Integrated Server Monitoring

The Management Station

© Wilhelm Buchholz, Im Bruche 6, 31275 Lehrte

http://www.monitor-site.de

mailto:new-monitoring@t-online.de

Contents

1. Introduction

This present monitoring system consists of three components:

- Autonomous agents on the monitored servers (nodes): Messages are sent to the Management Station
- SNMP Traps respectively Notifications: Messages are sent to the Management Station
- Active monitoring of services: The remote server sockets are reviewed by the Management Station using the network

It is a text based and event-driven system with a graphical user interface.

The Management Station has the following tasks:

- Receive messages from the agents of the nodes
- Receipt of SNMP traps of the nodes and other network components
- Presentation of messages with X11 and WEB
- Forwarding of messages via SMTP mails and/or export
- Settings of the system by administrators

The combined task is executed with various background processes, with an X11 interface and a web interface. The Management Station is intended for the Linux operating system 64 Bit.

2. Event Browser (X11): Central Representation Of The Messages

Here - in addition to the web interface - the central output of the system takes place. A user - administrator or operator - must register in advance with the user ID and password.

The messages are tabulated. The latest message is displayed by default at the top of the table. By default, you see the active messages. An administrator sees all messages, an operator only those whose groups were assigned to him by the administrator.

The program requires for the encrypted communication with the agents the file "monitorkeys.sig" located either in the same directory as the executable program or in the user's home directory or in the directory “/etc”. The signature of the file is determined at the beginning of the operation and not changed in the following.

A message has the following attributes:

- OrMaEx: Indicates whether an original event text is available; also indicates whether the message is exported and/or was forwarded to a mail; if the transfer is incomplete, the letter 'E' appears in red, the letter 'X’ appears on success
- Sev.: Severity (“inform“, “minor“, “warning“, “major“, “critical“) with color display
- Date/Time: Reception time (date and time) of the message
- Nodename: Indication of the origin of a message, network name of the message source in Unix servers according to "uname-n"
- IP Address: IP address of the sending server, another attribute for identifying the source of a message, ipv4 or ipv6
- Group: Message group, attribute for the multi-user capability
- Object: Object of the message, attribute to differentiate messages
- Event Type: Attribute for the classification with respect to cause and origin of a message; it is assigned by the system and can not be changed; in addition, there is a display of the total number of entries found and the corresponding time period; Example see below
- RepCnt: Retry count for the same or similar messages, in square brackets besides the number of suppressed messages for this event; the indication is missing, if the number is zero; so you have control over the frequency of events
- Event Text: Text of the message for Diagnostics and Error Handling

In the "History Event Browser" there is instead of column RepCnt the column SupCnt indicating the number of suppressed messages by the corresponding filter in a period.
Lower part of the Browser:

Event Browser:

- Accept: Accept one or more messages, depending on whether it has selected with the mouse. The system records the time of acknowledgment and the name of the administrator or the operator who acknowledged the message. The information is obtained by double-clicking a message.
- Severities: Sum of the Severities, such as are present in the active Browser.
- Popup critical event: If you activate the checkbox, a message with the Severity "critical" also appears in a special window
- Popup major event: The same happens when a message with severity "major" appears

The attribute Nodename must be unique. It can be set for the agents in the configuration files as needed. The attribute IP Address is not used for comparison with other messages, but can be operationally used in connection with the export functions.

In the upper part of the window, pull-down menus are for setting the system.

Further have the pull-down menus of the Browser to be explained.

- Actions: For administrators and operators
- Operators: Only for administrators
- Groups: Only for administrators
- SNMPTraps: Only for administrators
- Services: Only for administrators
- Filter: Only for administrators
- Mails: Only for administrators
- TimeFilter: Only for administrators
- Export: Only for administrators
- EcFilter: Only for administrators
- NodesConfig: For administrators and operators

Example of representing Event Type:

LogfileFormat#10/2m30s

The number after the '#' (10) character is the total number of items that have been found over a period of 2 minutes and 30 seconds for the filter concerned, regardless of how many items have been actually transferred. The format for the time specification: Ns, Nm, NmKs, Nh, NhKm; s: second, m: minute, h: hour, N,K: natural number.

3. Actions (X11)

3.1 Event Browser

View and renew the active, unprocessed messages.

3.2 History Event Browser Dialog

Through this submenu you have the chance to search for accepted messages by their attributes. The search results are presented in tabular form in the Browser. One can write the result in a text file with the name of his choice and then further processed.

- Selection of period: The times of the interval from DateTime from and DateTime to refer to the times of reception of the messages as they were displayed in the browser as active messages.
- Severity: Severity, one is looking for. By default, all severities are selected.
- Nodename (Reg.Exp.): Looking up node name. If the field is empty, it means: each node name
- Group (Reg.Exp.): Search by message group; the field is empty, this means: each group
- Object (Reg.Exp.): Search object of a message; the field is empty, this means: each object
- EventTypes: Selection box for Event Type, "default" means: any Event Type
- Regular expression for Event Text: Search by message text by *regular expression*; the field is empty, this means: every message text
- Delta Latest Suppr. (hor): Selects event/messages whose “Time Latest Suppression” is within the entered recent hour(s). The operation is only defined for the data area in the *shared memory*.
- File name for download: Specifying the file name of a text file into which the search result is written, one line per data record. The columns of each line are separated by a semicolon ';'. The length of the file is limited to 500.000 lines. If the input field is empty, the operation is omitted.
- FileSelectionBox: Open the graphical representation of the file system to determine the file name
- Enter: Start the search process
- Cancel: Exit the submenu

The ESC key clears the input fields (also applies to the other input masks).

3.3 History Event Browser

Renew the display with the values entered in History Event Browser Dialog

3.4 Selected Events Dialog

Selecting events of active messages

- Severity: Severity of a message
- Nodename (Reg.Exp.): Search pattern for Nodename
- Group (Reg.Exp.): Search pattern for message group
- Object (Reg.Exp.): Search pattern for object
- Event Type: Selection box for Event Type
- Regular expression for Event Text: Search pattern for message text
- Enter: Perform the selection
- Cancel: Cancel the function

3.5 Selected Events

Renew the display with the values entered in Selected Events Dialog. The display has the same columns as the "Event Browser".

3.6 Lifecheck

List the nodes that are in the monitor. The database is located on the Management Station and can therefore be viewed at any time. The control messages coming from the agent basemonagent (Unix) or winmonagent.exe (Windows).

List of nodes: Table of Nodes

The table has the following columns:

- Sev.: Highest Severity of an active message for the node
- Nodename: Computer name of the node
- IP Address: IP address of the node
- Group: Message group for the node as declared in the agent basemonagent respectively winmonagent.exe
- delta (sec): Indicates the time difference in seconds since the last sign of life, and in parentheses, the time limit to be observed; the value in parentheses is the sum of Polling Interval and Alarm Offset.
- Polling Interval (sec): Polling interval of the standard monitoring; it forms the basis of the time limit; if exceeded, an exception occurs
- LifeSev.: Color representation of the time difference. The greater the time differential delta, the longer the server has not been reported. If delta is greater than the limit, there is a critical message for this node. After three

unsuccessful messages every 15 minutes, the server goes on to state "disabled".

