Integrated Server Monitoring

Die Management-Station

© Wilhelm Buchholz, Im Bruche 6, 31275 Lehrte

http://www.monitor-site.de

mailto:new-monitoring@t-online.de

Inhalt

1. Einleitung

Das vorliegende Überwachungssystem besteht aus drei Komponenten:

- Autonome Agenten auf den zu überwachenden Servern (Nodes): Meldungen werden zur Management-Station geschickt
- SNMP-Traps bzw. Notifications: Meldungen werden zur Management-Station geschickt
- Aktive Überwachung von Services: Die Sockets entfernter Server werden von der Management-Station aus unter Benutzung des Netzwerkes geprüft

Es handelt sich um ein text basierendes und eventgesteuertes System mit graphischer Bedienoberfläche.

Die Management-Station hat die folgenden Aufgaben:

- Empfang der Meldungen von den Agenten der Nodes
- Empfang der SNMP-Traps der Nodes und anderen Netzwerkkomponenten
- Darstellung der Meldungen mit X11 und WEB
- Weiterleitung von Meldungen per SMTP-Mails und/oder durch Export
- Einstellung des Systems durch die Administratoren

Die kombinierte Aufgabenstellung wird mit verschiedenen Hintergrundprozessen, mit einer X11-Oberfläche und einer Web-Oberfläche wahrgenommen. Ferner gibt es verschiedene Utility-Funktionen. Die Management-Station ist bestimmt für das Betriebssystem Linux 64 Bit.

2. Event Browser (X11): zentr. Darstellung der Meldungen

Hier findet - neben der Web-Oberfläche - die zentrale Ausgabe des Systems statt. Ein Benutzer - Administrator oder Operator - muss sich vorher mit Benutzerkennung und Passwort anmelden.

Die Meldungen werden tabellarisch dargestellt. Die neuste Meldung erscheint in der Standardeinstellung am oberen Ende der Tabelle. In der Voreinstellung sieht man die aktiven Meldungen. Ein Administrator sieht alle Meldungen, ein Operator nur diejenigen, deren Gruppe(n) ihm vom Administrator zugeteilt wurden.

Das Programm benötigt für die verschlüsselte Kommunikation mit den Agenten die Datei "monitorkeys.sig", die entweder im gleichen Verzeichnis wie das ausführbare Programm oder im Home-Verzeichnis des Benutzers oder im Verzeichnis "/etc" liegt. Die Signatur der Datei wird zu Beginn des Betriebes festgelegt und im Weiteren nicht mehr verändert.

Eine Meldung hat die folgenden Attribute:

- OrMaEx: Zeigt an, ob ein originaler Event Text vorliegt; zeigt ferner an, ob die Meldung exportiert und/oder mit einer Mail weitergeleitet wurde; wenn die Weiterleitung fehlgeschlagen ist, erscheint der Buchstabe 'E' in roter Farbe; bei Erfolg erscheint der Buchstabe 'X'
- Sev.: Severity, Meldungsschwere ("inform", "minor", "warning", "major", "critical"), farbliche Darstellung der Meldungsschweren
- Date/Time: Empfangszeit (Datum und Uhrzeit) der Meldung
- Nodename: Angabe über die Herkunft einer Meldung; Netzwerk-Name der Meldungsquelle, bei Unix-Servern gemäß "uname -n"
- IP Address: IP-Adresse des absendenden Servers, weiteres Attribut zur Identifizierung der Herkunft einer Meldung, ipv4 oder ipv6
- Group: Meldungsgruppe, Attribut für die Mehrbenutzerfähigkeit
- Object: Object der Meldung, Attribut zur Differenzierung von Meldungen
- Event Type: Attribut zur Klassifizierung bezüglich Ursache und Herkunft einer Meldung; es wird vom System vergeben und kann nicht verändert werden; zusätzlich gibt es eine Darstellung für die Gesamtzahl der gefundenen Einträge sowie den dazugehörigen Zeitraum; Beispiel siehe unten
- RepCnt: Wiederholungszähler für gleiche oder ähnliche Meldungen; in eckigen Klammern daneben die Anzahl von unterdrückten Meldungen für dieses Event; die Angabe fehlt, wenn die Anzahl gleich Null ist; damit hat man eine Kontrolle über die Häufigkeit von Events
- Event Text: Text der Meldung für Diagnose und Fehlerbehandlung

In der Ansicht “History Event Browser“ gibt es anstelle der Spalte RepCnt die Spalte SupCnt, die die Anzahl der von dem entsprechenden Filter in einem Zeitraum unterdrückten Meldungen angibt.

Unterer Teil des Browsers:

Event Browser:

- Accept: Anerkennen einer oder mehrerer Meldungen, je nachdem ob man sie mit der Maus selektiert hat. Das System registriert die Uhrzeit des Anerkennens und den Namen des Administrators oder Operators, der die Meldung anerkannt hat. Man erhält die Information durch Doppelklick auf eine Meldung.
- Severities: Summe der Meldungsschweren, wie sie im aktiven Browser vorhanden sind.
- Popup critical event: Bei Aktivieren der Checkbox erscheint eine Meldung mit der Severity “critical“ zusätzlich in einem speziellen Fenster
- Popup major event: das gleiche geschieht bei einer Meldung mit der Severity “major“

Das Attribut Nodename muss eindeutig sein. Es kann bei den Agenten in den Konfigurationsdateien bei Bedarf gesetzt werden. Das Attribut IP Address wird nicht zum Vergleich mit anderen Meldungen herangezogen, kann aber operativ in Zusammenhang mit den Export-Funktionen verwendet werden.

Im oberen Teil des Fensters befinden sich die Pulldown-Menüs zur Einstellung des Systems.

Im Weiteren werden die Pulldown-Menüs des Browser erklärt.

- Actions: Für Administratoren und Operatoren
- Operators: Nur für Administratoren
- Groups: Nur für Administratoren
- SNMPTraps: Nur für Administratoren
- Services: Nur für Administratoren
- Filter: Nur für Administratoren
- Mails: Nur für Administratoren
- TimeFilter: Nur für Administratoren
- Export: Nur für Administratoren
- EcFilter: Nur für Administratoren
- NodesConfig: Für Administratoren und Operatoren

Beispiel für Darstellung von Event Type:

Logfile#10/2m30s

Die Zahl nach dem Zeichen ’#’ (10) ist die Gesamtzahl der Einträge, die in einem Zeitraum von 2 Minuten und 30 Sekunden für den betreffenden Filter gefunden worden sind (unabhängig davon, wie viele Einträge tatsächlich übertragen worden sind). Format für die Zeitangabe: Ns, Nm, NmKs, Nh, NhKm; s: Sekunde, m: Minute, h: Stunde, N,K: natürliche Zahl.

3. Actions (X11)

3.1 Event Browser

Anzeigen und erneuern der aktiven, unbearbeiteten Meldungen

3.2 History Event Browser Dialog

Durch dieses Untermenü hat man die Möglichkeit, nach anerkannten Meldungen anhand ihrer Attribute zu suchen. Das Suchergebnis wird tabellarisch im Browser dargestellt. Man kann das Ergebnis auch in eine Textdatei mit dem Namen seiner Wahl schreiben und dann weiterverarbeiten.

- Selection of period: Die Zeitangaben des Intervalls DateTime from und DateTime to beziehen sich auf die Empfangszeiten der Meldungen, wie sie im Browser als aktive Meldungen dargestellt wurden.
- Severity: Meldungsschweren, nach denen man sucht. In der Voreinstellung sind alle Meldungsschweren selektiert.
- Nodename (Reg.Exp.): Suche nach Rechnernamen; ist das Feld leer, bedeutet dies: Jeder Nodename
- Group (Reg.Exp.): Suche nach Meldungsgruppe; ist das Feld leer, bedeutet dies: Jede Gruppe
- Object (Reg.Exp.): Suche nach Object einer Meldung; ist das Feld leer, bedeutet dies: Jedes Object
- EventTypes: Auswahlbox für Event-Typ, “default“ bedeutet: Jeder Event-Typ
- Regular expression for Event Text: Suche nach Meldungstext durch *regular expression*; ist das Feld leer, bedeutet dies: Jeder Meldungstext
- Delta Latest Suppr. (hor): Selektiert Meldungen/Events, deren “Time Latest Suppression“ innerhalb der letzten, eingegebenen Stunde(n) ist. Die Operation ist nur für den Datenbereich im *shared memory* definiert.
- File name for download: Angabe des Dateinamens einer Textdatei, in die das Suchergebnis hineingeschrieben wird, pro Datensatz eine Zeile. Die Spalten jeder Zeile sind getrennt durch ein Semikolon ‘;‘. Die Länge der Datei ist begrenzt auf 500.000 Zeilen. Ist das Eingabefeld leer, unterbleibt die Operation.
- FileSelectionBox: Öffnen der grafischen Darstellung des Dateisystems, um einen Dateiname zu bestimmen
- Enter: Starten des Suchevorganges
- Cancel: Verlassen des Untermenüs

Mit der ESC-Taste lassen sich die Eingabefelder löschen (gilt für alle Masken).

3.3 History Event Browser

Erneuern der Anzeige mit den in History Event Browser Dialog eingegebenen Werten

3.4 Selected Events Dialog

Auswählen von Events der aktiven Meldungen

- Severity: Meldungsschwere
- Nodename (Reg.Exp.): Suchmuster für Nodename
- Group (Reg.Exp.): Suchmuster für Meldungsgruppe
- Object (Reg.Exp.): Suchmuster für Object
- Event Type: Auswahlbox für Event-Typ
- Regular expression for Event Text: Suchmuster für Meldungstext
- Enter: Ausführen der Selektion
- Cancel: Abbrechen der Funktion

3.5 Selected Events

Erneuern der Anzeige mit den in Selected Events Dialog eingegebenen Werten. Die Anzeige hat die gleichen Spalten wie der „Event Browser“.

3.6 Lifecheck

Auflisten der Nodes, die sich in der Überwachung befinden. Der Datenbestand liegt auf der Management-Station und kann deswegen jederzeit eingesehen werden. Die Steuermeldungen kommen von den Agenten basemonagent (Unix) bzw. winmonagent.exe (Windows).

List of nodes: Tabelle der Nodes

Die Tabelle hat die folgenden Spalten:

- Sev.: Höchste Meldungsschwere einer aktiven Meldung für den Node
- Nodename: Rechnername des Nodes
- IP Address: IP-Adresse des Nodes
- Group: Meldungsgruppe für den Node wie in den Agenten basemonagent bzw. winmonagent.exe vereinbart
- delta (sec): Zeigt an die Zeitdifferenz in Sekunden seit dem letzten Lebenszeichen und in runden Klammern das einzuhaltende zeitliche Limit, von

dem ab signalisiert wird; der Wert in runden Klammern ist die Summe aus Polling Interval und Alarm Offset.

