User Guide - English

FUJITSU

ServerView Suite

ServerView Event Manager

ServerView Operations Manager V6.00

Edition July 2012

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Contents

1 Introduction

The ServerView Event Manager (called simply Event Manager below) is a component of the Event Management of the ServerView Suite. After installation, this component is available both via the Windows Start Menu and via ServerView Operations Manager (called simply Operations Manager below).

The Event Manager function has a user-friendly Web-based graphical user interface (GUI) where you can obtain reliable, secure information about system faults quickly.

You can define the results and operating states about which you want to receive alarm messages. The availability of a server in a network is a critical factor and it therefore makes sense to configure the Event Manager so that you are informed about all the operating states that could endanger server availability.

On blade systems, the Event Manager can receive and display alarm messages from the blade system itself and also from individual server blades. Alarms are assigned to the entire blade system by default. This setting can be changed in the configuration.

The Event Manager works like this. An agent sends an alarm (trap) over the SNMP to the Event Manager informing the management station that an unexpected event has occurred. An unexpected event can be an error report or a status change caused by tripping of a threshold value.

Traps are assigned the severity levels: critical, major, minor and informational. Different actions, triggered by traps, can be assigned to each severity level and to each server. Events at the alarm severity level *critical* are always recorded in the alarm log of the log file.

i When you are installing the agents you can also specify that alarm messages are to be sent to the Windows event log.

1.1 Changes from the previous version

This edition is valid for the Event Manager of ServerView V6.00 and replaces the online manual: “Event Manager“ as of ServerView V5.50, Edition November 2011.

The manual has been updated to reflect the latest software status and includes the following additions:

- Alarm entries can be filtered by clicking the corresponding filter icons in the header of the alarm list (see section "Filtering alarm entries" on page 25). Because of the filter icon, chapters *Setting the number of alarms per page* and *Managing the alarm list* have been omitted.
- Settings of an existing alarm rules can be copied to new alarm rules (see section "Managing alarm rules" on page 40).

1.2 ServerView Suite link collection

Via the link collection, Fujitsu Technology Solutions provides you with numerous downloads and further information on the ServerView Suite and PRIMERGY servers.

For ServerView Suite, links are offered on the following topics:

- Forum
- Service Desk
- Manuals
- Product information
- Security information
- Software downloads
- Training

The downloads include the following:

- Current software versions for the ServerView Suite as well as additional Readme files.
- Information files and update sets for system software components (BIOS, firmware, drivers, ServerView agents and ServerView update agents) for updating the PRIMERGY servers via ServerView Update Manager or for locally updating individual servers via ServerView Update Manager Express.
- The current versions of all documentation on the ServerView Suite.

You can retrieve the downloads free of charge from the Fujitsu Technology Solutions Web server.

For PRIMERGY servers, links are offered on the following topics:

- Service Desk
- Manuals
- Product information
- Spare parts catalogue

Access to the ServerView link collection

You can reach the link collection of the ServerView Suite in various ways:

1. Via ServerView Operations Manager.

   ► Select *Help – Links* on the start page or on the menu bar.

   This opens the start page of the ServerView link collection.

2. Via the ServerView Suite DVD 2 or via the start page of the online documentation for the ServerView Suite on the Fujitsu Technology Solutions manual server.

   i You access the start page of the online documentation via the following link:

   http://manuals.ts.fujitsu.com

   ► In the selection list on the left, select *Industry standard servers*.

   ► Click the menu item *PRIMERGY ServerView Links*.

   This opens the start page of the ServerView link collection.

3. Via the ServerView Suite DVD 1.

   ► In the start window of the ServerView Suite DVD 1, select the option *Select ServerView Software Products*.

   ► Click *Start*. This takes you to the page with the software products of the ServerView Suite.

   ► On the menu bar select *Links*.

   This opens the start page of the ServerView link collection.

1.3 Documentation for ServerView Suite

The documentation for the ServerView Suite can be found on the ServerView Suite DVD 2 supplied with each server system.

The documentation can also be downloaded free of charge from the Internet. You will find the online documentation at *http://manuals.ts.fujitsu.com* under the link *Industry standard servers*.

1.4 Notational conventions

The following notational conventions are used in this manual:

⚠ **Caution**	This symbol points out hazards that can lead to personal injury, loss of data or damage to equipment.
ℹ	This symbol highlights important information and tips.
►	This symbol refers to a step that you must carry out in order to continue with the procedure.
italic	Commands, menu items, names of buttons, options, variables, file names and path names are shown in *italics* in descriptive text.
`fixed font`	System outputs are indicated using a `fixed font`.

`semi-bold`
`fixed font`
	Commands to be entered via the keyboard are written in a semi-bold fixed font.

Key symbols	Keys are shown according to their representation on the keyboard. If uppercase letters are to be entered explicitly, then the Shift key is shown, e.g. SHIFT - A for A. If two keys need to be pressed at the same time, this is shown by placing a hyphen between the two key symbols.

Table 1: Notational conventions

References to text or sections of text in this manual are shown with the chapter or section heading and the page on which that chapter or section begins.

Screen outputs

Please note that the screen output is dependent in part on the system used and therefore some details may not correspond exactly to the output you will see on your system. You may also see system-dependent differences in the menu items available.

2 Event Manager

The Event Manager allows you to filter and forward alarm messages and specify the display.

For monitoring, ServerView agents must be installed on the managed servers and for servers with VMware vSphere ESXi 5 ServerView ESXi 5 CIM Provider must be installed. If an unusual operating status occurs, the ServerView agents automatically send an alarm (trap) to a management station. Which management stations are to receive traps is defined during installation of the ServerView agents or ServerView ESXi 5 CIM Provider. While setting up the SNMP service on the management station, you define the managed servers from which traps are to be received.

After installing the Event Manager you must first configure the alarm display and alarm handling. You do this by defining alarm rules and filter rules in the Alarm Configuration component. Using alarm rules, you specify which alarms are to be forwarded from which servers to which destinations. You can also specify, via filter rules, which alarms from which servers are to be filtered out. For a detailed description of this alarm configuration see the chapter "Alarm configuration" on page 37.

The Alarm Monitor component displays the received alarms, depending on the configuration set. The Alarm Monitor offers you further functions for editing the alarm list as well as for additional filtering of the alarm display. You can, for example, specify which alarms from which servers are not to be shown in the alarm list. For a detailed description of the Alarm Monitor see the chapter "Alarm Monitor" on page 21.

ServerView comes with a series of MIBs, which are integrated in the Event Manager. Traps from these MIBs can be received and processed in the Event Manager. To supplement the existing MIBs, additional third-party MIBs can be integrated into the Event Manager. Traps from these MIBs are also displayed in the Event Manager, once the MIB has been checked.

You integrate the MIBs using the MIB Manager, which is additionally provided when the Event Manager is installed under Windows or Linux. For more information on this tool, see the chapter "MIB integration" on page 171.

CIM-Indications for VMware vSphere ESXi 5

Events of servers with VMware vSphere ESXi 5 are provided as CIM indications. The CIM indications are analyzed by the ServerView Event Manager, which can manage and forward them as usual.

Via *Test Connectivity* you can test the connection to the VMware vSphere ESXi 5 server (see User Guide „ServerView Operations Manager“ manual).

The CIM indication provider is provided for the following operating system:

– VMware vSphere ESXi 5

For more information on ServerView ESXi CIM provider, see the "Monitoring VMware based PRIMERGY servers with ServerView" manual.

2.1 Installing the Event Manager

The Event Manager is part of the ServerView software, which can be found on the ServerView Suite DVD 1 (via Select ServerView Software Products). It can be installed under Windows and under Linux operating systems (SuSE and Red Hat). For details of how to install the ServerView software, see the ServerView Installation Guides.

2.2 Starting the Event Manager

If the Event Manager is installed on a Windows-based management station, you can start it directly on the management station via the Windows start menu.

- ► Select *Start – [All]Programs – Fujitsu – ServerView Suite – Event Manager – Event Manager.*

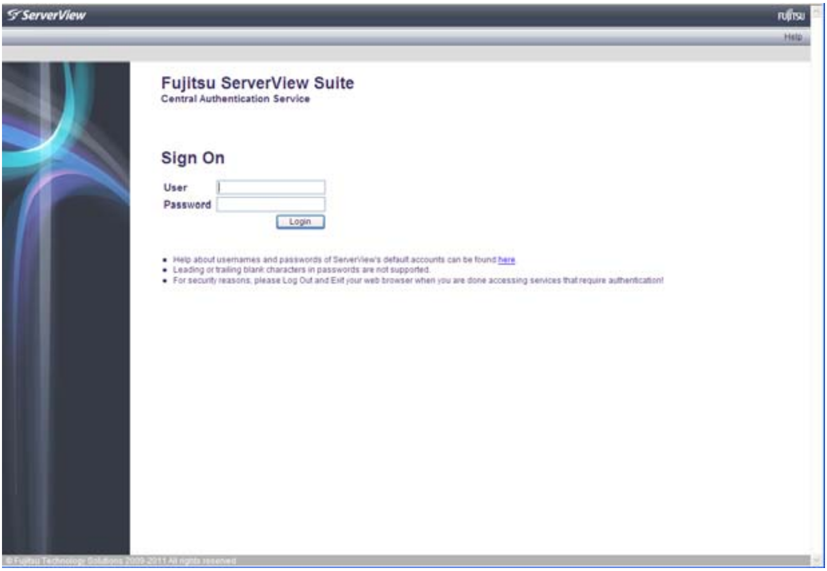
If the Event Manager Manager is installed on a Linux-based management station, you can start ServerView Event Manager via a suitable Web browser with the following Web addresses below:

- ► Enter the following Web address for SSL-protected (Secure Socket Layer) communication:

  https://<system_name>.<domainname>[:3170]/AlarmService

On startup the login window of the Central Authentication Service is displayed.

> i If the server's IP address is an IPv6 address, you must enter it in square brackets if you specify a port number.



Fujitsu ServerView Suite
Central Authentication Service

Sign On

- Help about usernames and passwords of ServerView's default accounts can be found here
- Leading or trailing blank characters in passwords are not supported.
- For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication!

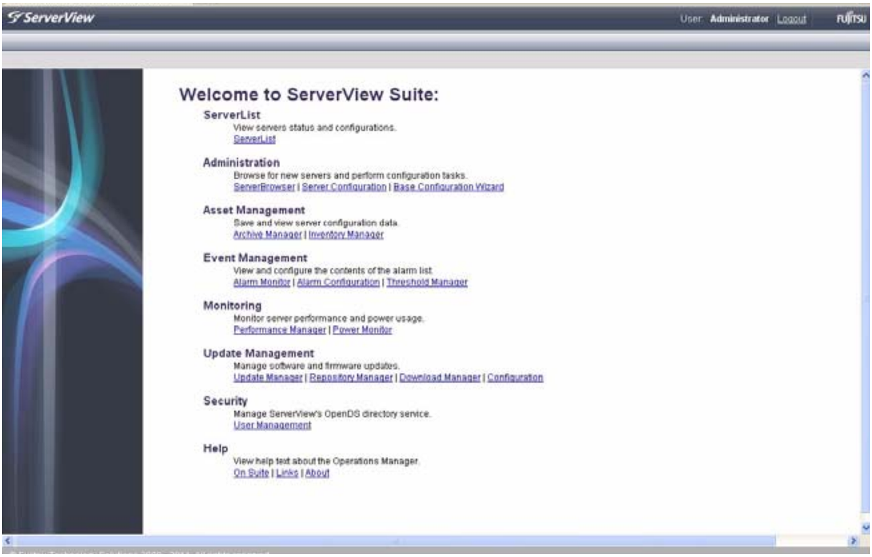
© Fujitsu Technology Solutions 2009-2011 All rights reserved

Figure 1: Login window of the Central Authentication Service

In this window, enter the user name and the password of the ID under which you are authorized to use Event Manager.

