ereignisse, die sich auf Anwender-Operation beziehen, z.B. Login
  „IP Manager“: Ereignisse, die sich auf IP-Knoten und Netzwerke beziehen.
  „<Name of plugin>“: Fehler-Ereignisse, für überwachte Geräte.

  Eine Liste der verfügbaren Ereigniskategorien findet sich im OpenScape FM Ereignis-Browser.

- **Status:**
  Ein Status-Filter vergleicht den Status, der im Feld **Wert** angegeben wird, mit dem Status des Ereignisses. Um einen Status-Filter zu definieren, muß im Feld Typ der Wert „Status“ und im Feld **Wert** der entsprechende Status angegeben werden. Es gibt sechs mögliche Status-Werte: ’Unknown’, ’Normal’, ’Warning’, ’Minor’, ’Major’ oder ’Critical’. Diese Werte entsprechen den Status-Werten im OpenScape FM Ereignis-Browser.

- **Ursprung:**
  Ein Ursprungs-Filter überprüft, ob der Ursprungs-Objekt-Name des Ereignisses mit dem Namen übereinstimmt, der im Feld **Wert** definiert ist. Um einen Ursprungs-Filter zu definieren, muß im Feld **Typ** der Wert 'Ursprung' und im Feld **Wert** der OpenScape FM Objektname des gewünschten Ursprung-Objektes eingegeben werden. Der Ursprungs-Name kann über den Menüeintrag 'Objekt->Eigenschaften' im OpenScape FM Clienten für ein Objekt ermittelt werden (Attribut: Name).

- **Ursprung (Reg.-Exp.):**
  Entspricht der Option 'Ursprung'. Nur das hier der Vergleich gegen einen regulären Ausdruck durchgeführt wird, der im Feld **Wert** konfiguriert wird.

- **Klasse (Reg.-Exp.):**
  Ein Klassen-Filter überprüft, ob die Klasse des Ursprungs-Objektes des Ereignisses mit dem regulären Ausdruck übereinstimmt, der im Feld **Wert** definiert ist. Um einen Klassen-Filter zu definieren, muß im Feld **Typ** der Wert 'Klasse (Reg.-Exp.)' und im Feld **Wert** eine Konstante oder ein regulärer Ausdruck angegeben werden, der die Objekt-Klasse der gewünschten Objekte repräsentiert. Die Klasse eines Objektes kann über den Menüeintrag 'Objekt->Eigenschaften' im OpenScape FM Clienten für ein Objekt ermittelt werden (Attribut: Klassen-Fähigkeit).

- **Tenant-Domäne (Reg.-Exp.):**
  Sollen nur Ereignisse verwendet werden, die sich auf Objekte beziehen, die zu einer bestimmten Tenant-Domäne gehören, so kann der Filter-Typ 'Tenant-Domäne' verwendet werden. Diese Filter treffen nur zu, wenn ein Objekt zu einer Tenant-Domäne gehört, deren Name auf den regulären Ausdruck im Feld **Wert** zutrifft. Um einen Tenant-Domänen-Filter zu definieren, muß im Feld **Typ** der Wert „Tenant Domäne (Reg.-Exp.)“ ausgewählt werden, und eine Konstante oder ein regulärer Ausdruck in das Feld **Wert**, um den Namen der OpenScape FM Tenant-Domäne zu beschreiben.

- **Ereignis-Attribut:**
  Ein Ereignis liefert eine Reihe von Informationen. Im Gateway kann auf diese Informationen durch sogenannte Ereignis-Attribute zugegriffen werden. Beispielsweise ist die Enterprise OID des Traps, der das Ereignis ausgelöst hat, ein Attribut. Über Ereignis-Attribut-Filter kann das Gateway überprüfen, ob ein Ereignis-Attribut einem spezifischen Wert entspricht. Dieser Wert kann ein weiteres Ereignis-Attribut sein, eine Konstante oder eine Variable, eine Operation (siehe Beschreibung der Formatierungssprache in der *OpenScape FM Desktop Bedienungsanleitung*) oder eine Kombination von diesen. (Das Kontextmenü, das für Ereignis-Attribute angezeigt wird, kann durch Anwender definierte Einträge erweitert werden - siehe *Kapitel 4, „Makros für Enterprise spezifische SNMP-OIDs“*.)
  Für Ereignis-Attribute ist die Spalte **Wert** dreigeteilt. In der Mitte kann ein Operator ausgewählt werden. Dieser Operator wird verwendet, um die Einträge im linken und rechten Feld zu vergleichen. Trifft der Vergleich zu, ist der Ausdruck gültig.

Wurde ein Filter spezifiziert, so wird ein Ereignis (das über die Eingangs-Verbindung erhalten wird, für die der Filter definiert wurde) nur dann an das Ziel-System (Trap Target) weitergeleitet, wenn der komplette Filter zutrifft.

Beispiel:
Sollen nur HiPath 4000 Ereignisse mit dem Status Major oder Crititcal empfangen werden, so sollte ein Kategorie-Filter mit dem Wert “HiPath 4000” und zwei Status-Filter mit den entsprechenden Werten („Major“ und „Critical“) definiert werden (*Bild 2*).

Achtung:
Falls mehr als eine Eingangs-Verbindung mit dem gleichen OpenScape FM Server für die gleiche Ziel-Konfiguration ausgewählt wurde, und ein Ereignis für mehrere dieser Eingangs-Verbindungen erfolgreich den Filter durchläuft, so können mehrere Traps für das gleiche Ereignis generiert werden. Um dies zu vermeiden, müssen die Filter so entworfen werden, das sie sich gegenseitig ausschließen.