- Polling Interval (sec): Polling Intervall der Standardüberwachung; bildet die Basis für das zeitliche Limit, bei dessen Überschreitung eine Ausnahmebehandlung stattfindet
- LifeSev.: Farbliche Darstellung der Zeitdifferenz. Je größer die Zeitdifferenz delta, desto länger hat sich der Server nicht gemeldet. Ist delta größer als das Limit, gibt es für diesen Node eine kritische Meldung. Nach dreimaliger Meldung im Abstand von 15 Minuten geht der Server in den Zustand „disabled“ über.
- Last Time: Zeitpunkt des letzten Lebenszeichens
- Date: Datum des letzten Lebenszeichens
- Alarm Offset (sec): Aufsatz in Sekunden für das zeitliche Limit, bis zu dem sich der Node spätestens melden muss
- Ping Offset (sec): Aufsatz in Sekunden für das zeitliche Limit, nach dessen Verstreichen ein Pingcheck durchgeführt wird
- Sysname/Release: Name und Release des Betriebssystems
- Daemon: Zeigt an, ob der Agent als Daemon betrieben wird oder nicht
- AutoRefresh: Die Liste wird automatisch aktualisiert
- Disabled Nodes: Umschalten auf die Tabelle der „disabled nodes“. Es sind die Server, die sich nach dreimaliger Signalisierung (ca. 90 Minuten) nicht gemeldet haben

Specification of node(s):

- Severity: Wahl der Severities für Meldungen im aktiven Browser
- Nodename (Reg.Exp.): Suche nach Rechnername mit *regular expressions*; ist das Feld leer, bedeutet dies: Jeder Nodename
- IP Address (Reg.Exp.): Suche nach IP-Adresse mit *regular expressions*; ist das Feld leer, bedeutet dies: Jede IP-Adresse
- Group (Reg.Exp.): Suche nach Gruppe mit *regular expressions*; ist das Feld leer, bedeutet dies: Jede Gruppe

Result: Anzahl der Nodes

- Nodes in display: Anzahl der gefundenen Server, die sich in der Anzeige befinden, die Zahl ist begrenzt auf 300
- Total: Gesamtzahl der gefundenen Nodes

Bearbeitungsmodus durch die Push-Button:

- Refresh: Aktualisieren der Liste
- EraseRefresh: Aktualisieren der Liste und Löschen der Suchfelder

- Delete: Löschen eines Nodes aus der Liste; nur für den Administrator
- DeleteAll: Im Modus disabled kann man alle Nodes löschen
- Quit: Verlassen der Maske ohne Änderung

3.7 LifecheckLimit

Einstellung der Schwellwerte für die Signalisierung, wenn Meldungen von einem Node ausbleiben

- Nodename: Eingabe von Namen des Nodes, Änderungen erfolgen nur für den Node
- Group: Eingabe Name einer Meldungsgruppe, Änderungen erfolgen für alle Nodes mit dieser Gruppe
- Alarm Offset (sec): Aufsatz in Sekunden für das Limit, ab dem die Alarmierung erfolgen soll
- Disable Alarm: Keine Signalisierung bei fehlendem Lebenszeichen
- Ping Offset (sec): Aufsatz in Sekunden für das Limit, ab dem ein Ping-Check erfolgen soll
- Disable Pingcheck: Ausschalten von Ping-Check
- Get Values: Holen der aktuellen Daten des Nodes, dessen Name unter Nodename eingegeben wurde
- Modify: Neue Werte für einen Node oder für eine Gruppe setzen
- Quit: Verlassen des Formulars ohne Änderung

3.8 Change password

Ändern des eigenen Passwortes für Administratoren und Operatoren

Es gibt die Eingabefelder:

- Old password: Eingabe des alten Passwortes (nur bei Operatoren)
- New password: Eingabe des neuen Passwortes
- Confirm new password: Bestätigung des neuen Passwortes
- Enter: Abschicken der Änderung
- Quit: Verlassen der Funktion ohne Änderung

3.9 Database

Hier wird die Auslastung der Archivdatei und des Shared Memory für die Meldungen angezeigt. Außerdem sieht man jeweils die Empfangszeiten des ersten und des letzen Datensatzes.

3.10 Reduce Archive

Verkürzen der Archiv-Datei durch Löschen der ältesten Datensätze. Man kann nur dann löschen, wenn die Archiv-Datei größer ist als der Datenbestand im Shared Memory für die Events.

Es gibt die Eingabefelder:

- Date of oldest record: Angabe eines Datums, bis zu dem alle älteren Datensätze gelöscht werden
- Delete N count oldest records: Anzahl der ältesten Datensätze, die gelöscht werden sollen

3.11 Noscroll

Einstellung für Scrollen oder nicht Scrollen; bei Scrollen springt der Fokus nach Erscheinen einer neuen Meldung zum Anfang der Tabelle, also nach oben oder unten; gilt nur für aktive Events

3.12 BoldSelect

Die selektierte Zeile wird fettgedruckt

3.13 UpsideDown

Umkehrung der zeitlichen Reihenfolge in der Liste der Meldungen; in der Voreinstellung steht die neueste Meldung oben

3.14 System

Anzeigen der Hintergrundprozesse auf der Management-Station mit den Start-/Stoppzeiten und der Prozess-Id

4. Operators (X11)

4.1 Processing: Bearbeiten der Operatoren bzw. Administratoren

Einrichten, Ändern, Löschen, Reports von Operatoren und Administratoren

List of operators: Liste der Operatoren und Administratoren. Es gibt die Spalte Admin, die kennzeichnet, ob ein Benutzer Admin-Rechte hat oder nicht.

Eingabe für Operatoren/Administratoren:

- Operator name: Name des Operators oder Administrators
- Password: Anfangspasswort für den Operator oder Administrator
- Check Box Adminpermission: Zuteilung von Administratorrechten
- Description: Beschreibende Angaben über den Benutzer
- Add: Hinzufügen eines Namens für Operator/Administrator. Der Name muss neu sein, ein bereits existierender Benutzername wird abgewiesen.
- Modify: Ändern eines Benutzers
- Search: Suchen nach Namen von Operatoren/Administratoren.
- Delete: Löschen eines Namens. Der Name muss zuerst selektiert werden.
- Quit: Verlassen der Maske ohne Änderung

4.2 Operators,Groups

Zuweisung Gruppen zu Operatoren und Umkehrfunktion

Es erscheinen drei Listboxen mit:

- Operators: Liste aller Operatoren (nicht Administratoren)
- All groups: Liste der Gruppen
- Groups for: <operatorname>: Listbox für die zugeteilten Gruppen

Zuerst selektiert man einen Operatornamen. Dann kann man aus der mittleren Listbox (alle Gruppen) jeweils eine Gruppe mit Hilfe eines Push-Button in die rechte Listbox befördern.

Die Umkehrfunktion - das Deselektieren einer Gruppe von einem Operator - geschieht folgendermaßen:

Zuerst selektiert man den Operator. Man sieht in der rechten Listbox die zugewiesenen Gruppen. Davon kann man eine selektieren. Danach betätigen des Push-Button Delete.

Es gibt die Push-Button:

- ->: Nach Selektion aus der mittleren Listbox anhängen an die Liste der zugewiesenen Gruppen
- Enter: Abschluss einer Zuweisung
- Delete: Nach Selektion aus der rechten Listbox löschen aus der Zuweisung
- Quit: Verlassen der Maske

5. Groups (X11)

Einrichten, Ändern, Löschen, Reports von Gruppen.

List of groups: Liste der bestehenden Datensätze für Gruppen; das Selektieren eines Datensatzes geschieht durch Mausklick auf die linke Spalte (Groups) einer Zeile. Die Spalte Opcount zeigt an, wie viele Operatoren dieser Gruppe zugeordnet sind.

Input group:

- Group name: Eingabe eines Gruppennamens oder Echo eines selektierten Gruppennamens aus der Liste der Gruppen
- Description: Beschreibung der Gruppe
- Add: Hinzufügen einer Gruppe. Der Name muss neu sein, ein bereits existierender Gruppenname wird abgewiesen.
- Search: Suchen nach Gruppennamen
- Delete: Löschen eines Gruppennamens. Der Name muss zuerst selektiert werden.
- Quit: Verlassen der Maske ohne Änderung

6. SNMP-Traps (X11)

Hier findet die Einstellung der Signalisierung mit SNMP-Traps (*Notifications*) statt, die von dem Trap Receiver snmptraplistener (siehe unten) empfangen werden. Die Einstellung kann nur ein Administrator vornehmen.

6.1 Processing

List of trap specifications: Liste der bestehenden Datensätze für die Handhabung der SNMP-Traps; zwei Push-Button Up, Down zum Umordnen der Liste; das Selektieren eines Datensatzes geschieht durch Mausklick auf die linke Spalte (Community String) einer Zeile.

Bei dem Empfang eines Traps wird die bestehende Liste zum Vergleich durchlaufen. Ist bei einem Listenelement der Vergleich positiv, erscheint der Trap mit den angegebenen Spezifikationen und es endet der Listendurchlauf. Es kommt somit auf die Reihenfolge der Listenelemente an.

Traps/Notifications der Version 3 (SNMP-v3) dürfen nicht verschlüsselt sein.

Specification Snmp Trap: Eingabefelder zur Bestimmung des ankommenden Traps

- Community String/Username: Eingabe Community String für Version 1, 2c oder Username (*securityUser*) für Version 3; keine Eingabe: jeder Community String oder Username trifft
- Nodename: Angabe des Nodenames. Der hier eingegebene Name muss eindeutig sein. Wenn dieses Feld leer ist, vergibt das System den DNS-Namen, der sich aus der Auflösung der Absende-IP-Adresse ergibt. Ist eine Auflösung nicht möglich, erscheint als Hostname der Text unresolved::<ip adresse>; gilt für Version 2c und 3, Version 1 siehe unten
- IP Address (Reg.Exp.): Vergleich der eingegebenen IP-Adresse als Suchmuster für die IP-Adresse des Absenders des Traps. Ist das Feld leer, bedeutet dies: Jede IP-Adresse
- Generic Trap: ComboBox für Generic Trap 0..5
- Enterprise Specific Trap: Eingabe Zahlenwert für die enterprise specific trap id
- Object Identifier (OID): Eingabe numerische OID oder Teil einer OID, die mit der OID eines ankommenden Traps verglichen wird, keine Eingabe: Jede OID eines empfangenen Traps
- Compare: ComboBox für Vergleichsoperatoren

- Threshold (Numeric Value): Zahlenwert für den Vergleich mit dem zu Object Identifier (OID) gehörenden Wert
- Trim: Shift nach links bis zu der unter Object Identifier (OID) eingegebenen numerischen OID, der Text vor der OID geht verloren
- Matching for Trap Text (Reg.Exp.): Vergleich des eingegebenen Textes als Suchmuster mit dem ankommenden Meldungstext in der Normalform. Ist das Feld leer, bedeutet dies: Jeder Text
- Suppress: CheckBox für Anzeige oder Unterdrückung der spezifizierten Trap-Meldung