- Last Time: Time of the last sign of life
- Date: Date of the last sign of life
- Alarm Offset (sec): Offset in seconds for the time limit, up to which the node must report no later than
- Ping Offset (sec): Is offset in seconds for the time limit after which a Ping check is performed
- Sysname/Release: Name and release of the operating system
- Daemon: Indicates whether the agent is run as a daemon or not
- AutoRefresh: The list is automatically updated
- Disabled Nodes: Switching to the table of "disabled nodes". There are servers that have not been reported after three signaling (about 90 minutes)

Specification of node(s):

- Severity: Choice of Severities for messages in the active Browser
- Nodename (Reg.Exp.): Looking up nodename with *regular expressions*; the field is empty, this means: any nodename
- IP Address (Reg.Exp.): Looking up IP address with *regular expressions*; the field is empty, this means: any IP address
- Group (Reg.Exp.): Looking up Group with *regular expressions*; the field is empty, this means: any Group

Result: Number of Nodes

- Nodes in display: Number of found servers that are in the display, the number is limited to 300
- Total: Total number of nodes found

Processing mode by the push buttons:

- Refresh: Refresh the list
- EraseRefresh: Refresh the list and clear search fields
- Delete: Deleting a node from the list; only for the administrator
- DeleteAll: In the “disabled” mode, you can delete all nodes
- Quit: Leave the mask without a change

3.7 LifecheckLimit

Setting the thresholds for signaling if messages from a node are missing.

- Nodename: Enter the name of the node; changes are made only for the node
- Group: Input name of a message group; changes take place for all nodes in this group
- Alarm Offset (sec): Offset in seconds for the limit at which the alarm is to be made
- Disable Alarm: No signaling in the absence of any sign of life
- Ping Offset (sec): Offset in seconds for the limit at which a Ping check is done
- Disable Pingcheck: Turn off of Ping check
- Get Values: Get the latest data from the nodes, whose name has been entered under Nodename
- Modify: Set new values for a node or a group
- Quit: Leave the form without changing

3.8 Change password

Change their own password for administrators and operators

There are the input fields:

- Old password: Enter the old password (only for operators)
- New password: Enter the new password
- Confirm new password: Confirmation of the new password
- Enter: Submit the change
- Quit: Exit function without change

3.9 Database

Here the utilization of the archive file and the shared memory for the messages is displayed. Moreover, one can see each of the reception timings of the first and of the last data set.

3.10 Reduce Archive

Shorten the archive file by deleting the oldest records. You can only delete if the archive file is larger than the database in shared memory for events.

There are the input fields:

- Date of oldest record: Specifying a date by which all the older records are deleted

- Delete N count oldest records: Number of the oldest records to be deleted

3.11 Noscroll

Setting for scrolling or not scrolling; the focus jumps after a new message to the top of the table (up or down); applies only to active events

3.12 BoldSelect

The selected line is bold

3.13 UpsideDown

Reversal of temporal order in the list of messages, in the pre-setting the latest message is above

3.14 System

View the background processes on the Management Station with the start/stop times and the process id

4. Operators (X11)

4.1 Processing: Edit the Operators and Administrators

Setting, changing, deleting, reports of operators and administrators

List of operators: List of operators and administrators. There is the column Adminpermission, which indicates whether a user has admin rights or not.

Input for operators/administrators:

- Operator name: Name of the operator or administrator
- Password: Initial password for the operator or administrator
- Check Box Adminpermission: Assignment of administrative rights
- Description: Descriptive information about the user
- Add: Add a name for operator/administrator. The name must be new; an existing user name is rejected.
- Modify: Change dataset of a use
- Search: Search for names of operators/administrators.
- Delete: Delete a name. The name must be selected first.
- Quit: Leave the input without storing changes

4.2 Operators, Groups

Assigning groups to operators and inverse function
There appear three list boxes with:

- Operators: List of all operators (not administrators)
- All groups: List of groups
- Groups for: <operatorname>: List box of the assigned groups

First, one selects an operator name. Then you can carry from the middle list box (all groups) each group using a push button in the right list box.
The inverse function - the deselecting of a group from an operator - is done as follows:

First you select the operator. You can see in the right list box the assigned groups. Of these, one can select one. Then use the push button Delete.

There are the push buttons:

- ->: After selection from the middle list box to append to the list of assigned groups
- Enter: Completion of an assignment
- Delete: After selection of the right list box delete the assignment
- Quit: Leaving the mask

5. Groups (X11)

Setting, changing, deleting, reports of groups.

List of groups: List of existing data sets for groups; selecting a data set is done by clicking on the left-hand column (Groups) of a line. The column “Opcount” indicates how many operators are assigned to this group.

Input group:

- Group name: Inputting a group name or a group name selection from the list of groups in the upper portion
- Description: Description of the group
- Add: Add a group. The name must be new; an existing group name is rejected.
- Search: Search for group names
- Delete: Deleting a group name. The name must be selected first.
- Quit: Leave the mask without storing changes

6. SNMP-Traps (X11)

Here the setting for signaling with SNMP Traps (*Notifications*) takes place that are received by the Trap Receiver snmptraplistener (see below). The setting can make only an administrator.

6.1 Processing

List of trap specifications: List of existing records for handling SNMP traps; there are two push buttons Up, Down to rearrange the list; selecting a data set is done by clicking on the left-hand column (Community String) of a line.

At the reception of a trap the existing list is traversed for comparison. If a list item is positive for the comparison, the trap is displayed with the given specifications and the list run ends. Thus it depends on the order of list elements.

Traps/Notifications of version 3 (SNMP-v3) must not be encrypted.

Specification Snmp Trap: Input fields to determine the incoming traps

- Community String/Username: Enter Community String for version 1, 2c or Username (*securityUser*) for version 3; no input: meets any Community String or Username
- Nodename: Indication of node name. The name entered must be unique. If this field is blank, the system assigns the DNS name, which results from the resolution of the sender IP address. If a resolution is not possible, the hostname appears as text: unresolved::<ip address>; applies to Version 2c and 3, Version 1 see below
- IP Address (Reg.Exp.): Comparison of the IP address you entered as search string to the IP address of the sender of the trap. If the field is empty, this means: any IP address
- Generic Trap: Combo Box for Generic Traps 0..5
- Enterprise Specific Trap: Enter numerical value for the enterprise specific trap id
- Object Identifier (OID): Input OID or part of an OID, which is compared to the OID of an incoming Trap, no input: any OID of a received Trap
- Compare: Combo Box for comparison operators (numeric values)
- Threshold (Numeric Value): Numerical value for the comparison to the Object Identifier (OID) associated value
- Trim: Shift to the left up to the in Object Identifier (OID) entered numeric OID; the text before the OID is lost
- Matching for Trap Text (Reg.Exp.): Comparison of the input text as a search pattern to the incoming message text in the normal form. If the field is empty, this means: any text