7 Trap-Weiterleitung

Der Trap Forwarder ist dafür zuständig, das OpenScape FM Ereignisse in SNMP-Traps konvertiert. Diese Traps können zu einem oder mehreren SNMP Trap-Empfängern versendet werden.

Der Trap Forwarder bietet als Voreinstellung ein einheitliches Trap-Format an, dieses kann aber durch den Anwender angepasst werden. Wird das einheitliche Trap-Format verwendet, so muss nur dieses auf dem Empfänger-System konfiguriert werden (z.B. Umbrella Management Plattform). Alle Ereignis-Daten der unterschiedlichen HiPath- und OpenScape-Technologien können so durch einen einzigen Trap-Typ repräsentiert werden.

Die Verwendung des Trap Forwarder erspart dem End-Anwender die Notwendigkeit, das Trap-Empfänger-System jedem einzelnen System zuweisen zu müssen, das Traps an das OpenScape FM versendet. Die Systeme versenden ihre Traps an das OpenScape FM, das Event Gateway sammelt alle relevanten Ereignisse, und der Trap Forwarder versendet sie zu einem oder mehreren Trap-Empfängern.

Die Standard SNMP MIB Definition des Trap Forwarder findet sich in *Anhang B, „SNMP Trap MIB Definition“*. Wenn nicht anders gewünscht werden eine Reihe von **Standard Trap Variablen Bindungen** gefolgt von Variablen-Bindungen aus dem Original-Trap versendet.

Die **Standard Trap Variablen Bindungen** sind:

- **IP-Adresse:** Diese Feld enthält eine IP-Adresse: Im Falle von HiPath 4000 Ereignissen (z.B. Alarm), ist dies die IP-Adresse des HiPath 4000 Managers. Im Falle von HiPath 3000 Ereignissen (weitergeleiteter HiPath 3000 Trap), ist dies die IP-Adresse des Ereignis auslösenden HiPath 3000 Systems. Handelt es sich um ein internes Ereignis, das durch das OpenScape FM erzeugt wurde, enthält das Feld die IP-Adresse des OpenScape FM Servers.
- **Priorität**: Ein Integer-Wert, der die Priorität repräsentiert, die dem Ereignis durch den OpenScape FM Server zugewiesen wurde (unknown(1), normal (2), warning (3), minor (4), major(5), critical(6), unmanaged (7), restricted(8), testing(9), disabled(10))
- **Objektname**: Der OpenScape FM Objektname des Objektes, dem das Ereignis zugeordnet wurde.
- **Datum**: Das Datum, zu dem das Ereignis im OpenScape FM empfangen wurde.
- **Kategorie**: Die Ereignis-Kategorie, die dem Ereignis im Ereignis-Browser zugewiesen wurde.
- **Meldung**: Eine Meldung, die das Ereignis wie im OpenScape FM zugewiesen beschreibt. Dies entspricht der Meldung im Ereignis-Browser.
- **Ereignistyp**: Ein Integer-Wert, der den Typ des Ereignisses repräsentiert. Wurde das Ereignis durch das Empfangen eines SNMP-Traps generiert, so ist der Ereignistyp snmp (2). Wurde das Ereignis intern im OpenScape FM generiert, so ist der Ereignistyp internal (1).
- **Source-IP**: Die IP-Adresse der Quelle, von der das Ereignis ursprünglich kam.
- **Source-Datum**: Das Datum, das von der Original-Quelle dem Ereignis zugeordnet wurde.
- **Ereignis-Schlüssel**: Ein String, um des inverse Ereignis zu identifizieren.
- **Enterprise-OID**: Die SNMP Enterprise OID, die ursprünglich dem Ereignis zugeordnet war.

- **Ereignis-ID**: Die ID des Ereignisses im Ereignis-Browser.

Zusätzlich zu diesem Standard-Verhalten bietet der Trap Forwarder die Möglichkeit, die Reihenfolge und/oder die Anzahl der zu sendenden Variablen des Traps zu verändern.

- Die Standard-Variablen-Bindungen können durch sogenannte **Zusätzliche Variablen** erweitert werden. Dies sind frei definierbare zusätzliche Trap-Variablen-Bindungen, die dem Trap durch den Anwender hinzugefügt werden können. In diesem Fall werden die Variablen-Bindungen der Original-Traps nicht mit dem Trap versendet. Die zusätzlichen Variablen-Bindungen werden auf der Karteikarte **Trap-Ziel-Parameter** konfiguriert.
- Das Versenden der Standard- und Original-Variablen kann unterdrückt werden. In diesem Fall werden nur die zusätzlichen Variablen versendet.

Auf diese Weise kann der Anwender seine eigenen Traps definieren. Dabei muss aber beachtet werden, dass in diesem Fall die Standard Trap Forwarder SNMP MIB Definition nicht mehr zutrifft. Das neue Trap Forwarder Trap-Format wird auf der **Trap-Ziel-Parameter** Karteikarte im Event Gateway Config Tool konfiguriert. Der Anwender muss das Format seines Traps im Zielsystem (z.B. Umbrella Management Tool) ebenfalls konfigurieren.

Die **Trap-Ziel-Parameter** Karteikarte findet sich im Event Gateway Config Tool. Es besteht aus zwei Teilen: die linke Seite enthält eine Liste der Trap-Empfänger. Die rechte Seite enthält die Parameter, die beim Versenden von SNMP Traps an den ausgewählten Empfänger verwendet werden sollen.