Specification Event: Festlegung zur Ausgabe der Meldung

- Severity: ComboBox für Meldungsschwere (inform, minor, warning, major, critical), mit der die Meldung erscheinen soll
- Group (CommunityString|InputField): Vereinbarung der Meldungsgruppe: entweder der *community string* (v1, v2c) bzw. *secName* (v3) vom sendenden Server oder Eingabefeld auf der Management-Station; folgt der in das Feld eingegebenen Meldungsgruppe ein Sternchen '*', wird sie bei Bedarf ersetzt durch die in der Datenbasis für den Lifecheck unter der IP-Adresse stehenden Gruppennamen
- Object: Vereinbarung des Attributes "Object" der Meldung
- ShortName: CheckBox für die Wahl des Short-DNS-Namens; aus dem Namen "OTTO.firma.de" wird "OTTO"
- Accept: Trap-Meldung soll gleich in History-Datenbasis kommen
- Format Trap Text: Parametergesteuerter Ersetzungsmechanismus durch Formatstring; an dieser Stelle hat der Operator '$' gefolgt von einer Null "$0" die Bedeutung: Ausgabe von *Community String/secName*

Bearbeitungsmodus durch die Push-Button:

- Add: Hinzufügen eines Datensatzes
- Modify: Ändern eines Datensatzes
- Search: Suchen nach einem Datensatz
- Delete: Löschen eines Datensatzes. Die erste Spalte mit Nodename muss zuerst selektiert werden.
- LookUp: Ermittelt die zu Nodename gehörige IP-Adresse. Das Ergebnis erscheint in dem Feld IP Address (Reg.Exp.). Der Fokus der Eingabe muss auf dem Feld Nodename liegen. Umgekehrt kann man den zu IP Address (Reg.Exp.) gehörigen Rechnernamen erhalten.
- Quit: Verlassen der Maske ohne Änderung

Anmerkung zu Group (CommunityString|InputField): Mit der Wahl vom *community string* bzw. *secName* bestimmen die sendenden Server ihre Meldungsgruppe selber, ohne dass zusätzliche Tabelleneinträge notwendig sind, es findet eine dynamische Zuweisung statt. Die Vereinbarung auf den SNMP-Clients von *community string*/*secName* für *snmp notifications* (Port 162) geschieht unabhängig von SNMP-Abfragen (Port 161). Wenn man wünscht, dass der *community string/secName* als Name einer Gruppe nicht nach aussen dringt, kann man ihn mit der Einstellung in Filter (siehe unten) umdefinieren.

SNMP-v1: Die Namensauflösung von Traps der Version 1 und IPv4 geschieht **nicht** mit Hilfe der Absendeadresse, sondern mit der im Trap (PDU) selbst enthaltenen Adresse (IPv4) des ursprünglichen Servers. Wenn die Nachricht von einem anderen Server als dem Quellserver kommt, erscheint diese Adresse (IPv4) in dem Feld “Object“ des Event Browsers mit dem Hinweis “PROXY::“. Auf der Management-Station ist für eine korrekte Auflösung der Adressen zu sorgen.

6.2 Normalisierte Darstellung der SNMP-Traps

Eine Trap-Meldung wird in Form des Meldungstexts dargestellt als eine Folge der numerischen OID’s gefolgt von deren Wert und Datentyp, wenn der Wert keine Zeichenkette („octet string“) ist.

Der Generic Trap String kann sein: “coldStart(0)”, “warmStart(1)”, “linkUp(3), “linkDown(2)”, “authenticationFailure(4)”, “egbNeighborLoss(5)“.

Die Darstellung für Specific Traps:

- OID: Object Identifier in numerischer Form, zum Beispiel 1.3.6.1.4.1.1.2021.2.1.100
- Specific Trap-ID: Version 1, Zahlenwert, der den Fehler repräsentiert. Dieser Wert wird vom Hersteller bestimmt.
- Bei Auftreten von Variablen Argumenten: “VarTypes: ” (Version 1) “Var2Types: ” (Version 2c) “Var3Types: “ (Version 3)
- Variablen Argumente mit numerischer OID, Datentyp und Wert

Die Komponenten des Meldungstextes sind durch ein Leerzeichen getrennt.

Die Darstellung kann im laufenden Betrieb durch den parametergestützten Ersetzungsmechanismus Format Trap Text verändert werden, um die Aussagekraft zu erhöhen.

SNMP-v3: Der Trap Text beginnt mit der *snmpEngineID* des Agenten in hexadezimaler Darstellung direkt gefolgt vom *contextName*, wenn dieser definiert ist. Beide Datenobjekte lassen sich filtern.

7. Services (X11)

Auf entfernten Servern überprüft man die Funktionalität der Sockets. Der Test geschieht von der Management-Station aus.

7.1 Processing

Bearbeiten der Datensätze

List of services: Liste der bestehenden Datensätze für die aktive Überwachung; zwei Push-Button Up, Down zum Umordnen der Liste

Specification Service: Definition des Dienstes auf dem entfernten Server

- Nodename: Rechnername des entfernten Servers
- IP Address: IP-Adresse des entfernten Servers
- Port/Service: Programmnummer (=Port) des entfernten Servers, die man überprüfen möchte
- Encryption: Auswahlbox für SSL/TLS (z.B. https)
- Polling Interval (hor:min:sec): Aufrufintervall in Sekunden, Mindestzeit: Eine Minute
- Count Repeat: Maximale Anzahl der Wiederholungen, wenn eine Prüfung fehlgeschlagen ist
- Timeout (millisec): Auszeit in Millisekunden, bei Überschreitung wird Vorgang abgebrochen
- Response Time (millisec): Maximale Antwortzeit in Millisekunden
- Request (““=Empty String, <LF>=Return): Zeichenkette, mit der der Port angesprochen wird
- Reply (Reg.Exp.): Festlegung der Antwort, die erwartet wird.

Specification Event: Ausgabe der Meldung

- Group: Name der Gruppe für eine Meldung
- Object: Name von Object für eine Meldung
- Check Box Verbose: Gutmeldung erscheint zur Verifizierung, wenn der Port/Service erreichbar ist
- Check Box Enable: Ein/Ausschalten der Teilfunktion

Bearbeitung durch die Push-Button:

- Add: Hinzufügen eines Datensatzes für die aktive Überwachung
- Modify: Ändern der Datensätze
- Search: Suchen nach Datensätzen
- Delete: Löschen eines Datensatzes. Der Name Nodename muss zuerst selektiert werden.
- LookUp: Ermittelt die zu Nodename gehörige IP-Adresse. Das Ergebnis erscheint in dem Feld IP Address. Der Fokus der Eingabe muss auf dem Feld Nodename liegen. Analog kann man den zu IP Address gehörigen Rechnernamen erhalten.
- Quit: Verlassen der Maske ohne Änderung

7.2 Enable

Schalter zum Abschalten der aktiven Überwachung

8. Filter (X11)

Einrichten, Ändern, Löschen, Reports der Datensätze für das Filtern von Meldungen zum Zweck der Differenzenanzeige.

List of filters: Liste der bestehenden Datensätze für die Filterung von Meldungen; zwei Push-Button Up, Down zum Umordnen der Liste; das Selektieren eines Datensatzes geschieht durch Mausklick auf die linke Spalte (Severity) einer Zeile, das Anklicken der Spalten rechts davon bewirkt die Selektion der entsprechenden Komponente des Datensatzes.

Bei dem Empfang einer Meldung wird die bestehende Liste zum Vergleich durchlaufen. Ist bei einem Listenelement der Vergleich der Komponenten positiv, erfolgt die Behandlung der Meldung mit den angegebenen Spezifikationen, und es terminiert der Listendurchlauf. Das Ergebnis der Filterung ist somit von der Reihenfolge der Filter abhängig.

Trifft keine Spezifikation in der Liste, wird die Meldung angezeigt. Leere Eingabefelder werden nicht zum Vergleich herangezogen und wirken somit für diese Komponente positiv. Je nach der Einstellung wird die Meldung unterdrückt oder angezeigt. Wenn eine Meldung unterdrückt wird, gelangt sie nicht in die Datenbasis.

Specification Event (In): Festlegung der ankommenden Meldung

- Severity: Auswahl der Severity für die ankommende Meldung
- Group: Vergleich Eintrag mit Attribut “Group“ der ankommenden Meldung. Eingabe muss exakt mit der ankommenden Gruppe übereinstimmen. Wenn das Feld leer ist, bedeutet dies: Jede Gruppe
- Object (Reg.Exp.): Eintrag Suchmuster für Attribut “Object“ der ankommenden Meldung. Wenn das Feld leer ist bedeutet dies: Jedes Object
- Nodename (Reg.Exp.): Suchmuster (*regular expression*) für das Attribut “Nodename“ der ankommenden Meldung. Es macht keinen Unterschied zwischen Groß-/Kleinschreibung, leeres Feld bedeutet: Jeder Nodename
- Event Type: Auswahlbox für Event-Typ der eingehenden Meldung, “default“ bedeutet: Jeder Event-Typ
- Event Text (Reg.Exp.): Eintrag Suchmuster für “Event Text“ der ankommenden Meldung. Wenn das Feld leer ist, bedeutet dies: Jeder Meldungstext
- Suppress: Checkbox zum unbefristeten Unterdrücken der Meldung

Die ankommende Meldung wird mit der folgenden Spezifikation auf die herausgehende Meldung abgebildet. Man kann alle Attribute einer Meldung - außer den Zeitangaben, Event-Typ und dem Nodename - umdefinieren.

Specification Event (Out): Definition der herausgehenden Meldung

- Severity: Umsetzen der Meldungsschwere; bei “default” wird die ankommende Meldungsschwere beibehalten
- Group: Herausgehende Meldungsgruppe, wenn sie sich von der eingegangenen unterscheiden soll
- Object: dito für das Attribut “Object“ einer eingegangenen Meldung
- Counters (MaxDisplay/.../...): Es werden **maximal N ungleiche** Meldungen in dem Zeitraum angezeigt, die Wiederholung gleicher Meldungen aber unterdrückt
- .../MinDisplay/...: Es erscheint die Meldung erst nach der N. Wiederholung des **gleichen** Events und dann nur einmal
- .../MaxSuppress: Maximale Anzahl Unterdrückungen einer Meldung bis zur nächsten Anzeige; Anzeige erfolgt auch nach Verstreichen des Zeitraums
- Suppression Time (day-;-hor:min:sec): Zeitraum, in dem die Wiederholung einer spezifizierten Meldung unterdrückt werden soll; Eingabe: Tage, Stunden, Minuten, Sekunden; Wert Null (0;00:00:00) bedeutet: Keine zeitliche Unterdrückung, wenn auch die Counters nicht gesetzt sind
- Strict: Wiederholung von Meldungen, die sich nur im Event-Text unterscheiden bzw. variieren aber in den übrigen Attributen gleich sind, werden ebenfalls unterdrückt; das Eingabefeld für Event Text muss ausgefüllt sein, damit die ankommende Meldung ausreichend identifiziert werden kann
- Accept: Checkbox zum automatischen Quittieren einer Meldung, sie wird gleich archiviert
- Format Event Text: Eingabe des Formatstrings, der den Meldungstext des ankommenden Events formatiert. Bleibt das Eingabefeld leer, wird der ankommende Event-Text ausgegeben.