- Suppress: Check Box for the suppression of the specified trap message

Specification Event: Setting to output the message

- Severity: Combo Box for Severity (inform, minor, warning, major, critical) to appear to the message
- Group (CommunityString|InputField): Set the message group: either the *community string/secName* from the sending server or input field on the Management Station; if the message group following an asterisk '*', it will be replaced as required by the group name that is listed in the data base for the Lifecheck with the IP address
- Object: Attribute “Object“ of the message
- ShortName: Check Box for the selection of the short DNS name; the name "foo.company.com" becomes "foo"
- Accept: Trap message should come immediately to history data base
- Format Trap Text: Replacement mechanism controlled by the format string; at this point, the operator '$' followed by a zero "$0" has the meaning: output of *community string/secName*

Processing mode by the push buttons:

- Add: Add a data record
- Modify: Change a data record
- Search: Find a data record
- Delete: Deleting a data record. The first column with Nodename must be selected first.
- LookUp: Determines the IP address associated with Nodename. The result appears in the field IP Address (Reg.Exp.). The focus of the entry must be on the field Nodename. Conversely, one can obtain the node name by the corresponding IP Address (Reg.Exp.).
- Quit: Leave the mask without storing changes

Note to Group (CommunityString|InputField): With the selection of the *community string* or *secName*, the sending servers themselves determine their message group without the need for additional table entries; a dynamic assignment takes place. The setting on the SNMP clients of *community string/secName* for *snmp notifications* (port 162) is done independently of SNMP queries (port 161). If you wish that the *community string/secName* should not be displayed as the name of a group, you can redefine it with the setting in Filter (see below).

SNMP-v1: The name resolution of traps version 1 and IPv4 does not happen with the help of the sender address, but with the address (IPv4) of the original server contained in the trap (PDU) itself. If the message comes from a server other than the source server, this address (IPv4) appears in the field "Object" of the Event Browser with the note "PROXY ::". On the Management Station it is necessary to ensure a correct resolution of the addresses

6.2 Normalized representation of SNMP-Traps

A trap message is displayed in the form of the message text as a sequence of numeric OID's followed by the value and data type if the value is not a string ("octet string").

The Generic Trap String may be: “coldStart(0)”, “warmStart(1)”, “linkUp(3), “linkDown(2)”, “authenticationFailure(4)”, “egbNeighborLoss(5)“.

The representation for Specific Traps:

- OID: Object identifier in numeric form, for example 1.3.6.1.4.1.1.2021.2.1.100
- Specific Trap-ID: Version 1, numerical value representing the error. The manufacturer determines this value.
- In case of variable arguments: “VarTypes: ” (Version 1) “Var2Types: ” (Version 2c) “Var3Types: “ (Version 3)
- Variable arguments are displayed with numerical OID, data type and value

The components of the message text are separated by a space.

The display can be changed by the replacement mechanism Format Trap Text to increase the significance.

SNMP-v3: The Trap Text starts with the *snmpEngineID* of the agent in hexadecimal notation directly followed by the *contextName* if it is defined. Both data objects can be filtered.

7. Services (X11)

On remote servers one checks the functionality of the sockets. The test is done from the Management Station.

7.1 Processing

Editing the data records

List of services: List of existing records for the active monitoring and two push buttons Up, Down to rearrange the list

Specification Service: Definition of the service on the remote server

- Nodename: Computer name of the remote server
- IP Address: IP address of the remote server
- Port/Service: Port number of the remote server that you want to check
- Encryption: Selection box for SSL/TLS (e.g. https)
- Polling Interval (hor:min:sec): Call interval in seconds, minimum time: one minute
- Count Repeat: Maximum number of retries if a check has failed
- Timeout (millisec): Timeout in milliseconds, for exceeding operation is canceled
- Response Time (millisec): Maximum response time in milliseconds
- Request (““=Empty String, <LF>=Return): Request with which the port is connected
- Reply (Reg.Exp.): Determining the response, which is expected.

Specification Event: Output of the message

- Group: Name of the Group for a message
- Object: Name of Object for a message
- Check Box Verbose: OK message will appear to verify if the port/service is available
- Check Box Enable: On/off function

Processing by the push buttons:

- Add: Add a record for the active monitoring
- Modify: Changing data records
- Search: Searching for Records
- Delete: Deleting a record. The name Nodename must first be selected.

- LookUp: Determines the IP address associated with Nodename. The result appears in the field IP Address. The focus of the entry must be on the field Nodename. Analogously, one can obtain the corresponding host name to IP Address.
- Quit: Leave the mask without storing changes

7.2 Enable

Main switch to turn off the active monitoring

8. Filter (X11)

Setting, changing, deleting, reports of data records for the filtering of messages for the purpose of Difference Display.

List of filters: List of existing records for the filtering of messages and two push-button Up, Down to rearrange the list. Selecting a data set is done by clicking on the left-hand column (severity) of a line, clicking on the columns to the right causes the selection of the corresponding component of the data set.

Upon receiving a message, the existing list is checked by comparison. If for a list item the comparison of the components is positive, the treatment of the message with the given specifications takes place, and the operation will terminate. The result of the filtering is thus on the order of the filters.

If no specification meets in the list, the message is displayed. Empty fields are not used for comparison and thus act positively for this component. Depending on the setting, the message is suppressed or displayed. When a message is suppressed, it does not get into the database.

Specification Event (In): Definition of the incoming message

- Severity: Selection of the Severity of the incoming message
- Group: Compare entry with the attribute "Group" of the incoming message. Entry must exactly match the incoming group. If the field is empty, it means: any group
- Object (Reg.Exp.): Entry pattern for attribute "Object" of the incoming message. If the field is empty, this means: any Object
- Nodename (Reg.Exp.): Pattern (*regular expression*) for the attribute "Nodename" of the incoming message. The pattern ignores upper/lower case distinctions. If the field is empty, it means: any node name
- Event Type: Selection Box for Event Type of the incoming message, "default" means: any Event Type
- Event Text (Reg.Exp.): Entry pattern for "Event Text" of the incoming message. If the field is empty, this means: any event text
- Suppress: Check Box to permanent suppression of the message/event

The incoming message is mapped with the following specification on the outgoing message. You may redefine all the attributes of a message except for the times, Event Type and the node name.

Specification Event (Out): Definition of the outgoing message

- Severity: Converting the Severity, with "default" will keep the incoming Severity
- Group: Going out message group if it is to be different from the received
- Object: Ditto for the attribute "Object" of a received message
- Counters (MaxDisplay/.../...): A **maximum of N unequal** messages in the period are shown, but the repetition of same messages are suppressed
- .../MinDisplay/...: The following message appears after the Nth repetition of **the same** events and then only once
- .../MaxSuppress: Maximum number of suppressions a message until to the next display. The display is even after the expiry of the period.
- Suppression Time (day;hor:min:sec): Period for which the repetition of a specified message is to be suppressed; input: day(s), hour(s), minute(s), second(s); value zero (0;00:00:00) means no temporal suppression, though the Counters is not set
- Strict: The repetition of messages that differ only in the event text but in the other attributes are the same, are also suppressed, the input field for Event Text must be filled in so that the incoming message can be sufficiently identified
- Accept: Check Box to automatically acknowledge/accept a message, it will immediately archived
- Format Event Text: Input of the format string that formats the message text of the incoming event. If the field is empty, the incoming event text is output.