Trap-Ziel-Info: Hier werden alle definierten Trap-Empfänger aufgelistet.

Ziel: Der Empfänger des Traps. Der SNMP-Trap-Ziel-Name kann entweder ein Hostname oder eine IP-Adresse sein, die der Maschine bekannt ist, auf der das OpenScape FM Event Gateway läuft.

Port: Der Remote-Port zu dem der SNMP-Traps gesendet wird.

Community: Der Community-String, der verwendet wird, um die SNMP-Traps an das gegebene Ziel zu senden.

Verbindung: Hier können ein oder mehrere Verbindungs-Einträge ausgewählt werden. Diese Verbindungen werden als Quelle verwendet. Alle Ereignisse, die durch diese Quellen empfangen werden, und die ihren Filter passieren, werden an das durch das Feld **Ziel** definierte Ziel versendet. Der Verbindungs-Eintrag wird auf der Karteikarte **Verbindungs-Parameter** konfiguriert.

PDU Typ: Der Typ der SNMP Protocol Data Unit, der verwendet werden soll. Dies kann entweder ein v1 Trap (`V1TRAP`), ein v2 Trap (`V2TRAP`), ein v2 Information Request (`V2INFORM`), ein v3 Trap (`V3TRAP`) oder ein v3 Information Request (`V3INFORM`) sein.

Sollen SNMPv3 Traps versendet werden, können in den entsprechenden Feldern die **SNMPv3 Sicherheitsstufe**, das **SNMP v3 Authentisierungsprotokoll** und das **SNMPv3 Verschlüsselungsprotokoll** ausgewählt werden. Die zugehörigen Passworte können in den Feldern **SNMPv3 Sicherheitsname**, **SNMP v3 Authentisierungspasswort** und **SNMPv3 Verschlüsselungspasswort** definiert werden.

Enterprise ID: Die Enterprise OID des zu versendenden Traps.
Standardmäßig wird die OID durch zwei Variablen definiert, um die Enterprise OIDs, wie sie in der Trap Forwarder MIB definiert sind, zu erstellen.
`mmpgwEventOIDs.severityinteger`
Die Variable `mmpgwEventOIDs` steht für den, in der Trap Forwarder MIB definierten, festen Anteil der OIDs. Sie stellt alle Zahlen der OID außer der letzten bereit:
`.1.3.6.1.4.1.192.6.3.1.1.4.1.2.0`

Die Variable `severityinteger` liefert die letzte Ziffer der OID. Diese Variable ändert sich in Abhängigkeit von der Priorität des Ereignisses, das den Trap ausgelöst hat.
Um eine OID für eine bestimmte Priorität zu generieren, werden die Variablen für die unterschiedlichen Prioritäten (wie z.B. `Minor` oder `Critical` (siehe *Tabelle 1*)) dem festen Teil der OID hinzugefügt.

Tabelle 1 Enterprise ID Variablen

Unset	0
Unknown	1
Normal	2
Warning	3
Minor	4
Major	5
Critical	6
Unmanaged	7
Restricted	8
Testing	9
Disabled	10

Standard Variablen weglassen: Ist diese Option ausgewählt, so werden ausschließlich die in den Feldern **Zusatz Variable** definierten Variablen mit dem Trap versendet.

Zusatz Variablen: Hier können bis zu zwanzig zusätzliche Variablen-Bindungen definiert werden. Diese werden dem Trap hinzugefügt. Das Werte-Feld darf Daten vom Typ Konstante, eine Variable, eine Kommando der Formatierungssprache (siehe *OpenScape FM Desktop Bedienungsanleitung*) oder eine Kombination davon enthalten. Ein Rechtsklick in eines der Felder öffnet ein Menü, das dabei hilft den Wert zu definieren. Wird ein Trap versendet, wird der Inhalt des Wert-Feldes ausgewertet, und dann dem Trap als zusätzliche String-Variable hinzugefügt.

8 Logging/Troubleshooting

8.1 Logging

Die Logdatei, die sich mit Ereignissen und Fehlern bzgl. des OpenScape FM Event Gateway Servers beschäftigt, findet sich im Verzeichnis `<installation_dir>/server/log/`. Die Datei hat den Namen `megServer.log`.

Die Logdatei, die sich mit Ereignissen und Fehlern bzgl. des Gateway Config Tools beschäftigt, findet sich im Verzeichnis `<installation_dir>/client/log/`. Die Datei hat den Namen `megGui.log`.

Immer wenn eine Komponente (Server oder Config Tool) gestartet wird, oder wenn ein Logfile `<LogfileName>.log` eine Größe von 10 MB erreicht, so wird die Datei `<LogfileName>.log.old` nach `<LogfileName>.log.older` gesichert, und die Datei `<LogfileName>.log` nach `<LogfileName>.log.old`.

Im Falle eines Problems ist es eine gute Idee. in diesen Dateien nach Hinweisen auf das Problem zu untersuchen.