Bearbeitungsmodus durch die Push-Button:

- Add: Hinzufügen eines Filters
- Modify: Ändern eines Filters
- Search: Suchen nach Filtern
- Delete: Löschen eines Datensatzes für einen Filter. Zuerst muss mit der Maus die linke Spalte Severity in der oberen Liste selektiert werden.
- Quit: Verlassen der Maske ohne Änderung

Eine Meldung bzw. Event ist gleich, wenn die Attribute “Severity“, “Nodename“, “Group“, “Object“, “EventType“ und “Event Text“ übereinstimmen, sie ist ungleich, wenn nur ein Attribut nicht übereinstimmt. Den Event-Text kann man durch die Formatanweisung umsetzten, um Zeitangaben bei Protokolldateien und andere Komponenten zu entfernen oder zu verändern.

Ein Filter, der jede Meldung trifft, hat jede Severity gesetzt, keine Einträge für Group, Object, Nodename, Event Text und als Event Type “default“. Ein solcher Filter sollte am **Ende der Liste** stehen. Die davor stehenden Listenelemente stellen eine schrittweise Verfeinerung des allgemeinen Falles dar.

Achtung: Der Vergleich einer ankommenden Meldung mit den alten zum Zweck der Unterdrückung findet **nach** der Formatierung und den Ersetzungen statt, falls diese vorgesehen waren; also mit den Attributen einschliesslich Meldungs-Text, die auch dargestellt wurden. Das bedeutet, dass man durch die Art der Formatierung des Event-Textes bestimmen kann, in welchem Mass die Meldung zeitlich unterdrückt wird.

Im Fall einer Ersetzung bleibt der Meldungs-Text der Originalmeldung erhalten. Durch Doppelklick auf eine Meldung kann in dem Widget “Event Information“ neben der Entstehungs- und Empfangszeit auch die aktuelle Anzahl der unterdrückten Meldungen eingesehen werden.

9. Mails (X11)

Einrichten, Ändern, Löschen, Reports von Datensätzen, die Weiterleitung von Meldungen per SMTP-Mails bewerkstelligen.

Bei Empfang einer Meldung wird die Liste der Datensätze zum Vergleich bis zum Ende durchlaufen. Fällt der Vergleich positiv aus, wird eine Mail mit den spezifizierten Daten abgeschickt. Man kann eine Meldung zu mehreren Adressen schicken.

List of mail specifications: Liste der bestehenden Datensätze für die Weitergabe von Meldungen über SMTP-Mails; zwei Push-Button Up, Down zum Umordnen der Liste; das Selektieren eines Datensatzes geschieht durch Mausklick auf die linke Spalte (Severity) einer Zeile.

Specification Event: Festlegung der weiterzuleitenden Meldungen in der Form und mit den Attributen, wie sie ausgegeben worden sind.

- Severity: Vergleich Meldungsschwere mit der Severity der ausgehenden Meldung
- Group: Vergleich des Eintrages mit dem Attribut “Group“ der Meldung. Der Vergleich erfolgt exakt. Ist das Feld leer, bedeutet dies: Jede Gruppe
- Object (Reg.Exp.): Suchmuster für das Attribut “Object“ der Meldung. Ist das Feld leer, bedeutet dies: Jedes Object
- Nodename (Reg.Exp.): Suchmuster für das Attribut “Nodename“ der Meldung. Das Suchmuster macht keinen Unterschied zwischen Groß-/Kleinschreibung. Ist das Feld leer, bedeutet dies: Jeder Nodename
- Event Type: Auswahlbox für Event-Typ
- Event Text (Reg.Exp.): Suchmuster für “Event Text“ der Meldung. Ist das Feld leer, bedeutet dies: Jeder Meldungstext
- Counters: Schwellwert für die Anzahl der an der Management-Station durch Filter unterdrückter Events oder für die Summe der am Agenten gefundenen Einträge (bezogen auf einen Zeitraum der Unterdrückung). Die Überschreitung (>=) löst das Senden einer Mail aus. Das kann beim Erscheinen der Meldung sein, oder aber später. Diese Funktion ist nur aktiv, wenn der Wert grösser als Null ist
- Accept: Nach erfolgreichem Abschicken der Mail quittieren der Meldung

Specification Mails: Festlegung der Mail

- Mail Server #1: Name oder IP Adresse des Mailservers (Postausgangsserver)
- Mail Server #2: Name des Ausweichservers, wenn der erste versagt

- Port: Übertragungsport (z.B. 25, 465, 587)
- MaxNumber: Maximale Anzahl von abgeschickten Mails in einem Zeitraum; gilt individuell für die spezifizierte Meldung
- Time Interval (hor:min:sec): Zeitintervall für die Begrenzung der Anzahl; das Intervall beginnt mit dem Abschicken der ersten Mail, am Ende des Intervalls wird der Zähler zurückgesetzt
- OrigText: Sendet zusätzlich, wenn vorhanden, den “Original Event Text“ (bis zu 1024 Zeichen)
- Character Set: Zeichensatz für den ausgehenden Event Text; Auswahl ISO-8859-15 oder UTF-8
- Authentication (smtp/smtps): Auswahlbox für Authentifizierung am Mailserver (smtp, securesmtp)
- Username: Benutzername für das Postfach
- Password: Passwort für das Postfach
- Password confirm: Bestätigung der Passwortes
- Text for Subject: Text für den Betreff der Mail
- Checkbox enable: Ein/Ausschalten der Weiterleitung per Mail
- Mail Address #1: Erste Mailadresse
- enable: Ein/Ausschalten der Weiterleitung
- Mail Address #2: zweite Mailadresse

Bearbeitungsmodus durch die Push-Button:

- Add: Hinzufügen eines Datensatzes
- Modify: Ändern eines Datensatzes
- Search: Suchen nach einem oder mehreren Datensätzen
- Delete: Löschen eines Datensatzes. Zuerst muss mit der Maus die linke Spalte Severity in der oberen Liste selektiert werden.
- Quit: Verlassen der Maske ohne Änderung

10. TimeFilter (X11)

Einrichten, Ändern, Löschen, Reports von Datensätzen für die TimeFilter, die Meldungen in einem festen Zeitintervall unterdrücken.

Bei dem Empfang einer Meldung wird die bestehende Liste zum Vergleich durchlaufen. Ist bei einem Listenelement der Vergleich positiv, wird die Meldung unterdrückt, und es terminiert der Listendurchlauf. Anwendung findet diese Einrichtung zum Beispiel bei Wartungszeiten von Servern.

List of TimeFilters: Liste der bestehenden Datensätze für die Filterung von Meldungen; zwei Push-Button Up, Down zum Umordnen der Liste; das Selektieren eines Datensatzes geschieht durch Mausklick auf die linke Spalte (Severity) einer Zeile.

Specification Event: Definition der Meldungen in der Form und mit den Attributen, wie sie für die Ausgabe bestimmt sind.

- Severity: Vergleich Meldungsschwere mit der Meldungsschwere der Meldung
- Group: Vergleich der Eingabe mit dem Attribut “Group“ der Meldung. Der Vergleich erfolgt exakt. Ist das Feld leer, bedeutet dies: Jede Gruppe
- Object (Reg.Exp.): Suchmuster für das Attribut “Object“ der Meldung. Ist das Feld leer, bedeutet dies: Jedes Object
- Nodename (Reg.Exp.): Suchmuster für das Attribut “Nodename“ der Meldung. Das Suchmuster macht keinen Unterschied zwischen Groß- und Kleinschreibung. Ist das Feld leer, bedeutet dies: Jeder Nodename
- Event Type: Auswahlbox für Event-Typ
- Event Text (Reg.Exp.): Suchmuster für den Meldungstext. Ist das Feld leer, bedeutet dies: Jeder Meldungstext

Specification TimeFilter: Dauer der Meldungsunterdrückung

- enable: Ein/Ausschalten des Filters
- start hour (0..23): Anfangsstunde des Zeitintervalls
- start min (0..59): Anfangsminute des Zeitintervalls
- duration (hh:mm): Dauer des Zeitintervalls in Minuten; Format der Eingabe stunde:minute, maximale Dauer 1439 Minuten
- day of week: Tag der Woche
- day of month: Tag des Monats; 0 bedeutet: Option ausgeschaltet

Bearbeitungsmodus durch die Push-Button:

- Add: Hinzufügen eines TimeFilters
- Modify: Ändern eines TimeFilters
- Search: Suchen nach TimeFiltern
- Delete: Löschen eines Datensatzes für einen TimeFilter. Zuerst muss mit der Maus die linke Spalte Severity in der oberen Liste selektiert werden.
- Quit: Verlassen der Maske ohne Änderung

11. Export/Automatische Aktionen (X11)

Einrichten, Ändern, Löschen, Reports von Datensätzen, die den Export von Meldungen bewerkstelligen.

11.1 Processing

Bei Empfang einer Meldung wird die Liste der Datensätze von Anfang bis zum Ende durchlaufen. Fällt der Vergleich positiv aus, wird die Meldung mit dem angegebenen Programm exportiert. Man kann eine Meldung mehrmals exportieren.

List of export programs: Liste der bestehenden Datensätze für das Exportieren von Meldungen; zwei Push-Button Up, Down zum Umordnen der Liste; das Selektieren eines Datensatzes geschieht durch Mausklick auf die linke Spalte (Severity) einer Zeile.

Specification Event: Festlegung der zu exportierenden Meldungen in der Form und mit den Attributen, wie sie ausgegeben worden sind.

- Severity: Vergleich Meldungsschwere mit der Meldungsschwere der Meldung.
- Group (Reg.Exp.): Suchmuster für das Attribut “Group“ der Meldung. Ist das Feld leer, bedeutet dies: Jede Gruppe
- Object (Reg.Exp.): Suchmuster für das Attribut “Object“ der Meldung. Ist das Feld leer, bedeutet dies: Jedes Object
- Nodename (Reg.Exp.): Suchmuster für das Attribut “Nodename“ der Meldung. Das Suchmuster macht keinen Unterschied zwischen Groß- und Kleinschreibung. Ist das Feld leer, bedeutet dies: Jeder Nodename
- Event Type: Auswahlbox für Event-Typ
- Event Text (Reg.Exp.): Suchmuster für den Meldungstext. Ist das Feld leer, bedeutet dies: Jeder Text
- Counters: Schwellwert für die Anzahl der an der Management-Station durch Filter unterdrückter Events oder für die Anzahl der von den Agenten ermittelten Einträge (oder Summe davon bezogen auf einen Zeitraum der Unterdrückung). Die Überschreitung (>=) löst das Exportieren einer

Meldung aus. Das kann beim Erscheinen der Meldung sein, oder aber später. Die Funktion ist nur aktiv, wenn der Wert grösser als Null ist

Program name: Vereinbarung des Programmnamens

- enable: An/Abschalten des Programms
- MaxNumber: Maximale Anzahl von exportierten Meldungen in einem Zeitraum; gilt individuell für die spezifizierte Meldung
- Time Interval (hor:min:sec): Zeitintervall für die Begrenzung der Anzahl; das Intervall beginnt bei dem ersten Export, am Ende des Intervalls wird der Zähler zurückgesetzt
- Character Set: Zeichensatz für ausgehenden Event Text; Auswahl UTF-8 oder ISO-8859-15

Bearbeitungsmodus durch die Push-Button:

- Add: Hinzufügen eines Exportprogrammes
- Modify: Ändern eines Exportprogrammes
- Search: Suchen nach Exportprogrammen
- Delete: Löschen eines Datensatzes für ein Exportprogramm. Zuerst muss mit der Maus die linke Spalte Severity in der oberen Liste selektiert werden.
- Quit: Verlassen der Maske ohne Änderung

11.2 Parameterübergabe beim Exportieren

Das System übergibt dem Programm insgesamt 13 Parameter, die stellungsbezogen definiert sind. Die Position ergibt sich aus der Darstellung einer Meldung im Browser, von links nach rechts gelesen:

1) Severity: “inform“, “minor“, “warning“, “major“, “critical“
2) Datum
3) Uhrzeit
4) Nodename
5) IP-Adresse
6) Gruppe
7) Object
8) Event-Typ
9) Event-Text (Meldungstext)
10) Zeichensatz: “ISO-8859-15“ oder “UTF8“
11) Zeitstempel der Empfangszeit als Zahlenwert
12) Zeitstempel der Absendezeit

13) Zeitstempel der letzten Unterdrückung (kann auch Null sein)
14) Anzahl der unterdrückten Meldungen
15) Anzahl der von den Agenten ermittelten Einträge oder Summe davon (bezogen auf einen Zeitraum). Wert Null bedeutet: Ist für dieses Event nicht definiert
16) Zeitdifferenz in Sekunden

In einem Shellscript ist die Notation:

```
#!/bin/ksh -p
typeset SEVERITY=$1
typeset DATUM=$2
typeset ZEIT=$3
typeset NODENAME=$4
typeset IPADR=$5
typeset GROUP=$6
typeset OBJECT=$7
typeset EVENTTYPE=$8
typeset EVENTTEXT="$9"
typeset CHARSET=${10}
typeset TIMESTAMP=${11}
typeset TIMESTAMP_2=${12}
typeset TIMESTAMP_3=${13}
typeset SUPPRCOUNT=${14}
typeset TOTCOUNT=${15}
typeset DIFFSECS=${16}
integer RTC=0
# Aufruf von Exportprogramm seines Zweckes
exportprogramm "$SEVERITY" ... "$EVENTETEXT"
RTC=$?
exit $RTC
#end of script
```

Das angegebene Exportprogramm muss ausführbar sein und einen Returncode gleich Null zurückliefern. Es gibt sonst Systemfehlermeldungen. Außerdem gibt es eine Auszeit von 15 Sekunden. Wird diese überschritten, gibt es ebenfalls eine Systemfehlermeldung in die Protokolldatei des Hintergrundprozesses "browserctl".

12. EcFilter (X11)

Einrichten, Ändern, Löschen, Reports von EcFilter, die dafür sorgen, dass alte Meldungen automatisch quittiert und durch neue ersetzt werden. Die Einrichtung gilt für Events, die sich nur im Meldungstext unterscheiden, die übrigen Attribute (außer Datum und Wiederholungszähler "RepCnt") aber gleich sind. Beim Eintreffen einer Meldung wird die Liste der EcFilter durchlaufen und deren Suchmuster einerseits mit dem ankommenden Event-Text und andererseits mit dem Event-Text der bestehenden Meldungen im aktiven Browser verglichen. Fällt der Vergleich positiv aus, erfolgt die Ersetzung und der Listendurchlauf terminiert. Zum Abschluss der Operation wird der Wiederholungszähler "RepCnt" der alten Meldung um eins erhöht und der neuen zugeordnet.

EcFilter: Liste der bestehenden Datensätze für die Filterung; zwei Push-Button Up, Down zum Umordnen der Liste; das Selektieren eines Datensatzes geschieht durch Mausklick auf die Spalte EcFilter einer Zeile.
Input EcFilter: Eingabe für den EcFilter

Bearbeitungsmodus durch die Push-Button:

- Add: Hinzufügen eines Suchmusters oder einer Stringkonstante für den EcFilter
- Search: Suchen nach EcFiltern
- Delete: Löschen eines EcFilters. Zuerst muss mit der Maus aus der Liste selektiert werden
- Quit: Verlassen der Maske ohne Änderung

Bei der Bestimmung des Suchmusters oder der Stringkonstanten ist darauf zu achten, dass es signifikant genug ist, um den Event-Text der Meldung in ausreichendem Maß zu beschreiben. Die quittierten Meldungen gehen nicht verloren, sondern sind in den History-Daten jederzeit einsehbar.

13. NodesConfig, Kommando-Interface (X11)

Verwaltung der Datensätze zur Konfiguration der Nodes. Die Konfiguration geschieht durch das Bearbeiten der zugehörigen Konfigurationsdateien. Zusätzlich gibt es das Kommando-Interface für Administratoren und Operatoren.

List of nodes: Liste der bestehenden Datensätze für einen Operator, zur Selektion eines Datensatzes klickt man mit der linken Maustaste die linke Spalte Nodename einer Zeile. Durch Doppelklick auf diese Spalte wird das Kommandointerface aufgerufen (gleicher Effekt wie Execute). Durch Rechtsklick ruft man spezielle Funktionen in Abhängigkeit der anderen Eingabefelder auf. Es gibt zwei Push-Button Up, Down zum Umordnen der Liste.

Eingabefelder:

- Nodename: Feld für Nodename; ist prinzipiell frei wählbar, muss aber in Kombination mit IP Address eindeutig sein
- IP Address: IP-Adresse des Nodes; bildet das Funktionsargument für die nachfolgenden Operationen
- Admin Port: Portnummer; muss übereinstimmen mit der Portangabe für den Hintergrundprozesses “remoteconfd“ bzw. “remoteconfd.exe“ auf dem entfernten Server
- SockType: Socket-Typ *udp* oder *tcp*; muss mit der Einstellung von “remoteconfd“ bzw. “remoteconfd.exe“ auf dem entfenten Server übereinstimmen
- Group: Meldungsgruppe des Nodes
- Authentication String: Zeichenkette für eine zusätzliche Authentifizierung am Node; die Eingabe ist notwendig, wenn für den Hintergrundprozess “remoteconfd“ bzw. “remoteconfd.exe“ auf der Gegenseite der gleiche String vereinbart ist; die Zeichenkette muss mindestens acht Zeichen lang sein und darf keine Umlaute enthalten
- Platform: Betriebssystem des Nodes; eintragen Unix bzw. Unixderivat oder Windows
- Description: Beschreibung des Nodes, Text ist frei wählbar
- Character Set: Festlegung des Zeichensatzes für den Node aus seiner Auswahlliste; in der Liste enthalten unter anderem CP1250 bis CP1258, ISO-8859-1 bis ISO-8859-10, ISO-8859-13 bis ISO-8859-16; default: UTF-8
- Remote command (batch mode): Eingabe eines Kommandos, das auf dem Zielrechner ausgeführt wird. Der Start erfolgt durch die Enter-Taste, den Pushbutton Execute oder durch die rechte Maustaste in der Tabellenzeile, die den gewünschten Node enthält. Die Operation geschieht neben läufig im Hintergrund und endet mit dem Erscheinen des Editor-Fensters, das

die Ergebnisrückgabe liefert. Die Combo-Boxen Unix und Windows enthalten eine Auswahl von Befehlen zur Administration
- Execute: Aufruf des zuvor eingegebenen Befehls
- Cancel: Schickt ein Signal zum entfernten Server mit der Aufforderung, die Abarbeitung des Befehls vorzeitig zu beenden. Der Server beendet die Ausführung von selbst nach Verstreichen von 30 Sekunden (Timeout) oder wenn die Datenmenge 1 MB überschritten hat

Die Eingabefelder Nodename, IP Address, Group und Platform dienen auch als Suchfeld mittels *regular expressions*.

Bearbeitungsmodus durch die Push-Button:

- Refresh: Erneuern der Anzeige mit den Eingaben der Suchfelder; sind die Suchfelder leer, wird alles angezeigt.
- EraseRefresh: Löschen der Eingabefelder und Erneuern der Anzeige; geht auch mit der Esc-Taste
- Add: Hinzufügen eines Datensatzes mit den in Eingabefeldern gesetzten Werten
- Modify: Ändern eines Datensatzes mit den entsprechenden Werten der Eingabefelder
- Delete: Löschen eines Datensatzes, nachdem man in der Liste der Nodes eine Zeile selektiert hat
- LookUp: Ermittelt die unter Nodename eingegebene IP-Adresse oder den unter IP Address eingegebenen Nodename
- Quit: Schliessen der Maske

Rechter, unterer Teil der Maske:

- Remote edit – name of configuration file (full path name): Eingabe des vollständigen Pfadnamens einer Datei auf dem entfernten Server; durch Drücken der Enter-Taste wird der Datentransfer im Hintergrund gestartet. Das Ende der Übertragung wird erkennbar durch das Erscheinen des Editors mit dem Inhalt der Datei. Anschliessend kann man den Inhalt bearbeiten und dann zurück speichern. Die Funktion lässt sich auch durch Rechtsklick in der gewünschten Zeile der Tabelle starten, wenn das Eingabefeld von “Remote command“ leer ist. Durch den Pushbutton Store local lässt sich die Datei auch auf der Management-Station abspeichern
- ToList: Pushbutton, um den Namen der Konfigurationsdatei in die Liste der Dateinamen zu bringen. Der Name ist dann dauerhaft gespeichert
- GetFile: Holen der entfernten Datei, deren Name man unter List of files selektiert hat, und Aufruf des Editors zum Bearbeiten der Datei

- CheckNode: Prüfen, ob der selektierte Node mit dem Hintergrundprozess “remoteconfd“ erreichbar ist. Die Prüfung kann auch durch Rechtsklick einer Zeile in der Liste der Nodes erfolgen, wenn die Eingabefelder “Remote command“ **und** “Remote edit“ leer sind. Der Befehl wird neben läufig ausgeführt
- Remove From List: Entfernt einen selektierten Dateinamen aus der Liste der Dateinamen
- Read local files: Pushbutton zum Aufruf einer *File-Selection-Box*, mit der man eine lokale Datei auswählt, um sie dann auf einen oder mehreren Nodes zu verteilen. Die Datei kann auch eine Binärdatei (Programmdatei) sein. Die Grösse ist aber auf 1 MB beschränkt. Nach der Auswahl erscheint der Inhalt der Datei in dem Editor-Fenster. Dort gibt es ein zusätzliches Eingabefeld für den Dateinamen auf dem entfernten Server und den Pushbutton Save remote. Nach der Übertragung der Datei kann man das Ziel für die Verteilung durch Rechtsklick in der Liste der Nodes ändern und den Vorgang wiederholen
- List of files: Liste der Konfigurationsdateinamen, die einem Node zugeordnet ist. Die Dateinamen erscheinen, wenn man in der Tabelle der Server eine Zeile in der ganz linken Spalte “Nodename“ mit der linken Maustaste anklickt. Durch Doppelklick auf ein Listenelement wird der Editor aufgerufen, mit dem man die selektierte Datei bearbeiten kann

Die hier angebotenen Funktionen werden neben läufig abgearbeitet, so dass es keine Blockierung der Bedienoberfläche gibt.