Processing mode by the push buttons:

- Add: Adding a filter
- Modify: Changing a filter
- Search: Search for filters
- Delete: Deleting a record for a filter. Must first be selected in the top list with the mouse, the left column Severity.
- Quit: Leave the mask without storing changes

A message is equal, if the attributes "Severity", "Nodename", "Group", "Object", "EventType" and "Event Text" match. It is not equal, if only one attribute does not match. You can transpose the event text by the format statement to remove times in log files and to remove or alter other components.

A filter that meets each message has any Severity set, no entries for Group, Object, Nodename, Event Text and Event Type is "default". Such a filter should be

at the end of the list. Before that the list items are a progressive refinement of the general case.

Note: The comparison of an incoming message with the old for the purpose of suppression takes place **after** formatting and replacing if these were provided. This means that you can determine by the way of formatting the event text, the extent to which the message is suppressed in time.

In case of replacement of the message text the original message text is preserved. Double-click on a message and the current number of suppressed messages can be seen in the widget "Event Information" in addition to the creation and reception time.

9. Mails (X11)

Setting, changing, deleting, reports of records that accomplish the forwarding of messages via SMTP mail.

When a message is received, the list of records is traversed for comparison. If the comparison is positive, a mail is sent with the specified data. You can send a message to multiple addresses.

List of mail specifications: List of existing records for the transfer of messages via SMTP mail; two push buttons Up, Down to rearrange the list; selecting a data set is done by clicking on the left-hand column (Severity) of a line.

Specification Event: Determination of forwarded messages with the attributes as they are displayed.

- Severity: Compared with the severity of the outgoing message
- Group: Comparison of the entry with the attribute "Group" of the message. The comparison is exact. If the field is empty, this means: any group
- Object (Reg.Exp.): Search pattern for the attribute "Object" of the message. If the field is empty, this means: any Object
- Nodename (Reg.Exp.): Search pattern for the attribute "Nodename" of the message. The pattern ignores upper/lower case distinctions. If the field is empty, this means: any node name
- Event Type: Selection Box for Event Type
- Event Text (Reg.Exp.): Search pattern for "Event Text" of the message. If the field is empty, this means: any Event Text
- Counters: Threshold for the number of filter-suppressed events at the Management Station or for the sum of entries found on the agent (relative to a period of suppression). Exceeding (>=) triggers the sending of an e-mail. This can be when the message appears, or later. The function is only active if the value is greater than zero
- Accept: After successfully sending the mail, the message is acknowledged

Specification Mails: Definition of mail

- Mail Server #1: Name or IP address of the Outgoing Mail Server
- Mail Server #2: Name of the backup (alternate) server after the first has failed
- Port: Transmission port (e.g. 25, 465, 587)
- MaxNumber: Maximum number of the sent mails in a period of time. It is customized for the specified message

- Time Interval (hor:min:sec): The time interval for the limitation of the number; the interval begins with the sending of the first email; at the end of the interval, the counter is reset
- OrigText: It also sends, if available, the “Original Event Text” (up to 1024 characters)
- Character Set: Character set for outgoing Event Text; ISO-8859-15 or UTF-8
- Authentication (smtp/smtps): Selection Box for authentication to the mail server (smtp, securesmtp)
- Username: User name for the mailbox
- Password: Password for the mailbox
- Password confirm: Confirmation of the password
- Text for Subject: Text for subject of the mail
- Checkbox enable: Enable/disable forwarding by mail
- Mail Address #1: First mail address
- enable: Enable/disable forwarding by mail
- Mail Address #2: Second mail address

Processing mode by the push buttons:

- Add: Add a data record
- Modify: Change a data record
- Search: Search for one or more data sets
- Delete: Deleting a data record. Must first be selected in the top list with the mouse, the left column Severity.
- Quit: Leave the mask without storing changes

10. TimeFilter (X11)

Setting, changing, deleting, reports of records for the TimeFilter, which suppress messages in a fixed time interval.

Upon receiving a message, the existing list is checked by comparison. If in a list item the comparison is positive, the message is suppressed, and the list traversal terminates. Applications for this device are for example the maintenance periods of servers.

List of TimeFilters: List of existing records for the filtering of messages and two push buttons Up, Down to rearrange the list; selecting a data set is done by clicking on the left-hand column (Severity) of a line.

Specification Event: Define messages in the form and with the attributes as they are intended for output.

- Severity: Comparison to the Severity of the message
- Group: Comparison of the input with the attribute "Group" of the message. The comparison is exact. If the field is empty, this means: any group
- Object (Reg.Exp.): Search pattern for the attribute "Object" of the message. If the field is empty, this means: any Object
- Nodename (Reg.Exp.): Search pattern for the attribute "Nodename" of the message. The pattern ignores upper/lower case distinctions. If the field is empty, this means: any node name
- Event Type: Selection Box for Event Type
- Event Text (Reg.Exp.): Search pattern for the Event Text. If the field is empty, this means: any Event Text

Specification TimeFilter: Duration of message suppression

- enable: Enable/disable the filter
- start hour (0..23): Initial hour of the time interval
- start min (0..59): Initial minute of the time interval
- duration (hh:mm): Duration of the time interval; format of input: hour:minute, maximum duration of 1439 minutes
- day of week: Day of the week
- day of month: Day of the month; value 0 means: disabled option

Processing mode by the push buttons:

- Add: Add a TimeFilter
- Modify: Changing a TimeFilter

- Search: Search for TimeFilter
- Delete: Deleting a record for a TimeFilter. Must first be selected in the top list with the mouse, the left column Severity.
- Quit: Leave the mask without storing changes

11. Export/Automatic Actions (X11)

Setting, changing, deleting, reports of records that allow the export of messages.

11.1 Processing

When a message is received, the list of records is traversed. If the comparison is positive, the message is exported to the specified program. You can export a message several times.

List of export programs: List of existing records for exporting messages; two push-button Up, Down to rearrange the list; selecting a data set is done by clicking on the left-hand column (Severity) of a line.

Specification Event: Defining the messages in the form and with the attributes as they are issued.