8.2 Troubleshooting

Falls Probleme bei der Arbeit mit dem Gateway auftreten, kann eventuell ein Blick in die Logdateien (siehe *Abschnitt 8.1, „Logging“*) helfen, um festzustellen welche Art Fehler aufgetreten ist.:

Problem	Mögliche Ursache	Lösung
Es wird angezeigt, dass keine gültige Lizenz verfügbar ist. Das Gateway wird nicht gestartet.	Die Lizenz wurde nicht richtig installiert	Das Gateway muss korrekt lizenziert werden, siehe *Abschnitt 3.1, „Installation“*
Operation timed out: connect oder *Connection refused to host: <hostname>*	Der OpenScape FM Server ist nicht konfiguriert oder läuft nicht	Die Verbindungs-Parameter müssen im Gateway Config Tool definiert werden (siehe *Abschnitt 3.1, „Installation“*) und der OpenScape FM Server muss gestartet sein.
Exception *invalid Authentication*	Ein ungültiger OpenScape FM Anwender wurde konfiguriert (falscher Login-Name oder Passwort)	Es muss ein gültiger Anwender und ein passendes Passwort in den Verbindungs-Parametern konfiguriert werden. Siehe *Kapitel 5, „Verbindungs-Parameter“*

Problem	Mögliche Ursache	Lösung
Die Konfiguration des Gateway Config Tool wurde nicht gesichert, beim Neustart des Gateway Config Tool wird die alte Konfiguration angezeigt.	Die Konfiguration wurde nicht gespeichert, als das Gateway Config Tool geschlossen wurde.	Es ist sicherzustellen, dass das Speichern bestätigt wird, bevor das Gateway Config Tool beendet wird, siehe *Kapitel 4, „Allgemeine Konfiguration“*
Ereignis <in> has no license (EVENT_EXCEEDED) oder *Event <id> has no license (EXPIRED)*	Nicht genügend Lizenzen verfügbar	Die Lizenz muss entsprechend erweitert werden
Event <id> has no license (IP Node Grace Period EXPIRED) oder *Event <id> has no license (Port Grace Period EXPIRED)*	Nicht genügend Lizenzen verfügbar	Die Lizenz muss entsprechend erweitert werden

9 Konfigurations-Beispiel

Dieses Kapitel enthält einige bespielhafte Konfigurationen des Gateway für Szenarien mit spezifischen Anforderungen.

9.1 Scenario: Versenden spezifischer Ereignisse als Trap

9.1.1 Vorbedingung

In diesem Scenario sollen nur 'Major' HiPath 4000 Ereignisse mit den folgenden Alarm-Gruppen/-Klassen als SNMP-Trap an die Umbrella Management Plattform der Firma weitergeleitet werden: 3/1, 3/2, 3/3 und 3/4.

9.1.2 Konfiguration des OpenScape FM

Im OpenScape FM ist keine Konfiguration notwendig.

9.1.3 Konfiguration des Trap Forwarder

Zunächst muss eine Eingangs-Verbindung definiert werden. Aus der Karte **Verbindungs-Parameter** muss die Schaltfläche **Erstellen** betätigt werden, um einen neuen Eintrag zu erzeugen. Für den neuen Eintrag sind die folgenden Felder notwendig:

- **Verbindungs-Name**: Hier muss der Name der Verbindungs-Konfiguration eingetragen werden. Z.B. in der folgenden Syntax `<user>@<OpenScape FM server>/<connection type>`. In unserem Beispiel wählen wir den Namen `root@pulsar/PSAccount`
- **Host-Name**: Der Name des OpenScape FM Servers. In unserem Beispiel wählen wir den Server „pulsar“.
- **Benutzer**: Der Name des OpenScape FM Anwenders, mit dem sich der Trap Forwarder mit dem OpenScape FM verbinden soll. In diesem Beispiel verwenden wir den Anwender „`root`“.
- **Passwort, Passwort erneut eingeben**: Das Passwort des ausgewählten OpenScape FM Anwenders.
- **Verbindung**: Hier muss der Verbindungs-Typ ausgewählt werden. Im Falle des Beispiels wählen wir den Typ *PSAccount*.

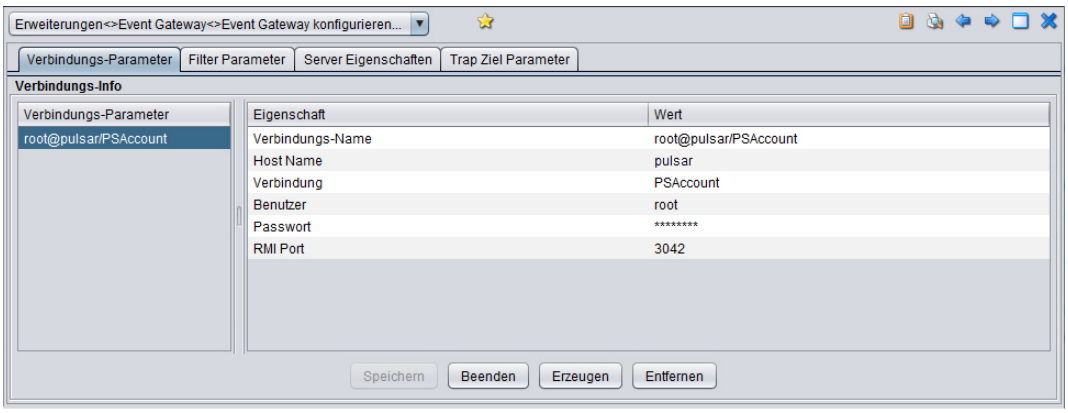

Bild 3 Verbindungs-Parameter

Als nächstes definieren wir einen Filter für diese Verbindung. Dazu wechseln wir auf die Karte **Filter Parameter** und wählen aus der Liste die gerade erstellte Verbindung aus. Unser Filter besteht aus fünf Filter-Ausdrücken, also betätigen wir die Schaltfläche Erzeugen fünf Mal, um fünf Zeilen in der rechten Liste zu erhalten. Der erste Filter-Ausdruck überprüft, ob die Enterprise OID zu einem HiPath 4000 Alarm gehört. Die anderen vier Ausdrücke überprüfen, ob die gewünschten Gruppen und Klassen empfangen wurden.