14. browserhtml (WEB)

Man erhält die WEB-Seite, indem man sich vorher mit seiner Benutzerkennung und seinem Passwort anmeldet. Man sieht die aktiven Meldungen in Tabellenform, analog zur X11-Ausgabe

Im oberen Teil ist der Name des Administrators oder Operators, die Anzahl der Meldungen insgesamt, die Anzahl der sichtbaren Meldungen, danach die Anzahl der Meldungen getrennt nach Meldungsschwere.

Darunter sind die Bedienungselemente:

- –UpsideDown: Umkehrung der zeitlichen Reihenfolge
- ENTER: Abschicken der Seite
- HistoryEvents: Aufruf der Seite der History-Daten
- Lifecheck: Aufruf der Seite für Lifecheck bzw. Heartbeat

Eine Zeile hat die Spalten:

- Accept: Anerkennen der Meldung. Die Uhrzeit des Anerkennens wird registriert. Ebenso der Operator oder Administrator, der die Meldung anerkannt hat
- OrMaEx: Spalte zur Einsicht in weitere Attribute einer Meldung mit Hinweis auf die Existenz von originalem Meldungstext, verschickter Mail oder erfolgtem Export; wenn der Export oder das Senden der Mail fehlgeschlagen ist, erscheint das Symbol ’E’ in roter Farbe
- Sev.: Severity, Meldungsschwere
- Date/Time: Empfangszeit (Datum und Uhrzeit) der Meldung
- Nodename: Lokaler Rechnername des Servers
- IP Address: Absende IP-Adresse des Nodes
- Group: Meldungsgruppe
- Object: Object einer Meldung
- Event Type: Attribut zur Klassifizierung bezüglich Ursache und Herkunft einer Meldung; es wird vom System vergeben und kann nicht verändert werden; zusätzlich gibt es eine Darstellung für die Gesamtzahl der gefundenen Einträge sowie den dazugehörigen Zeitraum; Beispiel siehe unten
- RepCnt: Wiederholungszähler und daneben in eckigen Klammern die Anzahl von unterdrückten Meldungen bezogen auf dieses Event; die Angabe fehlt, wenn die Anzahl gleich Null ist
- Event Text: Meldungstext des Events

Die WEB-Seite wird alle 30 Sekunden automatisch aktualisiert.

Beispiel für die Darstellung von Event Type:

LogfileFormat#10/2m30s

Die Zahl nach dem Zeichen ’#’ (10) ist die Gesamtzahl der Einträge, die in einem Zeitraum von 2 Minuten und 30 Sekunden für den betreffenden Filter gefunden worden sind (unabhängig davon, wie viele Einträge tatsächlich übertragen worden sind). Format für die Zeitangabe: Ns, Nm, NmKs, Nh, NhKm; s: Sekunde, m: Minute, h: Stunde, N,K: natürliche Zahl.

14.1 History Events (WEB)

Analog zur X11-Oberfläche hat man die Möglichkeit, nach anerkannten Meldungen anhand ihrer Attribute zu suchen. Das Suchergebnis wird tabellarisch dargestellt. Durch eine Checkbox kann man das Suchergebnis in eine Datei auf seinen Web-Frontend herunterladen. Anschliessend kann man dort die Datei weiter verarbeiten.

ReceiveTime: Die Zeitangaben des Intervalls beziehen sich auf die Empfangszeiten der Meldungen, wie sie im Browser als aktive Meldungen dargestellt wurden.

- DateFrom: Datum des Beginn des Intervalls in der Vergangenheit; voreingestellt ist die Jetzt-Zeit vermindert um 12 Stunden
- TimeFrom: Uhrzeit des Beginns des Intervalls in der Vergangenheit; voreingestellt ist die Jetzt-Zeit vermindert um 12 Stunden
- DateTo: Datum vom Ende des Intervalls; voreingestellt ist die Jetzt-Zeit
- TimeTo: Uhrzeit vom Ende des Intervalls; voreingestellt ist die Jetzt-Zeit
- Checkbox now: Stellt die Eingabefelder DateTo und TimeTo zurück auf die Jetzt-Zeit

Severity: Meldungsschweren, nach denen man sucht. In der Voreinstellung sind alle Meldungsschweren deselektiert. Das bedeutet: alle Meldungsschweren

- Checkbox inform
- Checkbox minor
- Checkbox warning
- Checkbox major
- Checkbox critical

Es folgen die Eingabefelder:

- Nodename: Suche nach Rechnernamen mit *regular expressions*. Ist das Feld leer, bedeutet dies: Jeder Nodename
- Group: Suche nach Meldungsgruppen mit *regular expressions*. Ist das Feld leer, bedeutet dies: Jede Gruppe
- Object: Suche nach Object einer Meldung mit *regular expressions*. Ist das Feld leer, bedeutet dies: Jedes Object
- Event Type: Auswahlbox für Event-Typ, “default“ bedeutet: Jeder Event-Typ
- Event Text: Suche nach Meldungstexten mit *regular expressions*. Ist das Feld leer, bedeutet dies: Jeder Text

Danach die CheckBoxen:

- Slim: Es fehlen die Attribute für AcceptTime und Operator/Administrator, der die Meldung anerkannt hat
- UpsideDown: Änderung der zeitlichen Sortierung; die ältesten Meldungen stehen oben
- DownLoad: Das Suchergebnis wird in eine Textdatei geschrieben, pro Datensatz eine Zeile. Die Spalten jeder Zeile sind getrennt durch ein Semikolon ‘;‘. Der Name der Datei wird vom System vergeben und lautet: <operator_name>.html. Die Länge der Datei ist auf 500.000 Zeilen begrenzt. Bei einem neuen Suchvorgang wird die alte Datei überschrieben.

Danach kommt der Submit-Button ENTER: Starten des Suchvorganges

14.2 Lifecheck (Heartbeat,WEB)

Analog zur X11-Oberfläche sieht man die Nodes, die sich in der Überwachung befinden. Der Datenbestand liegt auf der Management-Station und kann deswegen jederzeit eingesehen werden. Die Liste wird automatisch aktualisiert. Ein Administrator hat die Sicht auf alle Nodes, ein Operator nur auf die Nodes, deren Gruppen ihm zugewiesen sind.

Die Tabelle hat die folgenden Spalten:

- Nodename: Name des Servers
- IP Address: IP-Adresse des Servers
- Group: Meldungsgruppe, in dem der Server enthalten ist
- delta (sec): Zeigt an die Zeitdifferenz in Sekunden seit dem letzten Lebenszeichen und in runden Klammern das einzuhaltende zeitliche Limit, von

dem ab signalisiert wird; der Wert in runden Klammern ist die Summe aus Polling Interval und Alarm Offset.

- Polling Interval (sev): Polling Intervall der Standardüberwachung, bildet die Basis für das zeitliche Limit, bei dessen Überschreitung die Ausnahmebehandlung stattfindet
- LifeSev.: Farbliche Darstellung der Zeitdifferenz. Je größer die Zeitdifferenz delta, desto länger hat sich der Server nicht gemeldet. Ist delta größer als das Limit, gibt es für diesen Node eine kritische Meldung. Nach dreimaliger Meldung im Abstand von 15 Minuten geht der Server in den Zustand „disabled“ über.
- Last Time: Uhrzeit des letzten Lebenszeichens
- Date: Datum des letzten Lebenszeichens
- Alarm Offset (sec): Aufsatz in Sekunden für das Limit, bis zu dem sich der Node spätestens melden muss
- Ping Offset (sec): Aufsatz in Sekunden für das Limit, nach dessen Verstreichen ein Ping-Check durchgeführt wird
- Sysname: Bezeichnung des Betriebssystems
- Daemon: Zeigt an, ob der Agent als Daemon betrieben wird oder nicht
- Check Box Disabled Nodes: Umschalten auf die Tabelle der „disabled nodes“. Es sind die Server, die sich nach dreimaliger Signalisierung (ca. 90 Minuten) nicht gemeldet haben

Mit Eingabefeldern kann man nach bestimmten Nodes suchen:

- Nodename: Suche nach Rechnername mit *regular expressions*. Ist das Feld leer, bedeutet dies: Jeder Nodename
- IP Address: Suche nach IP-Adresse mit *regular expressions*. Ist das Feld leer, bedeutet dies: Jede IP-Adresse
- Group: Suche nach Gruppe mit *regular expressions*: Ist das Feld leer, bedeutet dies: Jede Gruppe

Mit dem Submit-Button ENTER startet der Suchvorgang.

Darunter erscheint die Anzahl der gefundenen Nodes:

- TotCount: Gesamtzahl der Nodes
- DispCount: Anzahl der Server, die sich in der Anzeige befinden. Die Zahl ist begrenzt auf 300

14.3 Konfigurationsdatei „browserhtml.conf“

Konfigurationsdatei für die Web-Oberfläche des Browsers. In ihr wird die Environment Variable “OMBDIR“ und das Verzeichnis zum Herunterladen von Daten festgelegt.

Beispiel:

```
OMBDIR=/opt/monitor/database
# Downloadverzeichnis: <path>:<relpath> absoluter und relativer Pfad zu DocumentRoot
# Keine Angabe: /var/tmp
DOWNLOAD=/var/www/monitor:/monitor
```

Document-Root ist “/var/www“, darunter das Verzeichnis “monitor“, in das die herunter geladenen Dateien kopiert werden sollen.

15. Hintergrundprozesse

Für die nachfolgenden Programme muss für die aufrufende Shell die Environment Variable “OMBDIR“ gesetzt sein. Der Inhalt der Variablen zeigt auf das Verzeichnis mit den Systemdateien.

Beispiel: OMBDIR=“/opt/monitor/database“

15.1 browserctl: Verwaltungsprozess

Der Hintergrundprozess nimmt die folgenden Funktionen wahr:

- Realisierung Mails
- Realisierung Exportprogramme
- Realisierung von EcFiltern
- Allozierung Shared Memory

Aufruf:

browserctl [-e <OMBDIR>][-L <logfilename>] [-m] &

-L: Name der Logdatei (default: browserctl.logfile)
-m: Keinen Eintrag in die Logdatei nach erfolgreichem Abschicken einer Mail

Wichtig: Bei Neustart der Management-Station muss dieser Prozess als erstes aufgerufen werden.

15.2 monlistener: Empfang der Meldungen von den Agenten

Der Hintergrundprozess nimmt die Meldungen der Nodes über einen tcp-Port entgegen. Der Port ist mit einer Option frei wählbar, zum Beispiel 55555. Das Programm benötigt für die verschlüsselte Kommunikation mit den Agenten die Datei “monitorkeys.sig“, die entweder im gleichen Verzeichnis wie das ausführbare Programm oder im Home-Verzeichnis des Benutzers oder im Verzeichnis “/etc“ liegt.

Aufruf: monlistener -p <portno> [-4] [-e <OMBDIR>] &

-p : Programmnummer (Port)
-4 : Empfang nur ipv4, ohne diese Option ipv4 und ipv6!
-e : Setzen der Environment Variable “OMBDIR“

15.3 lifechecker: Verwaltung der Lifechecker-Meldungen

Der Hintergrundprozess verwaltet die Lifechecker-Meldungen von den Nodes. Wenn ein Node sich innerhalb eines einstellbaren Zeitintervalls an der Management-Station nicht gemeldet hat, erfolgt eine Signalisierung.