- Severity: Compared with the severity of the message
- Group (Reg.Exp.): Search pattern for the attribute "Group" of the message. If the field is empty, this means: any Group
- Object (Reg.Exp.): Search pattern for the attribute "Object" of the message. If the field is empty, this means: any Object
- Nodename (Reg.Exp.): Search pattern for the attribute "Nodename" of the message. The pattern ignores upper/lower case distinctions. If the field is empty, this means: any Nodename
- Event Type: Selection Box for Event Type
- Event Text (Reg.Exp.): Search pattern for the Event Text. If the field is empty, this means: any Event Text
- Counters: Threshold for the number of filter-suppressed events at the Management Station or for the number of entries detected by the agents (or the sum of them related to a period of suppression). Exceeding (>=) triggers the export of a message. This can be when the message appears, or later. The function is only active if the value is greater than zero

Program name: Declaration of the program name

- enable: On/off switching of the program
- MaxNumber: Maximum number of the exports in a period of time. It is customized for the specified message
- Time Interval (hor:min:sec): The time interval for the limitation of the number; the interval begins with the exporting of the first message; at the end of the interval, the counter is reset

- Character Set: Character set for the outgoing Event Text; UTF-8 or ISO-8859-15

Processing mode by the push buttons:

- Add: Adding an export program
- Modify: Changing an export program
- Search: Search for export programs
- Delete: Deleting a record for an export program. Must first be selected in the top list with the mouse, the left column Severity.
- Quit: Exit the mask without storing changes

11.2 Passing Parameters When Exporting

The system gives the program a total of 13 positional parameters. The position is given by the representation of a message in the Browser, reading from left to right:

1) Severity: “inform“, “minor“, “warning“, “major“, “critical“
2) Date
3) Time of day
4) Nodename
5) IP Address
6) Group
7) Object
8) Event Type
9) Event Text (Message Text)
10) Character set: “ISO-8859-15“ or “UTF8“
11) Time stamp of the receipt time
12) Time stamp of the time sent
13) Time stamp of last suppression (can also be zero)
14) Number of suppressed events
15) Number of entries determined by the agents or the sum of them (related to a period). The value zero means that it is not defined for this event
16) Time difference in seconds

Notation in a shell script:

```
#!/bin/ksh -p
typeset SEVERITY=$1
typeset DATE=$2
typeset TIME=$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
# Call of export program
exportprogram “$SEVERITY“ ... “$EVENTETEXT“
RTC=$?
exit $RTC
#end of script
```

The specified export program must be executable and return a return code of zero. Otherwise there is a system error messages. There is a timeout of 15 seconds. If this is exceeded, there is also a system error message in the log file of the background process "browserctl".

12. EcFilter (X11)

Setting, changing, deleting, reports of EcFilter that ensure that old messages are automatically acknowledged and replaced by new ones. The mechanism shall be for events that differ only in the message text, but the remaining attributes (except the date and retry count "RepCnt") are the same. When a message arrives, the list of EcFiltet is traversed and the pattern compared on one hand to the incoming Event Text and on the other hand to the Event Text of messages in the active Browser. If the comparison is positive, the replacement takes place and the list traversal terminates. At the end of the operation, the repetition counter "RepCnt" of the old message is incremented by one and the new assigned.

EcFilter: List of existing data for filtering; two push buttons Up, Down to rearrange the list; selecting a data set is done by clicking on the column EcFilter of a row.

Input EcFilter: Input for EcFilter

Processing mode by the push buttons:

- Add: Add a search pattern or a string constant for the EcFilter
- Search: Search for EcFilter
- Delete: Deleting an EcFilter. Must first be selected with the mouse from the list
- Quit: Exit the mask without storing changes

In the determination of the pattern or string constants is to make sure that it is significant enough to describe the Event Text of the message to a sufficient degree. The acknowledged messages are not lost, but can be seen in the History Data any time.

13. NodesConfig, Command Interface (X11)

Administration of the data sets for the configuration of the nodes. The configuration is done by editing the corresponding configuration files. In addition, there is the command interface for administrators and operators.

List of nodes: List of existing records for an operator; for the selection of a data set, click with the left mouse button in the left column Nodename of a row. Double-clicking on this column, the command interface is invoked (same effect as Execute). By right-clicking you call special functions depending on the other input fields. There are two push buttons Up, Down to rearrange the list.

Input fields:

- Nodename: Node name field; is in principle freely selectable but must be unique in combination with IP Address
- IP Address: IP address of the node; is the function argument for the following operations
- Admin Port: UDP port number; must match the port specified for the background process "remoteconfd" respectively "remoteconfd.exe" on the remote server
- SockType: Socket Type *udp* or *tcp*; must match the setting of "remoteconfd" respectively "remoteconfd.exe" on the remote server
- Group: Message group of the node
- Authentication String: Additional authentication string for the node; the input is necessary when for the background process "remoteconfd" respectively "remoteconfd.exe" on the opposite side of the communication the same string is agreed; the string must be at least eight characters long.
- Platform: Operating system of the node; enter Unix or Unix derivative or Windows
- Description: Description of the node, text is freely selectable
- Character Set: Definition of the character set for the node from a selection list; the list includes among others CP1250 to CP1258, ISO-8859-1 to ISO-8859-10, ISO-8859-13 to ISO-8859-16; default: UTF-8
- Remote command (batch mode): Enter a command that is executed on the target machine and its return is displayed in a widget. The command is started by the Enter key, the Push Button Execute or by the right mouse button in the table row containing the desired node. The operation takes place concurrently in the background and ends with the appearance of the editor window, which returns the result. The combo boxes Unix and Windows contain a selection of administration commands
- Execute: Call the previously entered command

- Cancel: Sends a signal to the remote server asking it to stop processing the command prematurely. The server stops running automatically after 30 seconds have elapsed (Timeout) or when the amount of data has exceeded 1 MB

The input fields Nodename, IP Address, Group and Platform serve also as a search field using *regular expressions*.

Processing mode by the push buttons:

- Refresh: Renew the display with the inputs of the search fields; if the search fields are blank, everything appears.
- EraseRefresh: Clear the entry fields and renewing the display
- Add: Adding a record with the values set in input fields
- Modify: Change a data set with the corresponding values of the input fields
- Delete: After you have selected a row in the list of nodes deleting a data record
- LookUp: Get the IP address by Nodename; get the node name by IP Address
- Quit: Close the mask

Lower right part of the mask:

- Remote edit – name of configuration file (full path name): Enter the full pathname of a file on the remote server; pressing the Enter key starts the data transfer in the background. The end of the transfer becomes recognizable by the appearance of the editor with the contents of the file. Then you can edit the content and then save back. The function can also be started by right-clicking in the desired line of the table, if the input field of "Remote command" is empty. The pushbutton Store local also allows the file to be saved on the Management Station
- ToList: Push button to get the name of the configuration file in the list of file names. The name is then stored permanently
- GetFile: Get the remote file whose name you have selected from List of files, and then call the editor to edit the file
- CheckNode: Check whether the selected node with the background process "remoteconfd" is reachable. The check can also be done by right-clicking a line in the list of nodes, if the input fields "Remote command" **and** "Remote edit" are empty.
- Remove From List: Removes a selected file name from the list of file names
- Read local files: Push Button to call a File Selection box, which selects a local file to distribute to one or more nodes. The file can also be a binary

file (program file). The size is limited to 1 MB. After selection, the contents of the file appear in the editor window. There is an additional input field for the file name on the remote server and the push button Save remote. After transferring the file, you can change the destination for distribution by right-clicking in the list of nodes and repeat the process

- List of files: List of configuration file names associated with a node. The file names appear when you click on a line in the far left column "Nodename" in the table of the server with the left mouse button. By double-clicking on a list element, the editor is called, with which you can edit the selected file

The functions specified here are executed concurrently so that there is no blocking of the user interface.