To start / operate the Event Manager, you need the appropriate permissions. As the RBAC (Role-based access control) based user management of the ServerView Suite controls the assignment of permissions to users by means of user roles, please ensure that your user role is equipped with the required privileges. For details see the "User Management in ServerView" user guide.

When you launch the Event Manager, the following start page is displayed:



Welcome to ServerView Suite:

ServerList
View servers status and configurations.
ServerList

Administration
Browse for new servers and perform configuration tasks.
ServerBrowser | Server Configuration | Base Configuration Wizard

Asset Management
Save and view server configuration data.
Archive Manager | Inventory Manager

Event Management
View and configure the contents of the alarm list.
Alarm Monitor | Alarm Configuration | Threshold Manager

Monitoring
Monitor server performance and power usage.
Performance Manager | Power Monitor

Update Management
Manage software and firmware updates.
Update Manager | Repository Manager | Download Manager | Configuration

Security
Manage ServerView's OpenDS directory service.
User Management

Help
View help text about the Operations Manager.
On Suite | Links | About

Figure 2: Event Manager start window

Depending on whether only the Event Manager is installed or which privileges have been assigned to the user of the above **Sign On**, you will have access to some or all of the listed functions. The functions you are not authorized to use will either be disabled (gray) or not listed.

For an overview of the functions available to you with a role, see the manual "User management in ServerView”.

The first time you start ServerView Event Manager as administrator after installation, the Base Configuration Wizard also starts automatically. This wizard guides you through the initial steps for using ServerView Operations Manager.

If you do not want to automatically open the Base Configuration Wizard again when you start the Event Manager, select *Do not show this wizard again automatically* in the start window of the Base Configuration Wizard. Once you have been through the Base Configuration Wizard, it too will no longer be launched automatically. You can also call up the wizard at any time via ServerView Operations Manager under the *Administration* menu.

For more information see the separate documentation for the Base Configuration Wizard.

i If you get a security warning from Java when you start Event Manager, you can ignore it by clicking *No*. How to avoid such messages in future is described in the ServerView Operations Manager Installation Guide for Windows.

You start the individual components of the Event Manager (Alarm Monitor and Alarm Configuration) by clicking the corresponding link (*Alarm Monitor* or *Alarm Configuration*) under *Event Management*.

You can also start the individual components via the start page of ServerView Operations Manager.

► Select *Start – [All]Programs – Fujitsu – ServerView Suite – Operations Manager – Operations Manager.*

Then, as with the Event Manager, click the relevant link *(Alarm Monitor* or *Alarm Configuration)* under *Event Management*.

2.3 Icons

You will find a list of the icons in the *Alarm Monitor* and *Alarm Configuration* windows and their meanings in the following.

🔔	Red alarm: critical
🔔	Orange alarm: major
🔔	Yellow alarm: minor
🔔	Blue alarm: informational
🔔	Gray alarm: unknown
🔕	Alarm is ignored
✓	The alarm was confirmed by a user entry.
EXE	Some other executable program was triggered by this alarm.
📢	A broadcast message was sent for this alarm.
✉	A mail was sent for this alarm.
📟	This alarm triggered a pager call.
🖥	This alarm will be passed on to a management station.
📓	This alarm will be passed on to the local system event log.
📟	Green: Pager confirmed
📟	Yellow: Pager completed
📟	Red: Pager present (still active)

Table 2: Icons in the Alarm Monitor and Alarm Configuration

🟨	Yellow: Forwarding completed
🟥	Red: Forwarding present (still active)
▽	Table columns can be filtered according to different criteria.

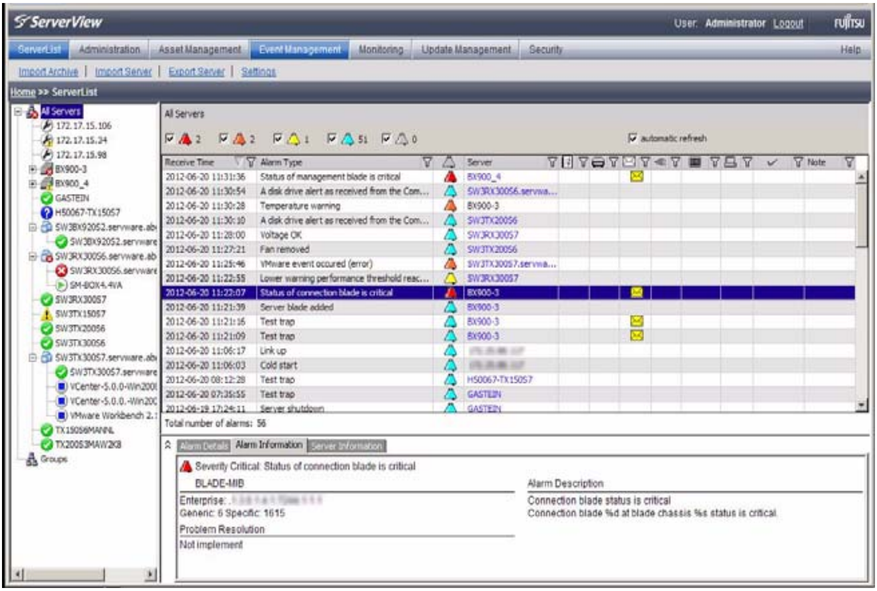
Table 2: Icons in the Alarm Monitor and Alarm Configuration

3 Alarm Monitor

The Alarm Monitor component displays all received alarms relating to the selected servers and server groups in the Operations Manager main window.

3.1 Viewing alarms

You start the Alarm Monitor via Event Manager start window (see page 15) or via the Operations Manager start window by clicking the *Alarm Monitor* link under *Event Management*. How to start Operations Manager is described in the ServerView Operations Manager documentation.



All Servers

Receive Time	Alarm Type		Server
2012-06-20 11:31:36	Status of management blade is critical	▲	BX900_4
2012-06-20 11:30:54	A disk drive alert as received from the Com...	▲	SW3RX30056.serverwa...
2012-06-20 11:30:28	Temperature warning	▲	BX900-3
2012-06-20 11:30:10	A disk drive alert as received from the Com...	▲	SW3TX20056
2012-06-20 11:28:00	Voltage OK	▲	SW3RX30057
2012-06-20 11:27:21	Fan removed	▲	SW3TX20056
2012-06-20 11:25:46	VMware event occured (error)	▲	SW3TX30057.serverwa...
2012-06-20 11:22:55	Lower warning performance threshold reac...	▲	SW3RX30057
2012-06-20 11:22:07	Status of connection blade is critical	▲	BX900-3
2012-06-20 11:21:39	Server blade added	▲	BX900-3
2012-06-20 11:21:16	Test trap	▲	BX900-3
2012-06-20 11:21:09	Test trap	▲	BX900-3
2012-06-20 11:06:17	Link up	▲	[redacted]
2012-06-20 11:06:03	Cold start	▲	[redacted]
2012-06-20 08:12:28	Test trap	▲	HS0067-TX15057
2012-06-20 07:35:55	Test trap	▲	GASTEIN
2012-06-19 17:24:11	Server shutdown	▲	GASTEIN

Total number of alarms: 56

Severity Critical: Status of connection blade is critical

BLADE-MIB

Enterprise: [redacted]
Generic: 6 Specific: 1615

Problem Resolution

Not implement

Alarm Description

Connection blade status is critical
Connection blade %d at blade chassis %s status is critical

Figure 3: Alarm Monitor

The window is divided into four sections:

- The menu bar below the title bar allows you to navigate between the Operations Manager functions:

  – Serverlist
  – Administration
  – Asset Management
  – Event Management
  – Monitoring
  – Update Management
  – Security (only if OpenDS is used as directory service)

  In the line below the menu bar, the individual menu items are listed, depending on which menu is selected.

  For more information on the menus in the menu bar, see the ServerView Operations Manager User Guide.

  i The menus excepting the Event Management menu are only available if Operations Manager is also installed on the management station.

- The left section shows a file tree structure containing the servers and server groups. This is where you make your selection for the display in the alarm or server list.

  i If you move the mouse pointer over a server in the file tree, a tooltip appears. The content of the tooltip depends on the length of the server name. If the server name is truncated in the file tree, the tooltip shows first the complete server name and below it the server type. If the server name is not truncated, the tooltip only shows the server type.

- The top right section of the window contains the alarm entries for the servers selected in the file tree. The alarm list is structured in pages.

  The icons in the header of the right-hand section indicate how many alarm entries per severity level there are on a page of the alarm list.

  You can use these icons to control the alarm list display. Click to select the alarm levels for which you want to display alarm messages.

  The display update in the Alarm Manager can be enabled or disabled via *automatic refresh*. If *automatic refresh* is selected, the display is reloaded automatically when an alarm is logged. Otherwise, only the display of logged alarms for *Total number of alarms* changes.

Below the status bar the alarm entries are displayed with the following information:

Receive Time
Time when the alarm was received.

Alarm Type
Brief description of the alarm.

Alarm icon (see table below)
Indicates the severity of the alarm.

Server
Server name. If you click the server name, the *ServerView [servername]* window opens, in which you can request detailed information about the selected server. For more information see the ServerView Operations Manager manual.

ℹ The *ServerView [servername]* window only opens if Operations Manager is also installed on the management station.

Forwarding icons (see table below)
Indicates the type of alarm forwarding.

Ack
Indicates whether the alarm was acknowledged.

Note
Indicates a note entered by the user.

The icons have the following meanings:

🔔	Indicates the alarm level.
📋	The alarm was written to the local event log.
📟	This alarm triggered a pager call.
✉	A mail was sent for this alarm.
📢	A broadcast message was sent for this alarm.

Table 3: Icons in the Alarm Monitor

EXE	An executable program was triggered by this alarm.
🖥	This alarm was forwarded to the management station.

Table 3: Icons in the Alarm Monitor

- In the bottom right section of the window you can find out information on the selected alarm entry in the alarm list via the two or three tabs provided:
  - *Alarm Details* tab - contains a brief description of the selected alarm entry in the alarm list.
  - *Alarm Information* tab - contains detailed information on the selected alarm entry as stored in the MIB.
  - *Server Information* tab - provides information on the server from which the selected alarm entry originates. Under *General Information* you will see general information about the server (e.g. system name, IP address, community name) and under *Additional Information* you will see additional information as stored in the Server Properties (e.g. administrator, location, model).

    On this tab you will also find a link, depending on whether the server in question is entered in the ServerView server list or not.

    If the server is in the server list, you can use the *Edit Server Settings* link to open the *Server Properties* window for this server, via which you can change the configured values for the server.

    If the server is not in the ServerView server list, you can use the *Add Server* link to start the Server Browser and add the server to the list. For more information on the Server Properties and the Server Browser, see the ServerView Operations Manager User Guide.

    The *Server Information* tab is only available if both the event manager and the Operations Manager are installed on the management station.

3.2 Viewing alarms for a server

If several alarm messages have been received for a server, the one with the highest severity level is displayed in the server list. In the bottom display area you will only see information on the last alarm message received with this severity.

To get an overview of all alarm messages for this server, you can switch to the Alarm Monitor function for this server only.