Außerdem schickt der Prozess ein Icmp-Ping zu einem Node, wenn dieser sich nach mehr als einer einstellbaren Anzahl von Minuten nicht gemeldet hat. Ist der Ping erfolglos, gibt es ebenfalls eine Signalisierung. Für diese Funktion braucht der Prozess Root-Rechte.

Aufruf: lifechecker [-n] [-e <OMBDIR>] &

-n : Aufruf ohne Root-Rechte, Icmp-Ping ist abgeschaltet
-e : Setzen der Environment Variablen “OMBDIR“

15.4 snmptraplistener: Trap Receiver

Der Hintergrundprozess empfängt die SNMP-Traps bzw. *Notifications der* Typen 1, 2c von den Nodes und anderen SNMP-fähigen Geräten. Traps der Version 3 können auch empfangen werden dürfen aber **nicht** verschlüsselt sein (zulässig: *authNoPriv*, *noAuthNoPriv;* hier unzulässig: *authPriv).*

Aufruf:

snmptraplistener [-p <portno>] [-t] [-L <logfilename>] [-4] [-e <OMBDIR>] &

-p : Programmnummer (Port) udp/tcp, voreingestellt 162/udp4+6;
-t : Empfang mit tcp sonst udp
-4 : Empfang nur ipv4, sonst ipv4 und ipv6
-L : Logfilename (default: snmptraplistener.logfile)
-e : Setzen der Environment Variablen “OMBDIR“

Das Programm benötigt Root-Rechte, wenn der Port kleiner als 1024 ist.

Hinweis: Wenn vorhanden können die Befehle snmptrap(1) oder snmpinform(1) auf beliebigen Plattformen benutzt werden, um Traps zur Management-Station zu schicken, sowohl über tcp als auch über udp.

15.5 udplistener: Empfang von anderen Management-Stationen

Der Hintergrundprozess empfängt Meldungen von anderen Management-Stationen, die ihre Meldungen weiterleiten. Er korrespondiert mit dem Programm rsendmsg_udp, der auf der sendenden Management-Station mit dem Exportmechanismus aufgerufen wird.

Aufruf: udplistener [-p <portno>] [-4] [-e <OMBDIR>]

-p : Programmnummer (Port) udp
-4 : Empfang nur ipv4
-e : Setzen der Environment Variablen “OMBDIR“

16. Programme für die Kommandozeile

Für die Nachfolgenden Routinen muss die Environment Variable “OMBDIR“ gesetzt sein. Der Inhalt der Variablen zeigt auf das Verzeichnis mit den Systemdateien.

Beispiel: OMBDIR=“/opt/monitor/database“

16.1 remotecmd: Fernaufruf von Kommandos

Das Programm ist ein Client für “remoteconfd“ bzw. “remoteconfd.exe“, das ein Kommando auf dem entfernten Node ausführen lässt und die Rückgabe einschliesslich Exit Status auf der Management-Station anzeigt. Die Datenübertragung erfolgt je nach Servereinstellung über Udp oder Tcp.

Aufruf: remotecmd <nodename|ip adresse> [<command>]

Der erste Parameter ist der Nodename oder die IP-Adresse des entfernten Servers, dann folgt der Name des auszuführenden Kommandos mit eventuellen Optionen oder Argumenten. Der Servername und die zugehörige Adresse müssen vorher an der grafischen Bedienoberfläche unter “NodesConfig“ (siehe oben) vereinbart worden sein. Die Ausführung eines Befehl kann mit Ctrl-C (SIGINT) abgebrochen werden. Die über das Netz gehenden Daten werden mit AES 256-Bit CBC verschlüsselt.

Man kann das Programm auch dazu benutzen, um Automatische Aktionen auf den Nodes als Reaktion auf bestimmte Meldungen an der Management-Station zu realisieren.

Beispiel: remotecmd 192.168.20.10 ls -lt /etc

Wenn der zweite Parameter <command> fehlt, erscheint eine Eingabeaufforderung (Prompt) für ein oder mehrere aufeinander folgende Kommandos auf dem gleichen Server. Diese Betriebsart wird durch Eingabe von “quit“ oder “exit“ beendet.

16.2 listnodes: Auflisten der registrierten Nodes

Das Programm listet die registrierten Nodes in Tabellenform auf. Die Tabelle hat die Spalten:

- Name: lokaler Rechnername
- Ip: IP-Adresse des Absenders

- Group: Meldungsgruppe für den Node
- Zeit: Datum und Uhrzeit der letzten Meldung
- Interval: Polling Intervall des Agenten für Standardüberwachung
- Sysname: Name des Betriebssystems
- Letzte Spalte: In der letzten Spalte erscheint die Angabe „DISABLED“, wenn der Node sich im Zustand „disabled“ befindet

Aufruf: listnodes [-d <nodename>]

-d : Löschen des Nodes mit dem Namen <nodename> aus der Liste

16.3 rsendmsg_p: Weiterleitung von Meldungen mit tcp

Der Befehl schickt eine Meldung von einem Exportprogramm per tcp zu einer anderen Management-Station, indem er mit dem dortigen Empfangsprogramm “monlistener“ über einen gemeinsamen Port kommuniziert.

Aufruf:

rsendmsg_p -p <portno> -d <managementstation> [-e <ausweichstation>] -i <ip-adresse> -u –c <charset> -g <gruppe> -o <objekt> [-t <event type>] [-a <time stamp>] -s <severity> [-v <gesamtzahl>] [-w <diffsecs>] -m <meldungstext>

Parameter:
+ -p: Portnummer tcp
+ -d: Managementserver
+ -e: Ausweichserver (optional)
+ -i: Ip-Adresse
+ -u: Unterdrücken von Prompt
+ -c: Zeichensatz [ISO-8859-1|UTF8]
+ -g: Meldungsgruppe
+ -o: Object
+ -t: Event Type (default: Import)
+ -a: Time stamp
+ -n: Nodename (optional)
+ -s: Severity [inform|minor|warning|major|critical]
+ -v: Gesamtzahl gefundener Einträge
+ -w: Zeitdifferenz in Sekunden
+ -m: Meldungstext

Rückgabewert: 0 erfolgreich, 1 Eingabefehler, 2 Kommunikationsfehler

16.4 rsendmsg_udp: Weiterleitung von Meldungen mit udp

Der Befehl schickt eine Meldung von einem Exportprogramm per udp zu einer anderen Management-Station, indem er mit dem dortigen Empfangsprogramm "udplistener" über einen gemeinsamen Port kommuniziert.

Aufruf:

rsendmsg_udp -p <portno> -d <managementstation> [-e <ausweichstation>] -i <ip-adresse> -g <gruppe> -o <objekt> [-t <event type>] [-a <time stamp>] -s <severity> [-v <gesamtzahl>] [-w <diffsecs>] -m <meldungstext>

Parameter:

- -p: Portnummer udp
- -d: Managementserver
- -e: Ausweichserver (optional)
- -i: Ip-Adresse
- -u: Unterdrücken von Prompt
- -c: Zeichensatz [ISO-8859-1|UTF8]
- -g: Meldungsgruppe
- -o: Object
- -t: Event Type (default: Import)
- -a: Time stamp
- -n: Nodename (optional)
- -s: Severity [inform|minor|warning|major|critical]
- -v: Gesamtzahl gefundener Einträge
- -w: Zeitdifferenz in Sekunden
- -m: Meldungstext

Rückgabewert: 0 erfolgreich, 1 Eingabefehler, 2 Kommunikationsfehler

17. Formatstrings

Bei der Spezifikation von SNMP-Traps und den Filtern gibt es die Möglichkeit, den ankommenden Text mit Hilfe eines Formatstrings umzusetzen. Ein Formatstring besteht aus verschiedenen Sonderzeichen, die mit bestimmten Operationen verbunden sind. Die Sonderbedeutung der Zeichen lässt sich mit vorangestelltem Backslash '\' ausschalten.

Es gibt die Sonderzeichen:

- $n oder ${n}: n ist eine Zahl [1..99]. Gibt aus das <n>. Wort des Eingangstextes
- %n oder %{n}: linksshift, gibt aus den um <n> Spalten nach links verschobenen Eingangstext, die Eingangszeile selbst bleibt unverändert
- &n oder &{n}: Verschiebung um <n> Zeichen (*character*) nach links des Eingangstextes, es gibt keine unmittelbare Ausgabe, der neue Textanfang der Eingangszeile wird automatisch auf den Anfang eines Wortes bzw. Spalte gelegt
- &{n,m}: Gibt aus <m> Zeichen ab dem <n>. Zeichen der Eingangszeile
- &{n[#|]substring}: Suche nach Substring in einem Wort. Gibt aus ab dem <n>. Zeichen bis zum Substring substring. Wenn substring nicht gefunden wird, erfolgt die Ausgabe bis zum Ende des Wortes (Sonderzeichen ist entweder '|' oder '#')
- @n oder @{n}: Verschieben der Eingangzeile nach links um <n> Spalten, die ursprüngliche Spalte <n+1> steht danach am Anfang der Eingangzeile, es gibt keine unmittelbare Ausgabe
- %<[n|]substring>: Suche nach einem Substring in der ganzen Zeile oder optional nach dem <n>. Auftreten eines Substrings in der Zeile (n > 0). Dann Shift nach links in der Eingangszeile zu dem Unterstrings substring. Der gefundene Substring bildet den neuen Anfang der Eingangszeile, es erfolgt keine unmittelbare Ausgabe
- ?<[n|]substring>: Gibt aus den bis substring nach links verschobenen Text der Eingangszeile. Wenn substring gefunden wird, terminiert die Formatierung, sonst wird mit dem folgenden Sonderzeichen fortgefahren; optional mehrmaliges Auftreten
- -<[n|]substring>: Gibt aus den an der Stelle des Auftretens von Substring substring abgeschnittenen Eingangstext, der gefundene Substring wird mit abgeschnitten, die Eingangszeile bleibt unverändert; optional mehrmaliges Auftreten
- $*: Gibt aus die ganze Eingangszeile
- $$: Gibt aus die letzte Spalte des Eingangstextes

Ein Wort ist ein zusammen hängender Textteil, der von Leerzeichen begrenzt wird. Eine Zeile ist eine Folge von Worten. Enthält der Formatstring keine Operatoren, wird die gefundene Zeile bzw. der gefundene Eintrag auf die Stringkonstante abgebildet. Die Suche nach einem Unterstring erfolgt von links nach rechts. Wird bei der mehrmaligen Suche die Anzahl <n> nicht erreicht, wird der am weitesten rechts stehende Unterstring genommen. Wird der Unterstring nicht gefunden, erfolgt keine Operation.