14. browserhtml (WEB)

You get the web page by logging in before with his user name and password. You can see the active messages in a table, similar to the X11 output.

The upper part is the name of the administrator or operator, the total number of messages, the number of visible messages, then the number of messages separated by Severities.

Underneath are the operating elements:

- –UpsideDown: Reverse chronological order
- ENTER: Send the page
- HistoryEvents: Call the side of history data
- Lifecheck: Call the page of Lifecheck respectively Heartbeat

One line has columns:

- Accept: Accept the message. The time of acknowledgment is registered. Similarly, the operator or administrator who has acknowledged the message
- OrMaEx: Column to inspect other attributes of a message with notice of the existence of original message text, of sent mail(s) or export(s) made; when exporting or sending mail is failed, the letter 'E' appears in red
- Sev.: Severity
- Date/Time: Reception time (date and time) of the message
- Nodename: Network name of the server
- IP Address: IP address of the node
- Group: Message group
- Object: Object of a message
- Event Type: Attribute for the classification with respect to cause and origin of a message, it is assigned by the system and can not be changed; in addition, there is a display of the total number of entries found and the corresponding time period; Example see below
- RepCnt: Retry count and right in brackets the number of suppressed messages related to this event. The information is not available when the number is equal to zero
- Event Text: Message Text of the event

The WEB page is automatically updated every 30 seconds.

Example of representing Event Type:

SyslogFormat#10/2m30s

The number after the '#' (10) character is the total number of items that have been found over a period of 2 minutes and 30 seconds for the filter concerned, regardless of how many items have been actually transferred. The format for the time specification: Ns, Nm, NmKs, Nh, NhKm; s: second, m: minute, h: hour, N,K: natural number.

14.1 History Events (WEB)

Analogous to the X11 interface you have the possibility to search for messages recognized by their attributes. The search results are tabulated. Through a check-box, you can download the search results to a file on your web front-end. Then you can work on the file.

ReceiveTime: The data of the interval relate to the reception times of the messages as they are displayed in the Browser as active messages.

- DateFrom: Date of the beginning of the interval in the past, the default is now time reduced by 12 hours
- TimeFrom: Time of the start of the interval in the past, the default is now time reduced by 12 hours
- DateTo: Date of the end of the interval, default is the present time
- TimeTo: Time of the end of the interval, default is the present time
- Checkbox now: Sets the input fields DateTo and TimeTo to the present time

Severity: Severity, one is looking. By default, all Severities are deselected. This means: all Severities

- Check Box inform
- Check Box minor
- Check Box warning
- Check Box major
- Check Box critical

The following are the input fields:

- Nodename: Looking up Nodenames with *regular expressions*. If the field is empty, this means: any node name
- Group: Search by message groups with *regular expressions*. If the field is empty, this means: any group
- Object: Search for attribute Object of a message with *regular expressions*. If the field is empty, this means: any Object
- Event Type: Selection Box for Event Type; "default" means: any Event Type
- Event Text: Search by Event Text with *regular expressions*. If the field is empty, this means: any Event Text

After that the Check Boxes:

- Slim: It lacks the attributes for AcceptTime and operator/administrator who acknowledged the message
- UpsideDown: Change of the temporal order, the oldest messages are at the top
- DownLoad: The search result is written to a text file, one line per record. The columns of each line are separated by a semicolon ';'. The length of the file is limited to 500.000 lines. The file name is assigned by the system and is: <operator_name>.html. A new search overwrites the old file.

After that the Submit Button is ENTER: Start the search process.

14.2 Lifecheck (Heartbeat, WEB)

Analogous to the X11 interface you can see the nodes that are to be monitored. The database is located on the Management Station and can therefore be viewed at any time. The list is automatically updated. An administrator has the view on all nodes, an operator only to the nodes, whose groups are assigned.

The table has the following columns:

- Nodename: Name of the server
- IP Address: IP Address of the server
- Group: Message group, wherein the server is included
- delta (sec): Indicates the time difference in seconds since the last sign of life, and in parentheses, the time limit to be observed; the value in parentheses is the sum of Polling Interval and Alarm Offset.
- Polling Interval (sev): Polling interval of the standard monitoring; it forms the basis of the time limit, above which occurs the exception handling
- LifeSev.: Color representation of the time difference. The greater the time differential delta, the longer the server has not been reported. If delta is greater than the limit, there is a critical message for this node. After three unsuccessful messages every 15 minutes, the server goes on to state "disabled".
- Last Time: Time of the last sign of life
- Date: Date of the last sign of life
- Alarm Offset (sec): Offset in seconds for the limit up to which the node must report no later than
- Ping Offset (sec): Offset in seconds for the limit after its expiration a Ping check is performed
- Sysname: Identification of the operating system

- Daemon: Indicates whether the agent is run as a daemon or not
- Check Box Disabled Nodes: Switching to the table of "disabled nodes". There are servers that have not been reported after three signaling (about 90 minutes)

With input fields you can search for specific nodes:

- Nodename: Looking up Nodename with *regular expressions*. If the field is empty, this means: any node name
- IP Address: Search by IP address with *regular expressions*. If the field is empty, this means: any IP address
- Group: Looking for Group with *regular expressions*: If the field is empty, this means: any Group

With the ENTER Submit Button starts the search process.

Below it will appear the number of nodes found:

- TotCount: Total number of nodes
- DispCount: Number of servers that are located in the display. The number is limited to 300

14.3 Configuration File “browserhtml.conf“

Configuration file for the Web interface of the Browser. In it, the environment variable "OMBDIR" and the directory for downloading is set.

Example:

```
OMBDIR=/opt/monitor/database
# Download directory: <path>:<relpath> absolute and relative path to DocumentRoot
# No entry: /var/tmp
DOWNLOAD=/var/www/monitor:/monitor
```

Document root is "/var/www". Below is the directory "monitor", in which the downloaded files to be copied.

15. Background Processes

For the following programs, the environment variable "OMBDIR" must be set. The content of the variable points to the directory containing the system files.

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

15.1 browserctl: Administrative Process

The background process performs the following functions:

- Implementation of mails
- Implementation of export programs
- Implementation of EcFiltern
- Allocation of shared memory

Call:

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

-L: Name of the log file (default: browserctl.logfile)
-m: Do not log after successfully sending of a mail to the log file

Note: When you restart the Management Station, this process must be called first.

15.2 monlistener: Receive Messages From The Agents

The background process receives the messages of the nodes on a tcp port. The port is freely selectable with an option, for example 55555. For the encrypted communication with the agents the program requires the file "monitorkeys.sig" located either in the same directory as the executable program or in the user's home directory or in the directory “/etc”.

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

-p : Port number
-4 : Receiving only ipv4, ipv4 and ipv6 without this option!
-e : Setting the environment variable "OMBDIR"

15.3 lifechecker: Management Of Lifechecker Reports

The background process manages the Lifechecker messages from the nodes. If a node has not been reported within an adjustable time interval to the Management Station, there is a signaling.

In addition, the process sends an ICMP Ping to a node if it has not been reported after more than a configurable number of seconds. If the ping is unsuccessful, there is also a signaling. For this function, the process needs root privileges.