Wir beginnen mit dem ersten Filter-Ausdruck. Die Enterprise OID eines Traps findet sich in der Trap Forwarder Variablen `${enterpriseid}`.

Die Enterprise ID eines HiPath 4000 major on Alarms sieht wie folgt aus:
`.1.3.6.2.4.1.231.7.2.1.21.2.2.30`

Die Enterprise ID eines HiPath 4000 major off Alarms sieht wie folgt aus:
`.1.3.6.2.4.1.231.7.2.1.21.2.2.31`

Sie unterscheiden sich in der letzten Stelle. Wir benötigen also einen Ausdruck, bei dem das letzte Element eine Beliebiges sein kann. Dies kann mit einem regulären Ausdruck erreicht werden. Ein beliebiges Zeichen wird durch „`.*`“ symbolisiert. Da „`.`“ ein spezifisches Symbol in regulären Ausdrücken ist, müssen die anderen „`.`“ escaped werden. In unserem Beispiel sieht der Ausdruck wie folgt aus:

```
${enterpriseid} ~ \.1\.3\.6\.2\.4\.1\.231\.7\.2\.1\.21\.2\.2.*
```

Dies ist unser erster Filter-Ausdruck.

Die folgenden Filter-Ausdrücke sollen überprüfen, ob es sich um einen Major-Alarm einer der folgenden Alarm-Gruppen-/-Klassen-Kombinationen handelt 3/1, 3/2, 3/3 oder 3/4. Für HiPath 4000 Alarme enthält die zweite Trap-Variable die Alarm-Gruppe, die dritte Variable die Alarm-Klasse, und die vierte Variable die Priorität (2=major, 1=minor, 3=device). Dieses Wissen erlaubt es einen Ausdruck zu definieren, der für die Alarm-Gruppen/Klassen-Kombination 3/1 wir folgt aussieht. Die ’2’ am Ende überprüft, ob es sich um einen Major-Alarm handelt. Das „`/`“ dient als Separator für die einzelnen Werte:

```
${var[2]}/${var[3]}/${var[4]}=3/1/2
```

Nun müssen weitere Ausdrücke für die anderen Alarm-Gruppen/-Klassen-Kombinationen definiert werden. Schließlich sieht unser Filter wie in der folgenden Abbildung aus:

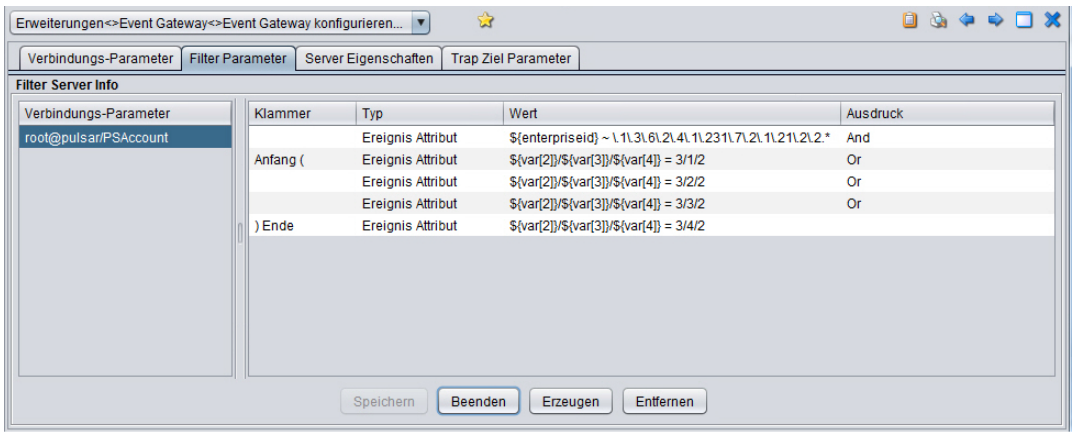

Bild 4 Filter-Konfiguration

Zuletzt konfigurieren wird das Trap-Ziel. In diesem Beispiel heißt das System, dass die Traps empfangen soll „umbrella_mgmt“. Sein SNMP-Agent lauscht auf Port 162. Wir wechseln auf die Karte **Trap-Ziel-Parameter** und betätigen die **Erzeugen** Schaltfläche. Im neuen Eintrag werden die folgenden Felder gefüllt:

Ziel: Hier muss der Hostname oder die IP-Adresse des Trap-Empfängers eingetragen werden. In unserem Beispiel „`umbrella_mgmt`“.

Port: Der Port auf dem der SNMP-Empfänger lauscht. In unserem Beispiel ist es der Standard-Wert 162.

Community: Hier muss die Community eingetragen werden, unter der die SNMP-Traps versendet werden sollen.

Verbindung: Hier muss die Eingangs-Verbindung für unsere Ereignisse ausgewählt werden. Wir wählen wie zuvor definiert „`root@pulsar/PSAccount`“.

Die anderen Felder können leer gelassen oder mit ihren Voreinstellungen belassen werden.

Schließlich muss die Konfiguration mit der Schaltfläche **Speichern** gespeichert werden.

Konfigurations-Beispiel

Scenario: Versenden spezifischer Ereignisse als Trap

A System-Voraussetzungen

Der Event Gateway ist Teil der OpenScape FM Installation.