One way of doing this is to select the server in the file tree and start the Alarm Monitor function via the menu bar in the Operations Manager main window.

A much quicker way is via the alarm icon (the alarm bell) in the server list. If you click the alarm icon, you switch to the Alarm Monitor function for this server only. This means that only the alarm messages for this particular server will be visible in the list section of the Operations Manager main window. Through appropriate selection of an alarm message in the alarm list, you can retrieve further information on every alarm message received in the display area.

3.3 Filtering alarm entries

You can filter the alarm entries by clicking the corresponding filter icons in the header of the alarm list.

Filter icon in the header of the alarm list.

When you click the filter icon, the associated dialog *Filtering for Column <column_name>* opens in each case. Make your selection and confirm it with *OK*. Then, only the filtered entries will be displayed, depending on what you have selected. In the standard filter (*Standard*), all selection elements are selected via checkboxes. In the customized filter (*Customize*), you either enter your selection directly or using an asterisk as a placeholder. An active filter is indicated by a blue filter icon.

3.4 Processing alarm entries

The following functions are available for processing the alarm entries:

– Acknowledge alarms
– Suppress alarms
– Reset alarm suppression
– Delete alarms

3.4.1 Acknowledging alarms

You can acknowledge alarms that have been received.

Proceed as follows:

► Select the alarm entries in the list.

► Select *Ack Alarm* from the context menu.

The acknowledgment is indicated in the *Ack* column with the following icon:

✓

3.4.2 Suppressing alarms

You can suppress individual alarms of a server. This is useful if the management station is being bombarded with messages from a server that is not running correctly.

Proceed as follows:

► Select the alarm entries in the list.

► Select *Suppress* from the context menu.

You must confirm the alarm suppression. Once you have done this, all alarm entries will be deleted from the alarm list and no further alarms of this type for the server in question will be added to the list.

You can reset this setting via *Filter Settings*, see section "Resetting alarm suppression" on page 27.

i When the server starts up, a RAID manager or Ethernet card, etc. may issue an alarm (SNMP trap) as a startup notification (e.g. RFC1157LinkUP). To suppress this kind of alarm, you can configure alarm suppression. This function must be specified for each server. If multiple servers are monitored, configure this setting for each server using the alarm function.

3.4.3 Resetting alarm suppression

You can reset an alarm suppression that has already been set. Proceed as follows:

► Select *Filter Settings* from the context menu.

The *Reset suppressings* window opens, in which all previously set alarm suppressions are listed. To reset a suppression, proceed as follows:

► Select the relevant suppression in the list.

► Click the *Delete* button.

► To close the window, click the *Close* button.

The entry is removed from the list and the alarm setting is active again.

3.4.4 Deleting alarms

To delete alarm entries, proceed as follows:

► Select the alarm entries in the list.

► Select *Delete* from the context menu.

i Alarms with the severity *critical* cannot be deleted until they have been acknowledged.

3.5 Testing the connection

To test the connection to a specific server, you can send a trap. Proceed as follows:

- ► Select *Test Trap* from the context menu.

The *Test Trap* window opens:

- ► Either select the server from the list under *Serverlist*,

  or

- ► Enter the IP address of the server. If you wish you can specify the server name.
- ► Either accept the default values for *Community* and *Timeout* or enter the relevant values in these fields.
- ► To test the connection, click the *Test trap* button.

A window informs you of the connection status. To close this window, click the Close button.

i *Note for Linux*

If you perform a connection test for the local host (127.0.0.1/localhost), the test trap times out. This is because the system is waiting for a response from the IP address of the local host to which ServerView Operations Manager made the request, whereas the actual response received by the trap comes from the real IP address of the server specified in the SNMP master agent.

3.6 Other settings

3.6.1 Editing an alarm note

You can edit the note displayed for an alarm entry:

- ► Click the relevant alarm entry.
- ► Select *Edit Note* from the context menu.

The *Edit Note* window opens:

- ► Enter your text.
- ► Confirm your input with *OK*.

3.7 iRMC S2 SEL entries relayed as SC2 MIB traps

The following table applies to PRIMERGY systems manufactured in 2009 or later.

If the iRMC S2 writes an event to the System Event Log (SEL), in some cases an SNMP trap is triggered. The following table shows the correlation between the iRMC S2 entries in the SEL and the traps they trigger.

Not all iRMC S2 entries made in the SEL trigger an SNMP trap. Some trigger the same trap.

Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
000011	System event log (SEL) warning threshold exceeded	The System Event Log for cabinet XY at server XY has exceeded XY percent of its capacity.	2101	sc2TrapMessageLogWarning
040000	’FAN XY’: Fan failed	Fan ’FAN XY’ failed in cabinet XY of server XY.	2014	sc2TrapFan Failed
040001	’FAN XY’: Fan is working	Fan ’FAN XY’ was added into cabinet XY of server XY.	2010	sc2TrapFan Added
		Fan ’FAN XY’ in cabinet XY of server XY is working again.	2012	sc2TrapFanOk
040002	’FAN XY’: Fan prefailure	Fan ’FAN XY’ will fail in near future in cabinet XY of server XY.	2013	sc2TrapFan Critical

Table 4: iRMC S2 SEL entry - SC2 MIB trap

Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
040003	’FAN XY’: Redundant fan failed	The redundant fan ’FAN XY’ failed in cabinet XY of server XY. System can become critical if another fan in this group fails.	2015	sc2Trap RedundantFan Failed
040004	’FAN XY’: Fan removed	Fan ’FAN XY’ was removed from cabinet XY of server XY.	2011	sc2TrapFan Removed
050001	’Temp XY’: Temperature OK	Temperature at sensor ’Temp XY’ in cabinet XY of server XY is within normal range.	2020	sc2TrapTemp Ok
050016	’Temp XY’: Temperature warning	Temperature at sensor ’Temp XY’ in cabinet XY of server XY has reached the warning level.	2021	sc2TrapTemp Warning
050017	’Temp YX’: Temperature critical	Temperature at sensor ’Temp XY’ in cabinet XY of server XY has reached the critical level.	2022	sc2TrapTemp Critical
070000	’PSU XY’: Power supply removed	Power supply ’PSU XY’ in cabinet XY at server XY was removed.	2031	sc2TrapPower Supply Removed

Table 4: iRMC S2 SEL entry - SC2 MIB trap

Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
070001	’PSU XY’: Power supply OK	Power supply ’PSU XY’ in cabinet XY at server XY was added.	2030	sc2TrapPower SupplyAdded
		Power supply ’PSU XY’ in cabinet XY at server XY is working again.	2032	sc2TrapPower SupplyOk
070002	’PSU XY’: Power supply failed	Power supply ’PSU XY’ in cabinet XY at server failed.	2034	sc2TrapPower SupplyFailed
		Redundant power supply ’PSU XY’ in cabinet XY at server XY failed. System can become critical if another power supply fails.	2035	sc2Trap Redundant PowerSupply Failed
070003	’PSU XY’: Redundant power supply AC failed	AC failure in cabinet XY of server XY.	2040	sc2TrapAcFail
070005	Power unit: power supply redundancy lost	Power supply redundancy in cabinet XY at server XY lost. System will become critical if a power supply fails.	2036	sc2TrapPower Supply Redundancy Lost
070009	’PSU XY’: Redundant power supply DC failed	DC power failure in cabinet XY of server XY.	2041	sc2TrapDcFail
070010	’PSU XY’: Power supply fan failure	Fan failure at power supply ’PSU XY’ in cabinet XY of server XY.	2039	sc2TrapPower SupplyFan Failure

Table 4: iRMC S2 SEL entry - SC2 MIB trap

Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
07000A	’PSU XY’: Power supply critical temperature	Temperature at power supply ’PSU XY’ in cabinet XY of server XY has reached the critical level.	2037	sc2TrapPower SupplyCritical Temperature
07000F	’PSU XY’: Power supply fan prefailure	Fan failure is predicted at power supply ’PSU XY’ in cabinet XY of server XY.	2038	sc2TrapPower SupplyFan Failure Prediction
0C0004	’CPU XY’: CPU internal error (IERR)	Internal error (IERR) occurred on CPU ’CPU XY’ in cabinet XY of server XY.	2082	sc2TrapCpu Ierr
0C0021	’CPU XY’: Uncorrected CPU Machine Check Architecture (MCA) error			
0C0007	’CPU XY’: CPU clock automatically throttled	CPU speed at server XY changed to XY percent of its maximum speed.	2080	sc2TrapCpu Speed Changed
0C0017	’CPU XY’: CPU failure predicted	CPU failure is predicted for CPU ’CPU XY’ in cabinet XY.	2081	sc2TrapCpu Prefail
0C000B	’CPU XY’: CPU disabled	CPU ’CPU XY’ in cabinet XY of server XY is disabled.	2083	sc2TrapCpu Disabled

Table 4: iRMC S2 SEL entry - SC2 MIB trap

Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
120030	PCI system error (SERR): Slot 0x%1	The system wa restarted after a severe problem at cabinet XY of server XY. See server management message log (recovery log) for detailed information.	2006	sc2TrapSevere SystemError
120031	PCI parity error (PERR): Slot 0%1			
120034	PCI bus parity error indicated by onboard device (PERR): Bus: %1 Device: 0x%2 Function: 0x%3			
120035	PCI bus system error indicated by onboard device (SERR): Bus: %1 Device: 0x%2 Function: 0x%3			
120042	CPU front side bus (FSB) error			
120047	Fatal NMI			
150000	’Voltage XY’: Voltage OK	Power supply voltage ’BATT XY’ in cabinet XY at server XY is within normal range again.	2050	sc2Trap VoltageOk
150030	Battery voltage ’BATT XY’ OK			
150012	’Voltage XY’: Voltage low critical: % Volt	Power supply voltage ’Voltage XY’ in cabinet XY at server XY is too low.	2051	sc2Trap VoltageTooLow
150032	Battery voltage ’BATT XY’ low critical: % Volt			
150017	’Voltage XY’: Voltage high critical: % Volt	Power supply voltage ’Voltage XY’ in cabinet XY at server XY it too high.	2052	sc2Trap VoltageToo High

Table 4: iRMC S2 SEL entry - SC2 MIB trap

Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
150031	Battery voltage 'BATT XY' low warning: % Volt	Battery voltage 'BATT XY' in cabinet XY at server XY: Battery is predicted to fail in near future.	2054	sc2TrapBatteryVoltagePrefail
190003	'DIMM XY' Memory: Uncorrectable error (ECC)	Uncorrectable memory error at module 'DIMM XY' in cabinet XY of server XY.	2065	sc2Trap Uncorrectable MemError Module
190040	'DIMM XY': Uncorrectable Parity memory error			
190007	Memory: Uncorrectable error (ECC)	Uncorrectable memory error in cabinet XY of server XY.	2067	sc2Trap Uncorrectable MemError
190008	Correctable memory error disabled	Too many correctable memory errors in cabinet XY at server XY. Error logging was disabled. If logging was disabled and not automatically enabled again, you have to reboot your server to enable memory error logging again. If logging is disabled, prefailure detection is also not active!	2071	sc2TrapMem ErrorLogging Disabled