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

-n : Call without root privileges ICMP Ping is switched off
-e : Setting the environment variable "OMBDIR"

15.4 snmptraplistener: Trap Receiver

The background process receives the SNMP Traps of types 1, 2c from the nodes and other SNMP-enabled devices. Traps of version 3 can also be received but **not** encrypted (allowed: *authNoPriv*, *noAuthNoPriv;* here not allowed: *authPriv).*

Call:

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

-p : Port number udp/tcp, preset 162/udp4+6
-t : Reception with tcp otherwise udp
-4 : Receiving only ipv4, ipv4 and ipv6 otherwise
-L : Log file name (default: snmptraplistener.logfile)
-e : Setting the environment variable "OMBDIR"

The program needs root privileges if the input for port is less than 1024.

Note: If present, the commands snmptrap(1) or snmpinform(1) can be used on any platform to send traps to the Management Station, both via tcp and over udp.

15.5 udplistener: Receiving From Other Management Stations

The background process receives messages from other Management Stations that transmit their messages. It corresponds with the program rsendmsg_udp, invoked on the sending Management Station with the export mechanism.

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

-p : Port number udp
-4 : Receiving only ipv4
-e : Setting the environment variable "OMBDIR"

16. Programs For The Command Line

For the following routines, the environment variable "OMBDIR" must be set. The content of the variable points to the directory containing the system files.

Example: OMBDIR="/opt/monitor/database"

16.1 remotecmd: Remote Call Of Commands

The program is a client program for "remoteconfd" or "remoteconfd.exe" which can execute a command on the remote node and displays the return (including Exit Status) on the Management Station. Depending on the server setting, data is transferred via Udp or Tcp.

Call: remotecmd <node name|ip address> [<command>]

The first parameter is the node name or the IP address of the remote server followed by the name of the command to be executed with any options or arguments. The server name and the associated address must have been previously set on the graphical user interface under "NodesConfig" (see above). The execution of a command can be canceled with Ctrl-C (SIGINT). The transmitted data is encrypted with AES 256-bit CBC.

Example: remotecmd 192.168.20.10 ls -lt /etc

You can also use the program to implement Automatic Actions on the nodes in response to certain messages to the Management Station.

If the second parameter <command> is missing, a prompt appears for one or more consecutive commands on the same server. This operating mode is ended by entering "quit" or "exit".

16.2 listnodes: List Of Registered Nodes

The program lists the registered nodes on a table. The table has the columns:

- Name: Nodename
- Ip: IP Address of the sender
- Group: Message group for the node
- time: Date and time of last message
- Interval: Polling interval of the agent for standard monitoring
- Sysname: Name of the operating system

- Last column: In the last column the word "DISABLED" will appear if the node is in the state "disabled"

Call: listnodes [-d <nodename>]

-d: Delete the node with the name <nodename> from the list

16.3 rsendmsg_p: Forwarding Of Messages With Tcp

The command sends a message of an export program via tcp to another Management Station by communicating with the remote listener "monlistener" via a common port.

Call:

rsendmsg_p -p <portno> -d <managementstation> [-e <alternate station>]
-i <ip-address> -u –c <charset> -g <group> -o <object> [-t <event type>] [-a <time stamp>] -s <severity> [-v <totalnumber>] [-w <diffsecs>] -m <message text>

Parameter:

+ -p: Port number tcp
+ -d: Management Station
+ -e: Alternate Management Station (optional)
+ -i: IP address
+ -u: Suppress prompt
+ -c: Character set [ISO-8859-1|UTF8]
+ -g: Message group
+ -o: Object
+ -t: Event Type (default: Import)
+ -a: Time stamp
+ -n: Nodename (optional)
+ -s: Severity [inform|minor|warning|major|critical]
+ -v: Total number of entries found
+ -w: Time difference in seconds
+ -m: Message text

Return code: 0 successful, 1 input error, 2 communication error

16.4 rsendmsg_udp: Forwarding Of Messages With Udp

The command sends a message of an export program via udp to another Management Station by communicating with the remote listener "udplistener" via a common port.

Aufruf:

```
rsendmsg_udp -p <portno> -d <managementstation> [-e <alternate station>]
-i <ip-address>   -g <group> -o <object> [-t <event type>] [-a <time stamp>] -s
<severity> [-v <totalnumber>] [-w <diffsecs>] -m <message text>
```

Parameter:

+ -p: Port number udp
+ -d: Management Station
+ -e: Alternate Management Station (optional)
+ -i: IP address
+ -u: Suppress prompt
+ -c: Character set [ISO-8859-1|UTF8]
+ -g: Message group
+ -o: Object
+ -t: Event Type (default: Import)
+ -a: Time stamp
+ -n: Nodename (optional)
+ -s: Severity [inform|minor|warning|major|critical]
+ -v: Total number of entries found
+ -w: Time difference in seconds
+ -m: Message text

Return code: 0 successful, 1 input error, 2 communication error

17. Format Strings

With the specification of SNMP Traps and filters, it is possible to change the incoming text using a format string. A format string consists of various special characters that are associated with certain operations. The special meaning of the characters can be switched off, preceded by a backslash '\'.

There are the special characters:

- $n or ${n}: n is a number [1..99]. Outputs the <n>th word of the input text
- %n or %{n}: Shift to the left, outputs the <n> columns to the left shifted input text, the input line remains unchanged
- &n or &{n}: Shift of <n> characters to the left of the input text, there is no immediate output, the new beginning of the text input field is automatically set to the beginning of a word or column
- &{n,m}: Outputs <m> characters from the <n>th character of the input line
- &{n[#|]substring}: Search for a sub-string in a word. Outputs from the <n>th character to the sub-string substring in the same word. If substring is not found, the output is to the end of the word (special character is either '|' or '#')
- @n or @{n}: Shift to the left by <n> columns in the input line, the original column <n+1> is then the beginning of the input line, there is no direct output
- %<[n|]substring>: Search for a sub-string in the whole line or optionally after the <n>th occurrence of a sub-string in the line (n > 0). Then shift left until substring in the input line. The sub-string found is the new beginning of the input line, there is no direct output
- ?<[n|]substring>: Outputs the sub-string shifted to the left of the text input line. If sub-string is found, terminates the formatting, otherwise continue with the following special characters; optional search for multiple occurrences
- -<[n|]substring>: Outputs the at the point of occurrence of sub-string substring truncated input text, the found sub-string is cut off, the input line remains unchanged; optional search for multiple occurrences
- $*: Outputs the whole line
- $$: Outputs the last column of the input text

A word is a coherent text delimited by blanks. A line is a sequence of words. If the format string does not contain any special characters, the line found or the found entry is mapped to the string constant. The search for a sub-string happens from left to right. If the number <n> is not reached during the repeated search, the rightmost sub-string is taken. If the sub-string is not found, no operation is done.