Die notwendigen System-Voraussetzungen finden sich in der *OpenScape FM Desktop Bedienungsanleitung*.

B SNMP Trap MIB Definition

```
MATERNA-MIB { iso org(3) dod(6) internet(1) private(4) enterprises(1) 192 }

DEFINITIONS ::= BEGIN

IMPORTS
    DisplayString
        FROM RFC1213-MIB
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
    Counter32, Integer32 ,IpAddress
        FROM SNMPv2-SMI
    OBJECT-GROUP
        FROM SNMPv2-CONF;
--    TruthValue
--        FROM SNMPv2-TC;
--    TRAP-TYPE
--        FROM RFC1215

manager MODULE-IDENTITY
    LAST-UPDATED    "0010061600+0100"
    -- last updated by glodde
    -- changes made:
    --  o definition of trap format for snmp forwarding

    ORGANIZATION "Materna GmbH Information and Communications BUI/NSM"
    CONTACT-INFO
        "Georg Lodde
        Vosskuhle 37
        44147 Dortmund
        Tel.:   +49 231 5599 203
        Fax.:   +49 231 5599 100
        E-mail:   Georg.Lodde@Materna.De"
    DESCRIPTION
        "This is the MIB module for the mmp gateway trap forwarder.
         It describes the SNMP trap format which is send to a nother ip system

         (trap receiver)."
    ::= { nsm 1 }

materna                 OBJECT IDENTIFIER ::= { enterprises 192 }
maternaProducts         OBJECT IDENTIFIER ::= { materna 1 }
maternaSystem           OBJECT IDENTIFIER ::= { materna 2 }
maternaMibs             OBJECT IDENTIFIER ::= { materna 3 }
maternaExperimental     OBJECT IDENTIFIER ::= { materna 4 }
maternaUnits            OBJECT IDENTIFIER ::= { materna 6 }
bui                     OBJECT IDENTIFIER ::= { maternaUnits 3 }
nsm                     OBJECT IDENTIFIER ::= { bui 1 }
ipm                     OBJECT IDENTIFIER ::= { manager 1 }
application             OBJECT IDENTIFIER ::= { manager 2 }
ers                     OBJECT IDENTIFIER ::= { manager 3 }
mmpgw                   OBJECT IDENTIFIER ::= { manager 4 }
```

```
-- this mib consists of the following subtrees/groups
mmpgwEventGroup        OBJECT IDENTIFIER ::= { mmpgw 1 }
mmpgwEventVars        OBJECT IDENTIFIER ::= { mmpgwEventGroup 1 }
mmpgwEventOIDs        OBJECT IDENTIFIER ::= { mmpgwEventGroup 2 }

-- The mmp gw event variable Group
-- There is no SNMP agent implementing the variables in a MIB.
--


ipaddress OBJECT-TYPE
    SYNTAX    IpAddress
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "This field contains an IP-Address:
             In case of a HiPath 4000 event (e.g. alarm), this will be the
         IP-Address of the HiPath 4000 Manager.
         In case of a HiPath 3000 event (forwarded HiPath 3000 trap), this
         will the the IP-Address of the event originating HiPath 3000
         system.
         If the event is an internal event, generated by the OpenScape FM,
         this field will contain the Ip-Address of the OpenScape FM server."
    ::= { mmpgwEventVars 1 }

severity OBJECT-TYPE
    SYNTAX    INTEGER {  unknown(1), normal (2), warning (3), minor (4),
              major(5), critical(6), unmanaged (7), restricted(8),
              testing(9), disabled(10)}
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "The severity assigned to the event. "
    ::= { mmpgwEventVars 2 }

objectname OBJECT-TYPE
    SYNTAX    DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "The name of the object in the OpenScape FM database to which
         the event is assigned.
         A HiPath 4000 object name is set up as follows:
         Hicom300:<IpAddressHiPath4000Manager>:<MnemonicHiPath4000>.
         MnemonicHiPath4000 represents the mnemonic name of the related
         HiPath 4000 switch.
         A HiPath 3000 object name has the structure:
         H150e:<IpAddressHipath3000>.
         IpAddressHipath3000 represents the IP-Address of the event
         originating HiPath 3000 /Hicom 150 switch.
    ::= { mmpgwEventVars 3 }

date OBJECT-TYPE
    SYNTAX    DateAndTime
    MAX-ACCESS    not-accessible
    STATUS    current
```

```
    DESCRIPTION
        "The date when the event was received by the OpenScape FM."
    ::= { mmpgwEventVars 4 }

category OBJECT-TYPE
    SYNTAX    DisplayString
    MAX-ACCESS not-accessible
    STATUS    current
    DESCRIPTION
        "The event category to which the event is assinged.
         Exampels: HiPath 3000/5000, HiPath 4000, IP Manager,
         HiPath MIB HIA, HiPath MIB HMH, HiPath MIB HMP.
         Traps of Hicom 150 systems are assigned to the category HiPath
         3000/5000 too.
         Traps of Hicom 300 systems are assigned to the category HiPath
         4000."
    ::= { mmpgwEventVars 5 }

message OBJECT-TYPE
    SYNTAX    DisplayString
    MAX-ACCESS not-accessible
    STATUS    current
    DESCRIPTION
        "The message describing the event as assigned by the OpenScape FM
        (see OpenScape FM event browser, field Description)."
    ::= { mmpgwEventVars 6 }

eventType OBJECT-TYPE
    SYNTAX    INTEGER {  internal(2), snmp (3)) }
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "The type of event. If the event was generated due to the reception
        of an SNMP trap the eventType will be snmp. If the event was
        generated internal in the OpenScape FM, the event type will be
        internal."
    ::= { mmpgwEventVars 7 }
-- Events

sourceIp OBJECT-TYPE
    SYNTAX    IpAddress
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "The ip address of the source from which the event was send originally. "
    ::= { mmpgwEventVars 8 }

sourceDate OBJECT-TYPE
    SYNTAX    DateAndTime
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "The date which was assigned to the event by the original source. "
    ::= { mmpgwEventVars 9 }

eventKey OBJECT-TYPE
```

```
    SYNTAX    DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "A string to identify inverse events. "
    ::= { mmpgwEventVars 10 }

enterprise OBJECT-TYPE
    SYNTAX    OBJECT IDENTIFIER
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "A enterprise id assigned to the event. "
    ::= { mmpgwEventVars 11 }

eventId OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwEventVars 12 }

additionalVar1 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 1 }

additionalVar2 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 2 }

additionalVar3 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 3 }

additionalVar4 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 4 }

additionalVar5 OBJECT-TYPE
```

```
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 5 }

additionalVar6 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 6 }

additionalVar7 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 7 }

additionalVar8 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 8 }

additionalVar9 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 9 }

additionalVar10 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 10 }

additionalVar11 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 11 }

additionalVar12 OBJECT-TYPE
```

```
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 12 }

additionalVar13 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 13 }

additionalVar14 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 14 }

additionalVar15 OBJECT-TYPE
    SYNTAX    INTEGER
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 15 }

additionalVar16 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 16 }

additionalVar17 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 17 }

additionalVar18 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 18 }

additionalVar19 OBJECT-TYPE
```

```
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 19 }

additionalVar20 OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS    not-accessible
    STATUS    current
    DESCRIPTION
        "An additional optional event variable. "
    ::= { mmpgwAdditionalVars 20 }

-- Events

mmpgwEventUnknown NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
             "This trap is generated to forward an event with unknown severity as
              represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 1 }

mmpgwEventNormal NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
             "This trap is generated to forward an event with normal severity as
              represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 2 }

mmpgwEventWarning NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
             "This trap is generated to forward an event with warning severity as
              represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 3 }

mmpgwEventMinor NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
             "This trap is generated to forward an event with minor severity as represented
              in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 4 }

mmpgwEventMajor NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
```

```
    STATUS  current
    DESCRIPTION
            "This trap is generated to forward an event with major severity as represented
             in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 5 }

mmpgwEventCritical NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
            "This trap is generated to forward an event with critical severity as
             represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 6 }


mmpgwEventUnmanaged NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
            "This trap is generated to forward an event with unmanaged severity as
             represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 7 }

mmpgwEventRestricted NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
            "This trap is generated to forward an event with restricted severity as
             represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 8 }

mmpgwEventTesting NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
            "This trap is generated to forward an event with testing severity as
             represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 9 }

mmpgwEventDisabled NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
    DESCRIPTION
            "This trap is generated to forward an event with disabled severity as
             represented in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 10 }

mmpgwEventUnset NOTIFICATION-TYPE
    OBJECTS { ipaddress, severity, objectname, date, category, message, eventType,
    sourceIp, sourceDate, eventKey, enterprise, eventId }
    STATUS  current
```

```
    DESCRIPTION
             "This trap is generated to forward an event with unset severity as represented
              in the OpenScape FM event browser, to a trap receiver."
    ::=  { mmpgwEventOIDs 0 }

mmpgwLicenseViolation NOTIFICATION-TYPE
    OBJECTS { message }
    STATUS  current
    DESCRIPTION
             "This trap is generated when the license of the MATERNA Event Gateway is
             violated."
    ::=  { mmpgwEventOIDs 100 }
END
```