Table 4: iRMC S2 SEL entry - SC2 MIB trap

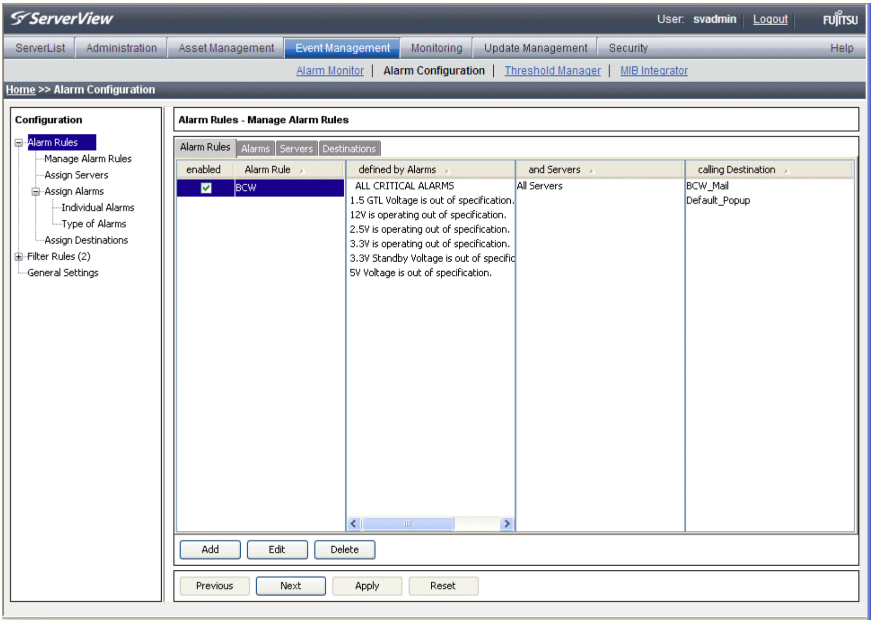
Error code	iRMC S2 SEL entry	Trap text	Trap no.	Trap name
190017	’DIMM XY’: Memory replaced by spare memory	Memory module ’DIMM XY’ in cabinet XY of server XY had failed and was replaced by a hot-spare module.	2070	sc2TrapMem ErrorModule Replaced
19001A	’DIMM XY’: Memory module failed predicted	Memory module failure is predicted for module ’DIMM XY’ in cabinet XY of server XY.	2068	sc2TrapMem ErrorModule Prefail
19001F	Memory: redundancy lost	Memory configuration in cabinet XY of server XY has lost redundancy.	2074	sc2TrapMem Error Redundancy Lost
190035	’DIMM XY’: Memory module error	Memory module ’DIMM XY’ in cabinet XY of server XY is failing. Too many errors have occurred.	2069	sc2Trap MemError ModuleFailing
190036	’DIMM XY’: Memory module failed (disabled)			
340002	Housing opened	The front door or housing of cabinet XY was opened on server XY.	2110	sc2Trap Intrusion Assertion
340003	Housing closed	The front door of housing of cabinet XY was closed on server XY.	2111	sc2Trap Intrusion Deassertion

Table 4: iRMC S2 SEL entry - SC2 MIB trap

4 Alarm configuration

The *Alarm Configuration* component in the Event Manager is used to define settings for alarm handling. You can define alarm rules, filter rules and general settings. The alarm rules define which alarms are forwarded from which servers to which destinations (see section "Alarm rules" on page 39). The filter rules define which types of alarm are filtered out (see section "Filter rules" on page 55). In the general settings you define the handling of all incoming and unfiltered alarms (see section "Making settings" on page 58). How to start the component is described in the section "Starting the Event Manager" on page 15.

When you select the *Alarm Configuration* component, the following window opens:



enabled	Alarm Rule	defined by Alarms	and Servers	calling Destination
☑	BCW	ALL CRITICAL ALARMS 1.5 GTL Voltage is out of specification. 12V is operating out of specification. 2.5V is operating out of specification. 3.3V is operating out of specification. 3.3V Standby Voltage is out of specific 5V Voltage is out of specification.	All Servers	BCW_Mail Default_Popup

Figure 4: Alarm Configuration

The menu tree in the left section shows the individual dialog windows for alarm handling.

The first time the window opens, the right-hand section shows the *Alarm Rules – Manage Alarm Rules* dialog window. The *Previous* and *Next* buttons take you step by step through the individual screens for setting the alarm parameters. You can also call up the individual screens directly by clicking the entries in the menu tree.

Buttons

The various screens contain the following buttons:

Add
Define a new setting.

Edit
Edit an existing setting.

Delete
Delete an existing setting.

Previous
Return to the previous screen.

Apply
Saves your changes to the database. You must click *Apply* before you quit the screen in which you have made changes, otherwise a warning message opens.

Reset
Your changes are reset to the settings stored in the database from the previous *Apply*.

Next
Go to the next screen.

OK
The new settings are saved and the screen is closed.

Cancel
The changes you have made are not applied and the screen is closed.

Help
Calls up a help text.

4.1 Alarm rules

An alarm rule forwards alarms from various servers to one or more destinations. A complete definition of a new alarm rule consists of the following four steps:

- Defining the name of the new alarm rule (see section "Managing alarm rules" on page 40).
- Assigning one or more servers to the alarm rule (see section "Assigning servers" on page 43). The alarm rule then only applies to alarms from these servers.
- Assigning one or more alarms to the alarm rule (see section "Assigning alarms" on page 47).
- Defining the response to the incoming alarms (see section "Forwarding alarms" on page 51). Here you can use the standard destinations or define your own (e.g. Execute forwarding, Mail forwarding or Mobile forwarding).

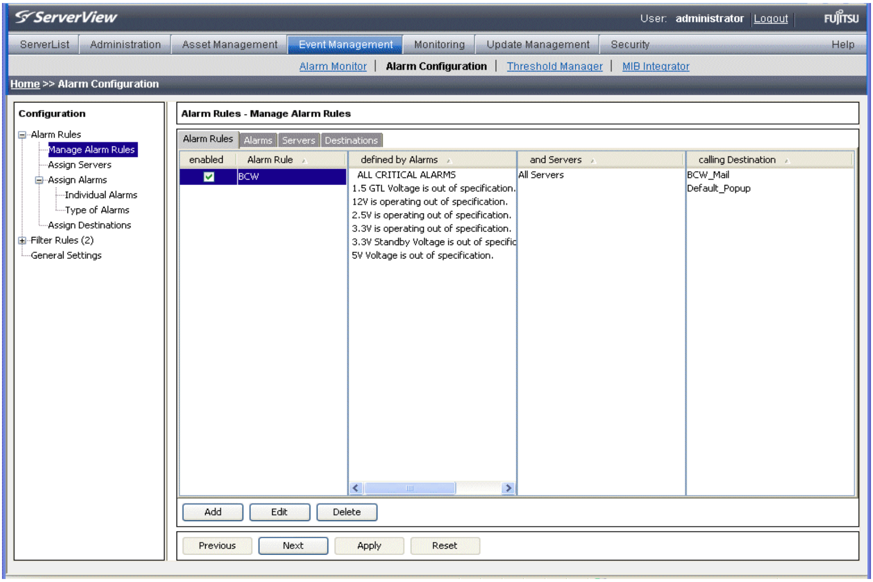
When defining a new alarm rule, you will be guided step by step through the individual screens for setting the alarm parameters. If you are changing an existing alarm rule you can also call up the individual dialog screens directly via the menu tree.

4.1.1 Managing alarm rules

The *Alarm Rules – Manage Alarm Rules* screen provides an overview of all defined alarm rules. The tabs *Alarm Rules, Alarms, Servers* and *Destinations* allow different views of the defined alarm rules, depending on which tab is selected.

The *Add* button allows you to add new alarm rules. It opens a window in which you can enter the name of the new alarm rule. You can also copy settings of an existing alarm rule over to the new one. To do this, select an existing alarm from the drop-down list. All settings of the existing alarm rule visible on the *Alarms, Servers, Destinations* tabs and from the drop-down list marked with *Copy settings from rule* will then be taken over by default. If you do not want to take over the settings from every tab, you can disable the individual tabs by clicking the selected checkbox directly. The assigned settings will then not be taken over for the new alarm rule.
If you do not want to take over any settings, select the empty field in the drop-down list.

The *Edit* button lets you modify existing alarm rules. With the *Delete* button you can delete a selected alarm rule.



enabled	Alarm Rule	defined by Alarms	and Servers	calling Destination
☑	BCW	ALL CRITICAL ALARMS 1.5 GTL Voltage is out of specification. 12V is operating out of specification. 2.5V is operating out of specification. 3.3V is operating out of specification. 3.3V Standby Voltage is out of specific 5V Voltage is out of specification.	All Servers	BCW_Mail Default_Popup

Figure 5: Alarm Rules - Manage Alarm Rules

Alarm Rules tab

The *Alarm Rules* tab is used to assign alarm rules to alarms, servers and alarm destinations.

The first column lists all known alarm rules. The *enabled* column indicates which alarm rules are activated (checkmark) and which are deactivated. By clicking in the *enabled* column you can set or remove a checkmark. You save the new setting by clicking the *Apply* button.

The second column lists the alarms that are assigned to the selected alarm rule. Only alarms assigned to the alarm rule are forwarded.

The third column shows the servers that are assigned to the selected alarm rule. Only alarms from assigned servers are forwarded by an alarm rule.

The fourth column shows all destinations of the incoming alarms for the selected alarm rule.

With the *Add* button you can define new alarm rules. A window opens for you to enter the new name of the alarm rule. With the *Edit* button you can modify an existing, selected alarm rule, and with the *Delete* button you can delete an existing alarm rule.

Alarms tab

The *Alarms* tab provides an overview of which alarms are assigned to which alarm rules. So you can quickly check which, if any, destination is assigned to an alarm.

The first column lists all known alarms in alphabetical order. Because the alarms are defined by many different manufacturers, the same name can be used twice.

The second column lists all the alarm rules to which the selected alarm is assigned.

The third column shows the servers that are assigned to the alarm rule selected in column two. Only alarms from assigned servers are forwarded by an alarm rule.

The fourth column shows all destinations of incoming alarms for the selected alarm rule.

Servers tab

The *Servers* tab shows you which servers are covered by which alarm rules. Here you can check whether alarms from a server are at least being forwarded to one destination.

The first column lists all known and unfiltered servers in alphabetical order (see section "Server filters" on page 55). You can find out more about a particular server by clicking its entry in the list.

The second column lists all the alarm rules to which the selected server is assigned.

The third column shows the alarms which are assigned to the selected alarm rule.

The fourth column contains all destinations to which the selected alarm rule forwards the incoming alarms.

Destinations tab

The *Destinations* tab tells you which destination incoming alarms are forwarded to with which alarm rules.

The first column lists all known destinations in alphabetical order.

The second column lists all alarm rules which forward the incoming alarms to the selected destination.

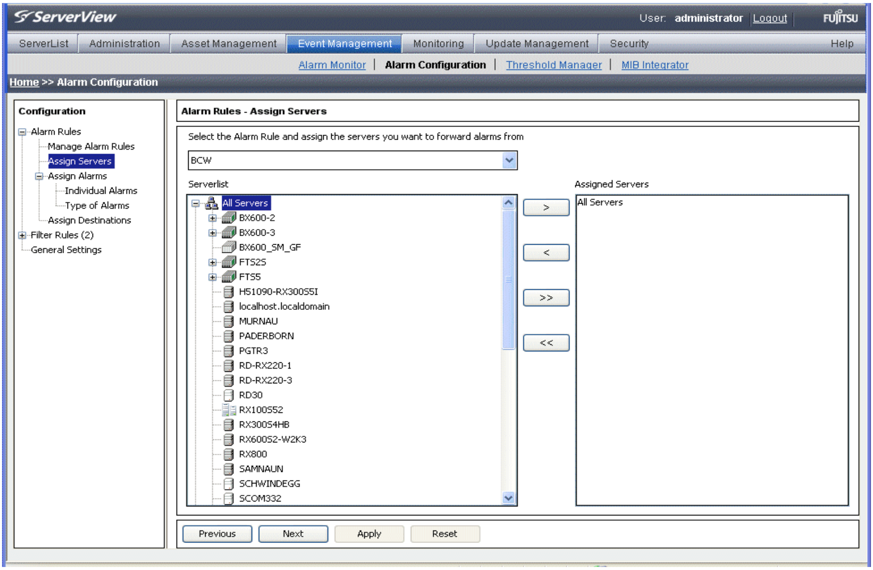
The third column contains the list of servers that are assigned to the selected alarm rule.