Beispiel 1:

Die folgende Zeile aus der Logfileauswertung soll formatiert werden:

SyslogEntry::messages: Mar 4 15:51:20 NEPTUN kernel: [1075.400809] httpd[2751]: segfault at 0 ip 00007f710deb3b97 sp 00007fff1314ef18 error 6 in libc-2.11.3.so[7f710de34000+159000] [/var/log/messages]

Formatstring: “$1%<1|] >@1 &{1|[}: %1“

oder “$1%<] >@1 &{1#[}: %1“

Ausgabe für den Event-Text des Browsers:

SyslogEntry::messages: httpd: segfault at 0 ip 00007f710deb3b97 sp 00007fff1314ef18 error 6 in libc-2.11.3.so[7f710de34000+159000] [/var/log/messages]

Der Ausdruck “$1“ setzt das erste Wort der Eingangzeile an die erste Stelle der Ausgangszeile. Der Ausdruck “%<] >“ (oder “%<1|] >“) verschiebt die Eingangszeile bis zum ersten Auftreten des Unterstrings “] “ nach links. Das nachfolgende “@1“ verschiebt die Eingangszeile nochmals um eine Spalte nach links, so dass der Unterstring verschwindet. Durch den Ausdruck “&{1#[}“ (oder “&{1|[}“) wird die Spalte “httpd[2751]“ an der Stelle “[“ abgeschnitten und zu “httpd“. Schließlich wird durch den Operator “%1“ die um eine Spalte nach links verschobene Eingangszeile ausgegeben. Die Ergebnisse der einzelnen Operationen werden in der Ausgabe miteinander verkettet.

Beispiel 2: Formatierung SNMP Traptext

E=80000002_01_09840301 Var3Types: 1.3.6.1.2.1.88.2.0.1 1.3.6.1.2.1.88.2.1.1.0 cpu usage idle too low 1.3.6.1.2.1.88.2.1.2.0 1.3.6.1.2.1.88.2.1.3.0 1.3.6.1.2.1.88.2.1.4.0 1.3.6.1.4.1.2021.11.11.0 1.3.6.1.2.1.88.2.1.5.0 Int: 1 1.3.6.1.2.1.1.5.0 SERVERX 1.3.6.1.4.1.2021.11.2.0 systemStats

Formatstring: ssCpuIdle: %<7| 1.3.6.1.>$3% (%4)

Ausgabe: ssCpuIdle: 1% (SERVERX 1.3.6.1.4.1.2021.11.2.0 systemStats)

Der Ausdruck “%<7| 1.3.6.1.>“ verschiebt die Eingangszeile bis zum siebten Auftreten des Unterstrings “ 1.3.6.1.“ nach links zum neuen Zeilenanfang. “$3“ gibt aus die dritte Spalte/Wort, “%4“ gibt aus die um vier Spalten nach links verschobene Restzeile, die von “(“ und “)“ umgeben ist.

18. Regular Expressions (Suchmuster)

Das System benutzt *extended regular expressions* nach dem POSIX Standard als Suchmuster. Die Eigenschaften sind in den *manual pages* von Unix nachzulesen. Für die speziellen Anforderungen dieses Systems gibt es optionale Zusätze, die an das Ende des Suchmusters nach einem Schrägstrich ’/’ angehängt werden.

Die Syntax ist: <RegExp>[/i|v|!]

Das eigentliche Suchmuster gefolgt von ’/’ und ’i’ oder ’v’ oder ’!’.

Die Bedeutung der Zeichen ist:

- ’i’: Kein Unterschied bei Groß/Kleinschreibung
- ’v’: Das Suchergebnis wird umgekehrt, Groß/Kleinschreibung wird unterschieden
- ’!’: Das Suchergebnis wird umgekehrt, Groß/Kleinschreibung wird **nicht** unterschieden

Die Sonderbedeutung kann man mit einem vorangestellten Backslash ’\’ aufheben.

Beispiele:

“^os$/i“ trifft die Zeichenkette “OS“, “Os“, “oS“, “os“
“fatal/i“ trifft Zeilen mit “Fatal“, “FATAL“, “fatal“, ...
“[0-9]/v“ trifft Zeilen, die keine Ziffern enthalten
“ABC/v“ trifft Zeilen, die **nicht** “ABC“ enthalten
“ABC/!“ trifft Zeilen, die **nicht** “Abc“, “ABC“, “abc“, ... enthalten
“[ ][1-9][0-9]{1,2}[ ]/v“ trifft eine Zahl, die mehr als drei Stellen hat
“[ ]3\.14[0-9]*[ ]“ trifft die Zahl 3.14...
“[ ]([3-9][0-9]{5})|([1-9][0-9]{6,})[ ]“ findet eine Zahl, die größer oder gleich 300000 ist

19. Installation

Die Hintergrundprozesse sollten einem unprivilegierten Benutzer zugeordnet werden. Zum Anstarten beim System-Boot kann man die folgenden Einträge in der “rc.local“ unter “/etc“ vornehmen. Der Prozess “browserctl“ muss als erstes gestartet werden:

```
export OMBDIR=“....“
export LD_LIBRARY_PATH=“.....“
su monitor -c ’/home/monitor/browserctl/browserctl -e $OMBDIR &’
sleep 2
su monitor -c ’/home/monitor/monlistener/monlistener -p 55555 -e $OMBDIR &’
# Horcht auf Port 5555/tcp, ipv4 und ipv6
sleep 1
su monitor -c ’/home/monitor/portchecker/portchecker -e $OMBDIR &’
/home/monitor/lifechecker/lifechecker &
# Root-Rechte wegen ICMP
/home/monitor/snmptraps/snmptraplistener &
# Horcht auf Port 162/udp, ipv4 und ipv6
logger “Server-Prozesse gestartet“
su - monitor -c /home/monitor/agents/basemonagent
logger “Agent fuer Standardueberwachung gestartet“
```

Dabei ist “monitor“ der Name eines unprivilegierten Benutzers. Unter diesem findet auch die Verwaltung der Daten statt. Das Gui-Programm “browser“ kann mit dem setuid-Bit versehen werden, da es nicht root gehört.

Eine andere Möglichkeit ist die Benutzung von *systemd* (system and service manager für Linux). Man legt für jeden Hintergrundprozess eine Datei <name>.service in dem Verzeichnis “/lib/systemd/system“ (Debian) an. Der entsprechende Prozess kann mit dem Befehl *systemctl* gestartet und gestoppt werden.

Beispiel:

```
[Unit]
Description=browserctl
[Service]
Type=simple
User=monitor
ExecStart=/home/monitor/browserctl/browserctl -e /opt/monitoringdata
[Install]
Alias=browserctl.service
```

Eine dritte Möglichkeit besteht in der Benutzung des Agenten für die Standard-überwachung. Es hat den Vorteil, dass die Hintergrundprozesse im laufenden Betrieb überwacht und bei Bedarf wieder gestartet werden.

Einträge in “basemonagent.conf“:

```
restart::browserctl/browserctl::/bin/su - monitor -c /home/monitor/browserctl/startbrowserctl.sh
restart::monlistener/monlistener::/bin/su - monitor -c /home/monitor/monlistener/startmonlistener.sh
restart::portchecker/portchecker::/bin/su - monitor -c /home/monitor/portchecker/startportchecker.sh
restart::lifechecker/lifechecker::/home/monitor/lifechecker/startlifechecker.sh
restart::snmptraps/snmptraplistener::/home/monitor/lifechecker/startsnmptraplistener.sh
```

Das Agentenprogramm wird von “cron“ für root aufgerufen. Eintrag für die crontab:

```
0-59 * * * * /root/basemonagent > /tmp/basemonagent_root.log 2>&1
```

20. Event-Typen

Attribut zur Klassifizierung der Meldungen durch das System

Event Type	Funktion	Programm
Filesystem	Überwachung Dateisysteme	basemonagent, winmonagent.exe
Inode	Belegungsgrad Inodes der Dateisysteme	basemonagent
Process	Prozessüberwachung Unix	basemonagent
ProcessRestart	Anstarten von Hintergrundprozessen	basemonagent
WinTask	Überwachung Tasks von Windows	winmonagent.exe
WinService	Überwachung Services von Windows	winmonagent.exe
Syslog	Logfileauswertung von Systemlogdateien	basemonagent
SyslogFormat	Logfileauswertung mit Formatierung am Agenten	basemonagent
Logfile	Logfileauswertung	logmonagent, asyncmonagent, asyncmonagent.exe, logmonagent.exe
LogfileFormat	Logfileauswertung mit Formatierung beim Agenten	logmonagent, asyncmonagent, asyncmonagent.exe, logmonagent.exe
Frequency	Logfileauswertung und Überwachungsskripte mit der Anzeige der Anzahl gefundener Zeilen für ein Suchmuster	basemonagent, logmonagent, asyncmonagent, asyncmonagent.exe, logmonagent.exe, scriptmonagent, scriptmonagent.exe, logdiragent, logrecagent,
WinSysEventlog	Überwachung system event log Windows	winmonagent.exe
WinApplEventlog	Überwachung	winmonagent.exe

	application event log Windows	
WinSecEventlog	Überwachung security event log Windows	winmonagent.exe
Performance	Überwachung Load Average, Swap, Memory, CPU	basemonagent, winmonagent.exe
ScriptStd	Überwachungsskripte	basemonagent, winmonagent.exe
ScriptStdFormat	Überwachungsskripte mit Formatierung der Ausgabe am Agenten	basemonagent, winmonagent.exe
Snmptrap	SNMP-Notifications	snmptraplistener
Portcheck	Prüfen entfernter Ports	portchecker
PortcheckLocal	Lokale Prüfung von Ports	basemonagent, winmonagent.exe
Uptime	Signalisierung von Reboots	basemonagent, winmonagent.exe
Import	Anzeige importierter Meldungen anderer Management-Stationen	rsendmsg_p, rsendmsg_udp, monlistener, udplistener

Rsendmsg	Direktmeldung zur Management-Station	rsendmsg
Zombie	Überwachung Zombie-Prozesse	basemonagent
System	Systemmeldungen	Management-Station
SystemAgent	Systemmeldungen	Agenten
Filesize	Überwachung Größe von Dateien	basemonagent, logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe, logdiragent, logrecagent
PingCheck	Heartbeat/Lifecheck	lifechecker
LogfileTotal	Logfileauswertung	logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe
LogfileTotalFormat	Logfileauswertung mit Formatierung am Agenten	logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe

LogfileDir	Logfileauswertung von Verzeichnissen	logdiragent
LogfileDirFormat	Logfileauswertung von Verzeichnissen mit Formatierung der Ausgabe am Agenten	logdiragent
LogfileRec	Logfileauswertung von Verzeichnissen und Unterverzeichnissen	logrecagent
LogfileRecFormat	Logfileauswertung von Verzeichnissen und Unterverzeichnissen mit Formatierung der Ausgabe am Agenten	logrecagent
Script	Überwachungsskripte	scriptmonagent, asyncmonagent, asyncmonagent.exe, scriptmonagent.exe
ScriptFormat	Überwachungsskripte mit Formatierung der Ausgabe am Agenten	scriptmonagent, asyncmonagent, asyncmonagent.exe, scriptmonagent.exe
Permission	Keine Leseberechtigung für Logdateien	basemonagent, logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe, logdiragent, logrecagent
Existence	Zieldatei existiert nicht	basemonagent, logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe, logdiragent, logrecagent
RegExpression	Fehler in regulärem Ausdruck	Agenten
Heartbeat	Säumnismeldungen, an-, abmelden von Nodes	monlistener, lifechecker
Security	Änderungen am Filesystem	secmonagent