C Variablen

Die folgenden Variablen können auf den Seiten Filter und Trap Parameter verwendet werden. Entweder als Teil der Ausgabe-Werte oder als Teil einer Abfrage oder Bedingung.

C.1 Basis Variablen

Diese Variablen können immer verwendet werden:

- `${enterpriseid}`: Die mit dem Ereignis verbundene Enterprise ID.
- `${date}`: Das Datum der Ereignisses im String-Format. Diese Variable verwendet die lokale Zeitzone.
- `${time}`: Die Zeit des Ereignisses im String-Format. Diese Variable verwendet die lokale Zeitzone.
- `${datetimeseconds}`: Der Zeitpunkt zu dem das Ereignis aufgetreten ist. Die Zeit wird in Sekunden seit Mitternacht des 1. Januar 1970 angegeben.
- `${datetimemillis}`: Der Zeitpunkt zu dem das Ereignis aufgetreten ist. Die Zeit wird in Milli-Sekunden seit Mitternacht des 1. Januar 1970 angegeben.
- `${currentTime}`: Die aktuelle Zeit im Milli-Sekunden seit dem 1.1.1970.
- `${WEEK}`: Eine Woche in Milli-Sekunden.
- `${DAY}`: Ein Tag in Milli-Sekunden.
- `${HOUR}`: Eine Stunde in Milli-Sekunden.
- `${MINUTE}`: Eine Minute in Milli-Sekunden.
- `${SECOND}`: Eine Sekunde in Milli-Sekunden.
- `${category}`: Die Ereignis-Kategorie, wie sie im OpenScape FM Ereignis-Browser angezeigt wird.
- `${severity}`: Die Priorität (severity) des Ereignisses (entweder ’minor’, ’major’ oder ’device’)
- `${severityinteger}`: Die Priorität (severity) des Ereignisses (entweder 0 (minor), 1 (major) oder 2 (device)
- `${eventid}`: Die eindeutige ID des Ereignisses.
- `${acknowledged}`: Diese Variable gibt an, ob das Objekt, das im OpenScape FM mit dem Ereignis verbunden ist, bestätigt oder unbestätigt ist. Der Wert ist entweder ’true’ oder ’false’.
- `${flashing}`: Diese Variable ist ’true’ wenn das Ereignis das im OpenScape FM zugeordnete Objekt zum Blinken bringt. Ansonsten ’false’.
- `${source}`: Der Quellenname des Objektes, das mit dem Ereignis verbunden ist.
- `${description}`: Eine Beschreibung des Ereignisses (Ereignis-Browser-Text).
- `${label}`: Der Bezeichner des Objektes, das mit dem Ereignis verbunden ist.