The fourth column shows all alarms that are assigned to the selected alarm rule.

On the *Destinations* tab you can use the *Add* button to define a new destination, the *Edit* button to modify an existing destination, and the *Delete* button to delete an existing destination. The destinations *Default_Popup* and *Event_Log* cannot be deleted. The destination *Event_Log* can also not be changed.

4.1.2 Assigning servers

In the *Alarm Rules – Assign Server* screen, you define the servers and/or server groups to be assigned to an alarm rule.



Select the Alarm Rule and assign the servers you want to forward alarms from

BCW

Serverlist: All Servers, BX600-2, BX600-3, BX600_SM_GF, FTS2S, FTS5, H51090-RX300S5I, localhost.localdomain, MURNAU, PADERBORN, PGTR3, RD-RX220-1, RD-RX220-3, RD30, RX100S52, RX300S4HB, RX600S2-W2K3, RX800, SAMNAUN, SCHWINDEGG, SCOM332

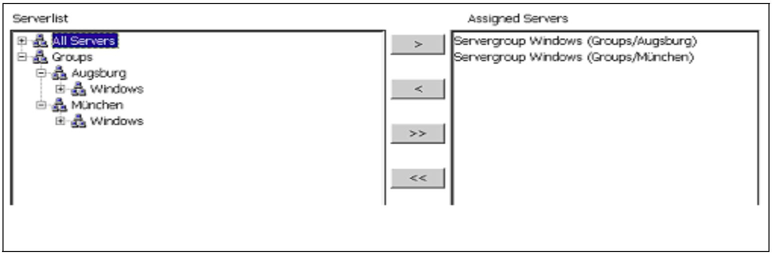
Assigned Servers: All Servers

Figure 6: Alarm Rules - Assign Servers

Via the drop-down list, you can select the alarm rule that you want to edit. The file tree in the *Serverlist* box contains all known and unfiltered servers. The *Assigned Servers* window shows the list of servers and server groups which are assigned to the alarm rule.

> **i** If you move a server group to *Assigned Servers*, associated subgroups are not moved with it and must be moved separately. This restriction does not apply to *All Servers*.

Because different server groups can have the same name, they are displayed in the *Alarm Configuration* component with their group hierarchy.



All Servers
Groups
Augsburg
Windows
München
Windows

Servergroup Windows (Groups/Augsburg)
Servergroup Windows (Groups/München)

Figure 7: Alarm Rules - Assign Servers group hierarchy

You can use the following buttons to specify which servers are to belong to this alarm rule:

>
: Adds the selected servers to the alarm rule.

<
: Removes the selected servers from the alarm rule.

>>
: Adds all known servers to the alarm rule.

<<
: Removes all servers from the alarm rule.

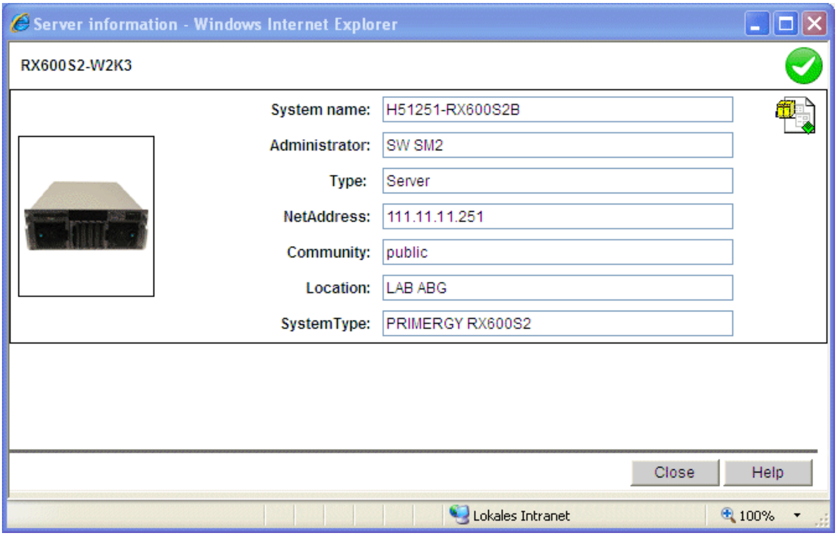
If you select *Show Information about Server* from the context menu, additional information about the selected server is displayed. If you select *Show unassigned servers only,* the server list will only contain the servers which are not yet assigned to an alarm rule. If you select *Show all Servers*, all servers are shown again.

Clicking the *Apply* button saves the new settings. Clicking the *Reset* button restores the settings from the last save.

If the window is leaved without applying the changed configuration, or if a necessary element for the alarm rule is missing, a corresponding warning message will be issued.

4.1.2.1 Displaying server information

If you select *Show Information about Server* from the context menu,the *Server information* window opens, showing additional information about the selected server.



RX600S2-W2K3

System name: H51251-RX600S2B

Administrator: SW SM2

Type: Server

NetAddress: 111.11.11.251

Community: public

Location: LAB ABG

SystemType: PRIMERGY RX600S2

Figure 8: Server information

The header gives the server name accompanied by a status icon which indicates the current server status.

Underneath the status icon there is another icon which indicates whether or not the server is entered in the server list:

The server is known, i. e. the server is present in the ServerView server list.

The server is unknown, i.e. the server is not present in the ServerView server list.

If the server is in the server list, the server information will be displayed. If the server is not in the server list but has the current status *manageable*, the Event Manager will obtain the information directly from the server itself.

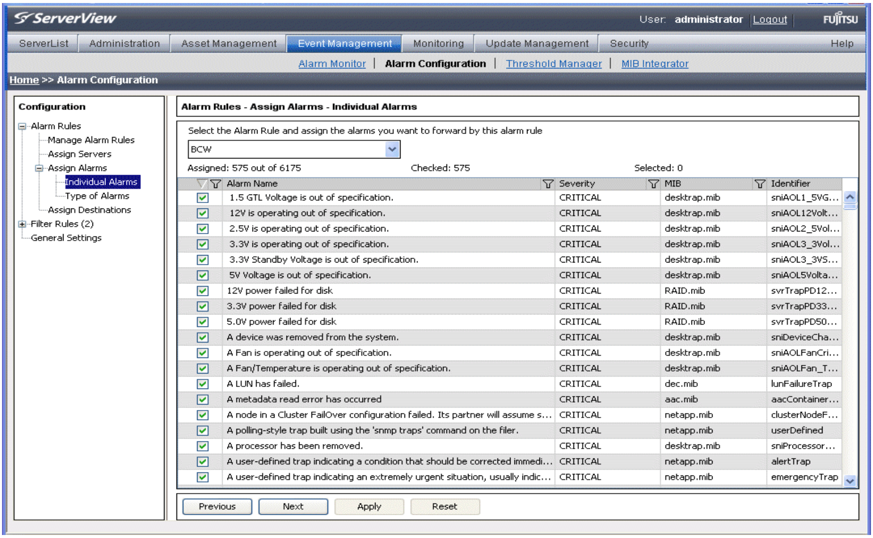
ℹ You can start Operations Manager for the selected server in this window. To do this, click the status icon in the top right-hand corner.

The status display, the server picture and the start command for Operations Manager are only enabled if Operations Manager is already installed.

To close the *Server information* window, click the *Close* button.

4.1.3 Assigning alarms

In the *Alarm Rules – Assign Alarms* dialog box you can define in the *Individual Alarms* dialog box the alarms for the alarm rule and display all details of the assigned alarms. In the *Type of Alarms* dialog box you can define for selected alarm rules what kind of alarms are to be forwarded.



Alarm Rules - Assign Alarms - Individual Alarms

Select the Alarm Rule and assign the alarms you want to forward by this alarm rule

BCW

Assigned: 575 out of 6175   Checked: 575   Selected: 0

	Alarm Name	Severity	MIB	Identifier
☑	1.5 GTL Voltage is out of specification.	CRITICAL	desktrap.mib	sniAOL1_5VG...
☑	12V is operating out of specification.	CRITICAL	desktrap.mib	sniAOL12Volt...
☑	2.5V is operating out of specification.	CRITICAL	desktrap.mib	sniAOL2_5Vol...
☑	3.3V is operating out of specification.	CRITICAL	desktrap.mib	sniAOL3_3Vol...
☑	3.3V Standby Voltage is out of specification.	CRITICAL	desktrap.mib	sniAOL3_3VS...
☑	5V Voltage is out of specification.	CRITICAL	desktrap.mib	sniAOL5Volta...
☑	12V power failed for disk	CRITICAL	RAID.mib	svrTrapPD12...
☑	3.3V power failed for disk	CRITICAL	RAID.mib	svrTrapPD33...
☑	5.0V power failed for disk	CRITICAL	RAID.mib	svrTrapPD50...
☑	A device was removed from the system.	CRITICAL	desktrap.mib	sniDeviceCha...
☑	A Fan is operating out of specification.	CRITICAL	desktrap.mib	sniAOLFanCri...
☑	A Fan/Temperature is operating out of specification.	CRITICAL	desktrap.mib	sniAOLFan_T...
☑	A LUN has failed.	CRITICAL	dec.mib	lunFailureTrap
☑	A metadata read error has occurred	CRITICAL	aac.mib	aacContainer...
☑	A node in a Cluster FailOver configuration failed. Its partner will assume s...	CRITICAL	netapp.mib	clusterNodeF...
☑	A polling-style trap built using the 'snmp traps' command on the filer.	CRITICAL	netapp.mib	userDefined
☑	A processor has been removed.	CRITICAL	desktrap.mib	sniProcessor...
☑	A user-defined trap indicating a condition that should be corrected immedi...	CRITICAL	netapp.mib	alertTrap
☑	A user-defined trap indicating an extremely urgent situation, usually indic...	CRITICAL	netapp.mib	emergencyTrap

Figure 9: Alarm Rules - Assign Alarms - Individual Alarms

The *Individual Alarms* dialog box contains in the top drop-down list the names of all known alarm rules. Here you can select the alarm rule that you want to edit.

f an unknown alarm occurs, you can assign an alarm rule to it. Make sure that unknown alarms are not suppressed but are explicitly allowed. You can do this via the filter settings in the *Filter Rules – Alarm Filtering* dialog box (see "Filtering alarms" on page 56). You must also select the appropriate checkbox under *Alarm Rules – Assign Alarms – Type of Alarms*

The *Assigned* counter indicates both the number of alarms that are currently assigned to this alarm rule and the number of all known alarms.

The *Checked* counter counts all alarms whose checkboxes are selected, regardless of whether the alarms were filtered.

The *Selected* counter shows the number of currently selected alarms in the alarm list.

The alarm list in the bottom section of the window shows via checkboxes which alarms are assigned to the alarm rule. It also shows the names of the alarms (*Alarm Name*), their severity (*Severity*), their MIB file (*MIB*), in which the alarm is defined, and their trap name (*Identifier*).