Example 1:

The following line from the log file analysis is to be formatted:

```
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]
```

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

or “$1%<] >@1 &{1#[}: %1“

Output for the event text of the Browser:

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

The term "$1" sets the first word of the input line to the first position of the output line. The expression "%<] >" (or "%<1|] >") shifts the input line to the left until the first occurrence of the sub-string "] ". The following "@1" shifts the input line again one column to the left so that the sub-string disappears. By the expression "&{1#[}” (or "&{1|[}”) the column "httpd[2751]" is cut off at the point "[" and becomes "httpd". Finally, by the operator "%1", the line is output by one column shifted to the left. The results of the different operations are chained together in the output.

Example 2: Formatting SNMP trap text

```
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
```

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

Output: ssCpuIdle: 1% (SERVERX 1.3.6.1.4.1.2021.

The expression "% <7| 1.3.6.1." shifts the input line to the left until the seventh occurrence of the sub-string " 1.3.6.1." to the new line beginning. "$3" outputs the third column/word, "%4" outputs the line shifted four columns to the left, surrounded by "(" and ")".

18. Regular Expressions (Search Patterns)

The system uses *extended regular expressions* according to the POSIX standard as search pattern. The properties can be found in the *manual pages* of Unix. For the special requirements of this system, there are optional additions that are appended to the end of the search pattern after a slash ‘/’.

The syntax is: <RegExp>[/i|v|!]

The real search pattern followed by '/' and 'i' or 'v' or '!'.

The meaning of the symbols:

- ‘i’: Perform case insensitive matching
- ‘v’: The search result is reversed, case sensitive matching is performed
- ‘!’: The search result is reversed, case **insensitive** matching is performed

The special importance of the option can be switched off with a preceding backslash ‘\’.

Examples:

“^os$/i” will match the string “OS”, “Os”, “oS”, “os”
“fatal/i” will match lines containing “Fatal”, “FATAL”, “fatal”, ...
“[0-9]/v” will match lines not containing any digits
“ABC/v” will match lines **not** containing “ABC”
“ABC/!” will match lines **not** containing “Abc”, ABC”, “abc”, ...
“[ ][1-9][0-9]{1,2}[ ]/v” will match a number that has more than three places
“[ ]3\.14[0-9]*[ ]” will match the number 3.14...
“[ ]([3-9][0-9]{5})|([1-9][0-9]{6,})[ ]” will match a number that is greater or equal 300000

19. Installation

The background processes should be assigned to an unprivileged user. To start at system boot, there are the following entries in the "rc.local" file under the directory "/etc". The process "browserctl" must be started first:

```
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 &’
# Listens to port 5555/tcp, ipv4 and ipv6
sleep 1
su monitor -c ’/home/monitor/portchecker/portchecker -e $OMBDIR &’
/home/monitor/lifechecker/lifechecker &
# Root permission because of ICMP
/home/monitor/snmptraps/snmptraplistener &
# Listens to port 162/udp, ipv4 and ipv6
logger “Server process started“
su - monitor -c /home/monitor/agents/basemonagent
logger “Agent for standard monitoring started“
```

It is "monitor" the name of a non-privileged user. Under this, the management of the data takes place. The Gui-program "browser" can be provided with the setuid bit, since it's not owned by root.

Another possibility is the use of *systemd* (system and service manager Linux). Set a file <name>.service in the “/lib/systemd/system” directory (Debian) for each background process. The corresponding process can be started and stopped using the *systemctl* command.

Example:

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

A third possibility is to use the agent for standard monitoring. It has the advantage that the background processes are monitored during operation, and started again when needed.

Entries 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
```

The agent program is called by "cron" for root. Crontab entry:

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

20. Event Types

Attribute for the classification of messages through the system

Event Type	Function	Program
Filesystem	Monitoring file systems	basemonagent, winmonagent.exe
Inode	Utilization rate Inodes of file systems	basemonagent
Process	Process monitoring Unix	basemonagent
ProcessRestart	Start background processes	basemonagent
WinTask	Monitoring tasks in Windows	winmonagent.exe
WinService	Monitoring of Windows Services	winmonagent.exe
Syslog	Log file analysis of system log files	basemonagent
SyslogFormat	Log file analysis with formatting by the agent	basemonagent
Logfile	Log file analysis	logmonagent, asyncmonagent, asyncmonagent.exe, logmonagent.exe
LogfileFormat	Log file analysis with formatting by the agent	logmonagent, asyncmonagent, asyncmonagent.exe, logmonagent.exe
Frequency	Log file analysis and monitoring scripts by displaying the number of lines found for a search pattern	basemonagent, logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe, scriptmonagent, scriptmonagent.exe, logdiragent, logrecagent
WinSysEventlog	Monitoring system event log Windows	winmonagent.exe
WinApplEventlog	Monitoring application event log Windows	winmonagent.exe

WinSecEventlog	Monitoring security event log Windows	winmonagent.exe
Performance	Monitoring Load Average, Swap, Memory, CPU	basemonagent, winmonagent.exe
ScriptStd	Monitoring scripts	basemonagent, winmonagent.exe
ScriptStdFormat	Monitoring scripts with output formatting on agents	basemonagent, winmonagent.exe
Snmptrap	SNMP-Notifications	snmptraplistener
Portcheck	Check remote ports	portchecker
PortcheckLocal	Local check of ports	basemonagent, winmonagent.exe
Uptime	Signaling reboots	basemonagent, winmonagent.exe
Import	Display imported messages from other Management Stations	rsendmsg_p, rsendmsg_udp, monlistener, udplistener
Rsendmsg	Direct message to the Management Station	rsendmsg
Zombie	Monitoring zombie processes	basemonagent
System	System messages	Management-Station
SystemAgent	System messages	Agenten
Filesize	Monitoring size of files	basemonagent, logmonagent, asyncmonagent, logmonagent.exe, asyncmonagent.exe, logdiragent, logrecagent
PingCheck	Heartbeat/Lifecheck	lifechecker
LogfileTotal	Log file analysis	logmonagent, asyncmonagent, logmonagent.exe, asyncmonagent.exe
LogfileTotalFormat	Log file analysis with formatting at the agent	logmonagent, asyncmonagent, logmonagent.exe, asyncmonagent.exe
LogfileDir	Log file analysis of	logdiragent

	directories	
LogfileDirFormat	Log file analysis of directories with formatting output at the agent	logdiragent
LogfileRec	Log file analysis of directories and subdirectories	logrecagent
LogfileRecFormat	Log file analysis of directories and subdirectories with formatting of the output at the agent	logrecagent
Script	Monitoring scripts	scriptmonagent, asyncmonagent, asyncmonagent.exe, scriptmonagent.exe
ScriptFormat	Monitoring scripts with output formatting at the agent	scriptmonagent, asyncmonagent, asyncmonagent.exe, scriptmonagent.exe
Permission	No permission to read log files	basemonagent, logmonagent, asyncmonagent, logmonagent.exe, asyncmonagent.exe, logdiragent, logrecagent
Existence	Destination file does not exist	basemonagent, logmonagent, logmonagent.exe, asyncmonagent, asyncmonagent.exe, logdiragent, logrecagent
RegExpression	Error in regular expression	Agenten
Heartbeat	Failure messages, logout from nodes, sign of nodes	monlistener, lifechecker
Security	Changes to the file system	secmonagent