- `${eventkey}`: Der Schlüssel, der verwendet wird, um das inverse Ereignis zu identifizieren. Der Schlüssel hängt von der Technologie ab, und wird nicht für alle Technologien bereit gestellt.
- `${requestid}`: Die AR Ticket-Nummer des letzten Tickets, das zu einem Ereignis mit dem gleichen Request-ID-Schlüssel gehört.
- `${sourceip}`: Die IP-Adresse der Quelle, die das Ereignis ausgelöst hat (z.B. die IP-Adresse eines Managers).
- `${serverIp}`: Die IP-Adresse des OpenScape FM, welches das Ereignis bereitgestellt hat.
- `${var.length}`: Die Anzahl der Trap-Variablen, die im Ereignis-Trap enthalten sind.
- `${var[0]}-${var[9]}`: Der Inhalt der Trap-Variablen des Ereignis-Traps. Hier werden die Variablen 0 .. 9 angeboten. Verfügt der Ereignis-Trap über mehr als 10 Variablen, können diese entsprechend frei eingegeben werden.

C.2 Enterprises

- `${HiPath4000MajorAlarmOn}`: Die Enterprise ID eines HiPath 4000 Major Alarm On Traps.
- `${HiPath4000MajorAlarmOff}`: Die Enterprise ID eines HiPath 4000 Major Alarm Off Traps.
- `${HiPath4000MinorAlarmOn}`: Die Enterprise Id eines HiPath 4000 Minor Alarm On Traps.
- `${HiPath4000MinorAlarmOff}`: Die Enterprise Id einesHiPath 4000 Minor Alarm Off Traps.
- `${HiPath4000DeviceAlarmOn}`: Die Enterprise ID eines HiPath 4000 Device Alarm On Traps.
- `${HiPath4000DeviceAlarmOff}`: Die Enterprise ID eines HiPath 4000 Device Alarm Off Traps.
- `${HiPath3000Trap}`: Die Enterprise ID eines HiPath 3000 Traps.
- `${OpenScapeVoiceOIDTreePrefix}`: Der Prefix des OpenScape Voice OID Baumes (1.3.6.1.4.1.4329.2.18.2.2.1.47).
- `${HiPathMIBHiPathHostUp}`: Die Enterprise ID eines HiPath MIB Host Up Traps.
- `${HiPathMIBHiPathHostDown}`: Die Enterprise ID eines HiPath MIB Host Down Traps.
- `${HiPathMIBHiPathHostStatusChange}`: Die Enterprise ID eines HiPath MIB Host Status Change Traps.
- `${HiPathMIBHiPathApplicationInstalled}`: Die Enterprise ID eines HiPath MIB Application Installed Traps.
- `${HiPathMIBHiPathApplicationDeinstalled}`: Die Enterprise ID eines HiPath MIB Application Dienstalled Traps.
- `${HiPathMIBHiPathApplicationStatusChange}`: Die Enterprise ID eines HiPath MIB Application Status Change Traps.
- `${HiPathMIBHiPathProcessUp}`: Die Enterprise ID eines HiPath MIB Process Up Traps.

- `${HiPathMIBHiPathProcessDown}`: Die Enterprise ID eines HiPath MIB Process Down Traps.
- `${HiPathMIBHiPathProcessStatusChange}`: Die Enterprise ID eines HiPath MIB Process Status Change Traps.

Die exakte Enterprise ID findet sich in der Datei `enterprises.properties` im Installations-Verzeichnis des OpenScape Event Gateway Servers: `<Event Gateway installation directory>/server/resources/macros`.

D Glossar

API: Application Programming Interface. Eine Sammlung von Funktionen, die es einem Anwendungs-Programmierer ermöglichen, auf die Funktionalität eines Produktes zuzugreifen.

OpenScape FM: OpenScape Fault Management, die Unify Umbrella Management Plattform für die OpenScape Enterprise Convergence Architecture. Eine Web basierte Client/Server-Lösung für die Überwachung integrierter Netzwerke aus PBX, IP und VoIP Geräten.

JVM: Java Virtual Machine, eine Betriebs-System spezifische Software, die benötigt wird, um auf einem Computer ein Java Programm auszuführen. Die JVM übersetzt (universell) Java-Code im Maschinensprache.

Event Gateway Config Tool: Das Event Gateway Configuration Tool wird verwendet um das Event Gateway zu konfigurieren.

ECE: Event Correlation Engine, ein Zusatz-Modul für das OpenScape FM, das verwendet wird um Ereignisse auszuwerten.

Stichwörter