Alarms which are assigned to the selected alarm rule are indicated by selected checkboxes. You can select or deselect a checkbox by clicking it.
Clicking the *Apply* button saves the changed settings for the alarm rule. The value of the *Assigned* counter then matches the value of the *Checked* counter.

All alarms in the alarm list can be sorted or filtered according to different criteria. This allows only certain alarms to be displayed.

You sort the alarms by clicking the relevant column in the header of the alarm list. You can sort them alphabetically by *Alarm Name*, *Severity*, *MIB* or *Identifier*.

You filter the alarms by clicking the corresponding filter icons in the header of the alarm list.
You can filter them according to selected alarms (selected checkboxes), *Alarm Name, Severity* or *MIB*. Clicking the filter icon opens the respective associated dialog box. If, for example, you have selected *Severity*, the dialog box shows the error severities, which you can then select. You make your selection and then confirm it with *OK*. Depending on your selection, the window then shows only the filtered alarms. An active filter is indicated by a blue filter icon.

In the standard filter (*Standard*), all selection elements are selected via checkboxes. In the customized filter (*Customize*) you make your selection either by entering it directly (e.g. MINOR) or using the asterisk as a wildcard. With Severity, for example, specifying M* selects the severities Major and Minor.

The alarm list offers a context menu, in which you can select the following items:

Show information about selected Alarm
: To see additional information on the selected alarm

Check all alarms
: To add all currently known alarms to the alarm rule

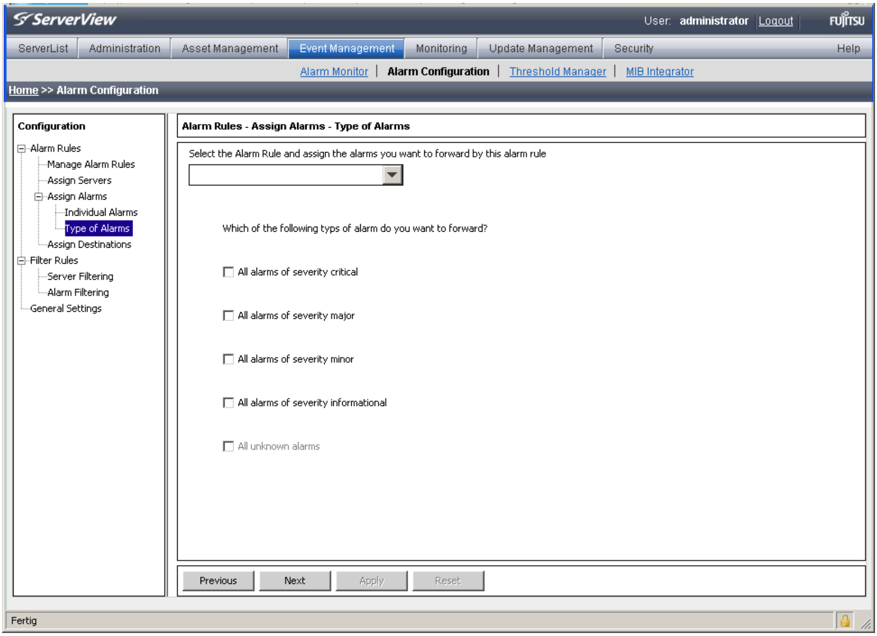
Check selected alarm(s)
: To add the selected alarms to the alarm rule

Uncheck all alarms
: To remove all currently known alarms from the alarm rule

Uncheck selected alarm(s)
: To remove the selected alarms from the alarm rule

Clicking the *Apply* button saves the new settings. If you click the *Reset* button, the settings from the last save are restored.

In the *Alarm Rules – Assign Alarms – Type of Alarms* dialog box you can define for selected alarm rules what kind of alarms are to be forwarded.



Alarm Rules - Assign Alarms - Type of Alarms

Select the Alarm Rule and assign the alarms you want to forward by this alarm rule

Which of the following typs of alarm do you want to forward?

☐ All alarms of severity critical

☐ All alarms of severity major

☐ All alarms of severity minor

☐ All alarms of severity informational

☐ All unknown alarms

Figure 10: Alarm Rules - Assign Alarms - Type of Alarms

The top drop-down list contains the names of all known alarm rules. Here you can select the alarm rule that you want to edit. You can activate or deactivate the following filter settings:

All alarms of severity critical
All alarms of severity *critical* are handled according to the alarm rule.

All alarms of severity major
All alarms of severity *major* are handled according to the alarm rule.

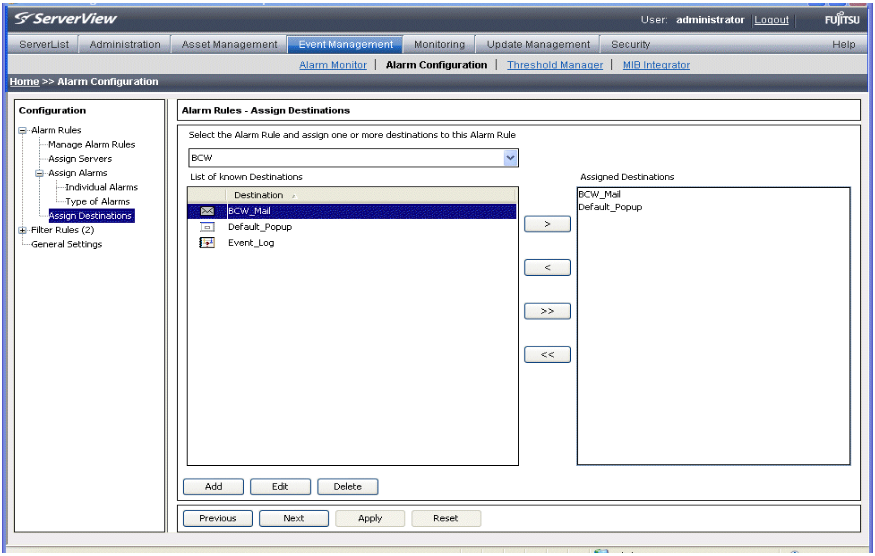
All alarms of severity minor
All alarms of severity *minor* are handled according to the alarm rule.

All alarms of severity informational
All alarms of severity *informational* are handled according to the alarm rule.

All *unknown alarms*
All unknown alarms are handled according to the alarm rule.

4.1.4 Forwarding alarms

In the *Alarm Rules – Assign Destinations* screen you can make settings relating to alarm destinations. Select an alarm rule and then define the actions to be triggered for the servers of this alarm rule in response to certain alarm messages.



Select the Alarm Rule and assign one or more destinations to this Alarm Rule

BCW

List of known Destinations

Destination
BCW_Mail
Default_Popup
Event_Log

Assigned Destinations

BCW_Mail
Default_Popup

Figure 11: Alarm Rules - Assign Destinations

The top drop-down list contains the names of all known alarm rules. Here you can select the alarm rule that you want to edit. The *List of known Destinations* box contains all known destinations. The *Assigned Destinations* box contains the list of destinations assigned to the alarm rule.

With the *Add* button you can define a new destination, with the *Edit* button you can change an existing destination, and with the *Delete* button you can delete an existing destination.
The destination *Automatic Service Mail* can be neither deleted nor moved to the *Assigned Destinations* window.

You can use the following buttons to activate or deactivate the forwarding of an alarm:

>

Activates the selected destinations.

<

Deactivates the selected destinations.

>>

Activates all known destinations.

<<

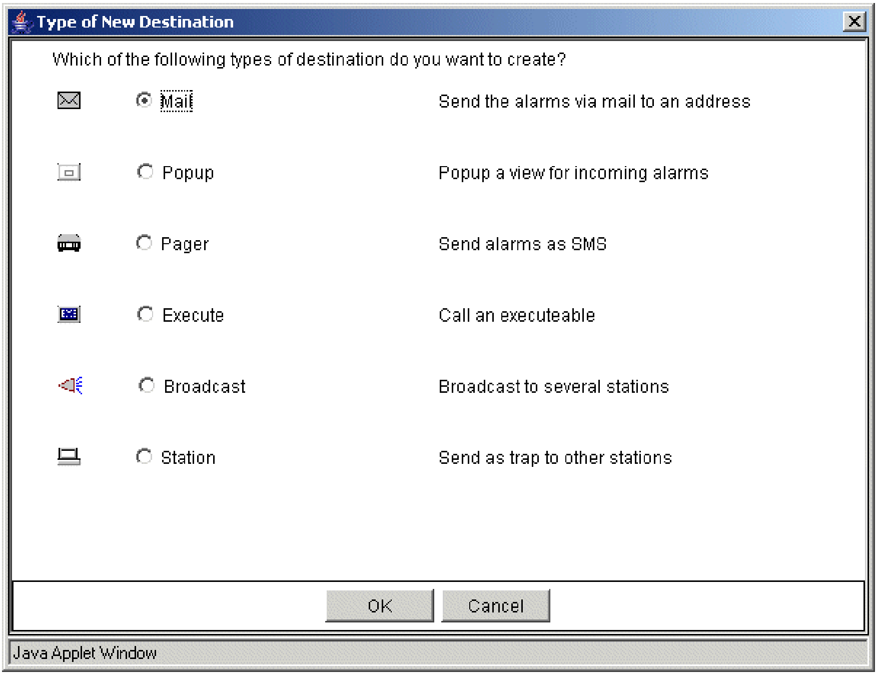
Deactivates all known destinations.

Clicking the *Apply* button saves the new settings. Clicking the *Reset* button restores the settings from the last save.

You can define the following responses for the alarm rule:

- Send a mail (*Mail*)
- Output a message (*Popup*)
- Log the alarm (*Event Log*)
- Trigger a call to a pager or mobile phone (*Pager*)
  (This feature is not supported in the Japanese market.)
- Trigger an executable program (*Execute*)
- Trigger a broadcast message (*Broadcast*)
- Generate a trap which is forwarded to another management station (*Station*)
- Send a mail to a special service address (*Automatic Service Mail*)
  (This feature is not supported in the Japanese market. For Japan another forwarding service called FJJ Service Mail is provided.)

By clicking the *Add* button you can define a new destination. The following window opens showing the available destinations.



Type of New Destination

Which of the following types of destination do you want to create?

● Mail	Send the alarms via mail to an address
○ Popup	Popup a view for incoming alarms
○ Pager	Send alarms as SMS
○ Execute	Call an executeable
○ Broadcast	Broadcast to several stations
○ Station	Send as trap to other stations

Figure 12: Type of New Destination

Clicking *OK* opens additional windows, depending on your selection, in which you must make further settings. There, via different tabs, you can define all the parameters necessary for forwarding. A detailed description of the various windows is available via the respective Help buttons. More information on the individual windows is provided in the later sections describing the respective forwarding actions and settings on page 59.

- Note for SMTP AUTH

  For sending mails, *SMTP AUTH* is supported. The supported authentication method is: CRAM MD5 / LOGIN / PLAIN. The authentication method used when you send a mail automatically switches to the safest method compatible with the authentication method supported by the destination SMTP server.

  If *User* and Password are left blank, mails will be sent by SMTP without authentication.

- If you have selected *Mail* mail forwarding, the character set (*charset*) in the mails for *Subject* und *Message* is set in the following way:

  – on a Windows-based management station *charset=Shift-JIS*
  – on a Linux-based management station *charset= UTF-8*

4.2 Filter rules

The filter rules define the servers or server groups from which you want to filter out alarms (see section "Server filters" on page 55) and/or which alarms are to be filtered out (see section "Filtering alarms" on page 56).

i Filter rules take priority over alarm rules. If a alarm is ignored because of the filter rules, the alarm rule assigned to the alarm is not activated.

4.2.1 Server filters

In the *Filter Rules – Server Filtering* screen, you define the servers or server groups whose alarms you want to filter out. If the Event Manager is running on a server and there are no other servers in the server list, this server is automatically displayed as the local host. No further settings are necessary for this.

The *Serverlist* box contains all servers and server groups in the server list. The *Suppress from handling* box contains the servers or server groups whose alarms are not to be handled.
You can filter the servers with the following buttons:

>

The alarms from the selected servers or server groups are ignored.

<

The alarms from the selected servers or server groups are forwarded.

>>

All alarms from the servers or server groups in the server list are ignored.

<<

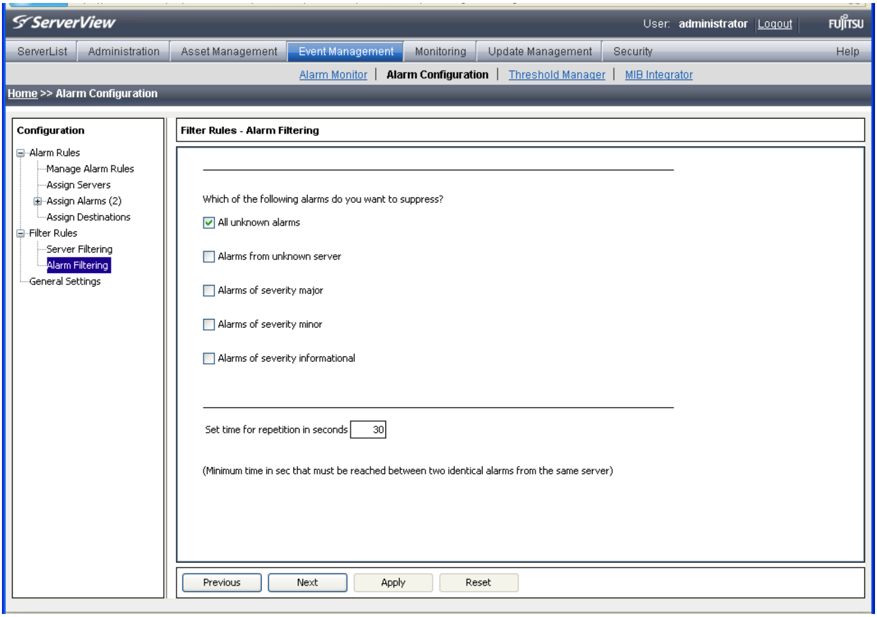
All alarms from the servers or server groups in the *Suppress from handling* box are handled again. All incoming alarms from the servers or server groups in the server list are forwarded.

If you select a server in the *Serverlist* window, you can display additional information about this server via *Show Information about Server* on the context menu.

Clicking the *Apply* button saves the new settings. Clicking the *Reset* button restores the settings from the last save.

4.2.2 Filtering alarms

In the *Filter Rules – Alarm Filtering* dialog box you can activate or deactivate filter settings for an alarm type.



Which of the following alarms do you want to suppress?

☑ All unknown alarms

□ Alarms from unknown server

□ Alarms of severity major

□ Alarms of severity minor

□ Alarms of severity informational

Set time for repetition in seconds 30

(Minimum time in sec that must be reached between two identical alarms from the same server)

Figure 13: Filter settings for an alarm type

You can activate or deactivate the following filter settings:

All unknown alarms
: Filter out unknown alarms. These are alarms which are not defined in any of the integrated MIBs.

Alarms from unknown server
: Filter out alarms from unknown servers.

Alarms of severity major
: Filter according to the severity level *major*.

Alarms of severity minor
: Filter according to severity level *minor*.

Alarms of severity informational
: Filter according to the severity level *informational*.

In the input field *Set time for repetition in seconds* you can specify the interval after which the same alarm is allowed through from the same server again. This is useful to prevent the management station from being bombarded with identical alarms from a server that is not running correctly.

When you specify, for example, an interval of 30 seconds, filter interval of each severity are as follows:

Severity of alarm	Value of severity	Expression from which filter interval is requested	Filter interval
Critical	1	30 seconds × 1	30 seconds
Major	2	30 seconds × 2	60 seconds
Minor	3	30 seconds × 3	90 seconds
Informational	4	30 seconds × 4	120 seconds

Table 5: Filter interval of each severity

4.3 Making settings

In the *General Settings* screen you can define general settings for alarm handling.

You can define the actions to be executed by default and regardless of the alarm groups whenever an alarm arrives.

You can define the following actions:

- Alarms relating to failed authentication are suppressed.
- Alarms from server blades are issued with the relevant name of the blade server.

For different error severities you can specify the following actions. Any combinations are possible.

- The alarm is to be written to the operating system event-log list.

  When you receive alarms with the checked severities, the alarms are logged in the operating system event log.
- When you receive alarms with the checked severities, a pop-up notification for each alarm is displayed on the management server.
- The Alarm Monitor window is to move to the foreground.

  Every time you receive an alarm with the checked severities, the AlarmMonitor window is displayed on top of any open windows. For this to happen, the AlarmMonitor window must be open already.

You can specify when the alarm is to be deleted. You can define whether the alarm is to be deleted when it reaches a certain age or when the log list contains a certain number of entries. Once a certain number of entries is reached, the oldest one in the list is deleted.

Clicking the *Apply* button saves the new settings. Clicking the *Reset* button restores the settings from the last save.

i With general settings, event logs are recorded independently from Alarm Rules. Depending on the configuration, two event logs may be recorded for the same alarm.

4.4 Mail forwarding in general

Points to note when setting up the mail service (MAPI)

To configure the mail service, check whether Microsoft Mail is installed.

If the Microsoft mail system is not installed, you will need to run the setup program of your operating system again to install the mail system.

For more information see the Readme files, which are located in the installation directory of ServerView.

The Readme files are located

– on Windows in:

<wwwroot>/ServerView/common/readme.txt

– on Linux in:

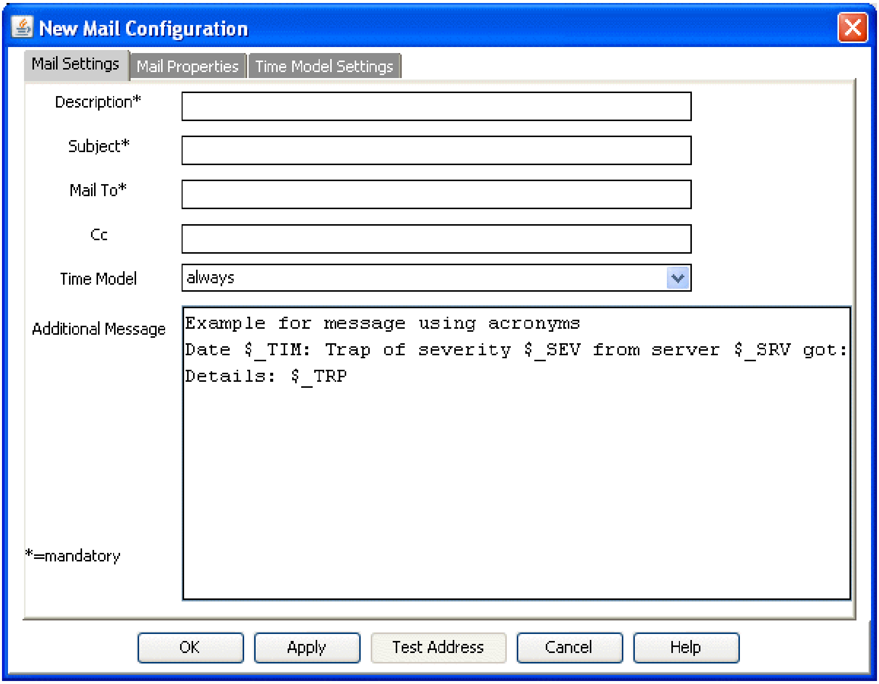
/usr/share/doc/fujitsu/ServerViewSuite/en/README

or

/usr/share/doc/fujitsuServerViewSuite/jp//README

Making mail settings

If you have selected *Mail* for the forwarding, the following *New Mail Configuration* window opens.



Description*

Subject*

Mail To*

Cc

Time Model: always

Additional Message

```
Example for message using acronyms
Date $_TIM: Trap of severity $_SEV from server $_SRV got:
Details: $_TRP
```

*=mandatory

Figure 14: New Mail Configuration

In this window you can define all the necessary parameters for forwarding on the *Mail Settings, Mail Properties* and *Time Model Settings* tabs. Fields marked with * are mandatory, while the other fields are optional.

Mail Settings tab

The *Mail Settings* tab provides fields for the mail settings, some of which already contain predefined settings.

The input fields in the *Mail Settings* window have the following meanings:

Name	**Meaning**
Description	Name of the mail settings If you want to change the mail settings for an existing mail forwarding (see *Edit* button, section "Forwarding alarms" on page 51), this field contains the already assigned name and is disabled.
Subject	Subject of the mail The mail subject can contain macros (see section "Macros" on page 78). If the subject contains characters which cannot be displayed, they are replaced by displayable ones (e.g. hex code).
Mail To	E-mail address of the person to whom you want to send the alarm. Multiple addresses must be separated with a semicolon or comma.
Cc	E-mail address of the person to whom you want to send a copy of the alarm (optional). Multiple addresses must be separated with a semicolon or comma.
Time Model	Time model indicating when an alarm is to be forwarded. Select a predefined time model from the drop-down list. You can set your own time model via the *Time Model Settings* tab.
Additional Message	Text field for defining the alarm message. Information about the servers can be inserted via different macros (see section "Macros" on page 78). A suggestion is offered here to simplify handling. Delete or change it if necessary.

Table 6: Input fields in the Mail Settings window

Mail Properties tab

The *Mail Properties* tab provides fields for the mail server. Depending on the mail service, *MAPI* (Windows only) or *SMTP* (Windows, Linux) must be selected.

Depending on the selected mail service, different input fields are enabled in the *Mail Properties* window. The input fields have the following meanings:

Name	Meaning
From	Sender (SMTP)
Server	SMTP server (SMTP)
User (optional)	User name (SMTP)
Password (optional)	Identification of the mailing system (optional with SMTP)
Confirm Password (optional)	Confirm the password (optional with SMTP)
Port	Port number (SMTP) The default value is *Port 25*
Profilename	Identification of the mailing system (MAPI) You must specify the profile name that was assigned during configuration of Microsoft Mail. If you assign a different profile name here, the mail mechanism will not work.
Password	Identification of the mailing system (MAPI) With MAPI you must specify the password that was assigned during configuration of Microsoft Mail. If you assign a different profile name and a different password here, the mail mechanism will not work.
Confirm Password	Confirm the password (MAPI)

Table 7: Input fields in the Mail Properties window

Time Model Settings tab

The *Time Model Settings* tab allows you to select, add or modify a time model. You can define hour by hour for the whole week when an alarm is to be forwarded.

If you click the *Test Address* button, a test mail is sent to check your settings.
If you click *OK*, your settings will be saved and you will be returned to the previous window.
Further buttons are offered depending on the type of forwarding and the selected tab (see "Buttons" on page 38).

McAfee virus scanner

The McAfee virus scanner contains a setting which prevents programs from sending e-mails if they are not registered.

To register the mail senders, you must enter the corresponding program name: *blat.exe* under Windows or *smtpm* under Linux.

4.5 Mail forwarding to the service provider

The Event Manager allows you to automatically forward alarms to the service provider by e-mail.

If mail forwarding to the service provider is activated, the service provider is notified by e-mail whenever certain traps occur. The group of traps that trigger a mail is defined by the service provider and can only be changed by them.

Activating mail forwarding

You activate mail forwarding to the service provider in the *Alarm Rules – Assign Destinations screen by selecting the alarm group Automatic Service Mail* in this screen.

If you click the *Edit* button you can make the necessary settings for mail forwarding to the service provider in the *Mail Settings* window.

The input fields in the *Mail Settings* window have the following meanings:

Name	Meaning
Mail To	E-mail address of the Service Center
Cc	The e-mail address to which a copy of the service mail is to be sent (optional)
Identnumber	Unique ID number of the server ℹ This number must be agreed with the service provider.
Name	Name of the server administrator
Phone	Telephone number of the server administrator
E-mail Address (optional)	E-mail address to be used by the Service Center for feedback (optional).
Country ID (optional)	Two-letter ISO code for the country (optional) (e.g. DE for Germany).
Customer ID (optional)	Customer code (optional) The customer code must be agreed with the provider.

Table 8: Input fields in the Service Mail Settings window

You can enable or disable this configuration with the *Enabled* option.

If you click the *Mail Properties* tab, you can specify additional information on the mail service in this window. Depending on the mail service, you must select *MAPI* (Windows only) or *SMTP* (Windows, Linux).

Depending on the selected mail service, different input fields are enabled in the *Mail Properties* window. The input fields have the following meanings:

Name	Meaning
From	Sender (SMTP)
Server	SMTP server (SMTP)
User (optional)	User name (SMTP)
Password (optional)	Identification of the mailing system (optional with SMTP)
Confirm Password (optional)	Confirm the password (optional with SMTP)
Port	Port number (SMTP) The default value is *Port 25*
Profilename	Identification of the mailing system (MAPI) You must specify the profile name that was assigned during configuration of Microsoft Mail. If you assign a different profile name here, the mail mechanism will not work.
Password	Identification of the mailing system (MAPI) With MAPI you must specify the password that was assigned during configuration of Microsoft Mail. If you assign a different profile name and a different password here, the mail mechanism will not work.
Confirm Password	Confirm the password (MAPI)

Table 9: Input fields in the Mail Properties window

If you click the *Test Address* button in the *Service Mail Settings* window, a test mail is sent to the service provider. The Service Center sends an automatic e-mail response to all test mails it receives. In doing so it uses the address specified in the *E-mail* input field.

A minimum period of 600 seconds has been specified for the sending of identical mails. This ensures that redundant messages are not sent.

In the Alarm Monitor, traps that have triggered a service mail are identified as follows:

✉ This icon identifies a trap that has been forwarded using the service mail function.

✉✉ This icon identifies a trap that has been forwarded using both the normal mail function and the service mail function.

4.6 Making pop-up settings

If you have selected *Popup* for the forwarding, the *New Popup Configuration* window opens. In this window you can use the *Popup Settings* and *Time Model Settings* tabs to make all necessary settings for pop-up forwarding.

i Pop-up notifications are only displayed on the local host. They cannot be displayed on any other host.

Popup Settings tab

The *Popup Settings* tab offers fields for the pop-up settings, some of which already contain predefined settings.

The input fields in the *Popup Settings* window have the following meanings:

Name	Meaning
Description	Name of the pop-up settings If you want to change the pop-up settings for an existing pop-up forwarding (see *Edit* button, section "Forwarding alarms" on page 51), this field contains the already assigned name and is disabled.
Time Model	Time model indicating when an alarm is to trigger a pop-up message. Select a predefined time model from the drop-down list. You can set your own time model via the *Time Model Settings* tab.
Additional Message (optional)	Text field for defining the message in the pop-up window. Information about the servers can be inserted via different macros (see section "Macros" on page 78). As of Windows Server 2008, the output is truncated after 255 characters.

Table 10: Input fields in the Popup Settings window

Time Model Settings tab

The *Time Model Settings* tab allows you to select, add or modify a time model. You can define hour by hour for the whole week when an alarm is to be forwarded.

Notes for Linux

1. To receive the forwarded alarm messages, a user must be logged onto the Linux system console. If no user is logged on, the forwarded alarm messages are not saved. This means that they will not be output the next time a user logs onto the system console.

2. Because with Linux systems the user is logged onto a virtual system console, they can either use graphical interfaces (GUI session, e.g. Gnome or KDE) or the command line interface (CLI session). The appearance of the layout depends on this.

   With a CLI session, the logged-on user receives the forwarded alarm message as a plain-text message.

   With a GUI session, the forwarded alarm message is output in a (non-modal) pop-up window.

3. The forwarding service uses the database under /var/run/utmp to obtain information on the users connected to the system console. The entries in the database should therefore be correct.
   If a graphics session is started on the system console with the *startx* program, the necessary entries are not made under /var/run/utmp. The forwarded alarms are then not output.
   To receive the forwarded alarm messages as pop-up messages on the ServerView management station, the Linux operating system should begin in graphics mode (runlevel 5) after a system start.
   The forwarding service does not forward alarms to Xconsoles.

4.7 Making pager settings (COM port and modem)

If you have selected *Pager* for the forwarding, the *New Pager Configuration* window opens. In this window you can use the *Pager Settings* and *Modem Settings* tabs to make the different settings for the serial interfaces and the modems connected to them (pager types).

You can define the following values:

– The name of the available interfaces (e.g. COM2 or COM4)
– The maximum transmission speed (baud rate)
– The type of data flow control
– The initialization and reset chain for the modem

The input fields in the *New Pager Configuration* window have the following meanings:

Name	Meaning
Description	Name of the pager settings
Owner	Name of the owner
Com Port	Name of the serial interfaces. The drop-down list contains the names of the available interfaces. You can select a specific interface or the entry *Any Available*. If you select the latter, any available interface can be connected to your COM ports. This is useful if you frequently change the attached devices.
Pager Number	(Telephone) number of the pager i With a text message the destination number may have to be preceded by an additional prefix of the relevant pager service. For example: D1 service in Germany: 49171XXXXXXX (XXXXXXX = pager ID) Must be prefixed by 49171 (without 00) D2 service in Germany: 0049172XXXXXXX 0049172 is optional

Table 11: Input fields in the Mail Settings window

Name	Meaning
Time Model	Time model indicating when an alarm is to be forwarded. Select a predefined time model from the drop-down list. You can set your own time model via the *Time Model Settings* tab.
Retry Delay	Delay in minutes between two pager attempts. Do not select too short a time, as calls to a pager can be delayed by a few minutes by the service provider. Also bear in mind the time required to reach the server management station. This delay can be around five or more minutes.
Retries	Maximum number of attempts to forward an alarm to a pager before a message appears.
Pager Type	Type of the pager (signal/numeric/alpha/SMS1 Service/ SMS2 Service/NTT Service) ℹ If you select the wrong pager type, the transmission will be ignored because of an invalid communication protocol.

Table 11: Input fields in the Mail Settings window

You specify the pager service via the *Pager, SMS-1* or *SMS-2* tabs.

The *Server Num* tab tells you which server numbers are assigned to which server name. The server number is sent to the pager type *numeric*.

You can test your settings by clicking the *Test* button.

For each service number, you make settings for data bits, parity and stop bits and you define the prompt used by the pager service for messages.
With the SMS1 and SMS2 service, two services with different protocols can be used to address a GSM mobile. SMS1 uses the TAP protocol, while SMS2 uses the UCP protocol.

Baud rate	2400 bps, 1200 bps or 300 bps
Data bits	8
Parity	none
Stop bits	1
Dialling prefix	ATDP0,01691

Table 12: Sample settings for the “Cityruf” pager service from Deutsche Telekom

i If you have defined settings for the serial interfaces, you can define whether an alarm is to trigger a call to a pager or mobile phone (see also section "Forwarding alarms" on page 51).

4.8 Making execute settings

If you have selected *Execute* for the forwarding, the *New Execute Configuration* window opens. In this window you can use the *Exec Settings* and *Time Model Settings* tabs to make all necessary settings for the Execute forwarding.

Exec Settings tab

The *Exec Settings* tab offers fields for the Execute settings, some of which already contain predefined settings.

The input fields in the *Exec Settings* window have the following meanings:

Name	Meaning
Description	Name of the Execute settings If you want to change the Execute settings for an existing Execute forwarding (see *Edit* button, section "Forwarding alarms" on page 51), this field contains the already assigned name and is disabled.
Command	Name of the command to be executed. The name can be entered with arguments as a command line. Information about the servers can be inserted into these arguments via different macros (see section "Macros" on page 78).
Working directory (optional)	Name of the working directory containing *Command*.
Time Model	Time model indicating when an alarm is to cause this command to be invoked. Select a predefined time model from the drop-down list. You can set your own time model via the *Time Model Settings* tab.

Table 13: Input fields in the Exec Settings window

Time Model Settings tab

The *Time Model Settings* tab allows you to select, add or modify a time model. You can define hour by hour for the whole week when an alarm is to be forwarded.

For Windows Server 2008, the CUI command is the only command that can be used for the program execution.

4.9 Making broadcast settings

Broadcast is a type of transmission whereby a pop-up window or a message is displayed on multiple servers or server groups simultaneously.

If you have selected for the forwarding, the *New Broadcast Configuration* window opens. In this window you can use the *Broadcast Settings* and *Time Model Settings* tabs to make all necessary settings for broadcast forwarding.

Broadcast Settings tab

The *Broadcast Settings* tab offers fields for the broadcast settings, some of which already contain predefined settings.

The input fields in the *Broadcast Settings* window have the following meanings:

Name	Meaning
Description	Name of the broadcast settings If you want to modify the broadcast settings for an existing broadcast forwarding (see *Edit* button, section "Forwarding alarms" on page 51), this field contains the already assigned name and is disabled.
Time Model	Time model indicating when an alarm is to be forwarded. Select a predefined time model from the drop-down list. You can set your own time model via the *Time Model Settings* tab.

Table 14: Input fields in the Broadcast Settings window

Name	Meaning
Mode Special user All users of domain All users with session	Mode for the broadcast forwarding Only one user is notified, whose name must be entered here. All users belonging to the same domain for the forwarding are notified. (Valid only with Windows, default.) As of Windows Server 2008, domain is no longer supported. All users who are associated with the forwarding through any session are notified (default with Linux).
Additional Message (optional)	Text field for defining the message for the broadcast window Information about the servers can be inserted via different macros (see section "Macros" on page 78). As of Windows Server 2008, the output is truncated after 255 characters.

Table 14: Input fields in the Broadcast Settings window

Time Model Settings tab

The *Time Model Settings* tab allows you to select, add or modify a time model. You can define hour by hour for the whole week when an alarm is to be forwarded.

i *Notes for Linux*

The forwarding service uses the database under /var/run/utmp (utmp(5)) to obtain information on the connected users and the type of the session (GUI or CLI). All sessions (local or remote) should therefore be correctly registered in the utmp database.

With SuSE Linux and RedHat Linux, the KDE session does not make any utmp entries via the console or the emulation that is started with it. Forwarded alarm messages are therefore not output in these windows.

These restrictions do not apply to the GNOME sessions with SuSE Linux and RedHat Linux, or for KDE sessions with Caldera OpenLinux.

Notes for Windows

Forwarding with broadcast can fail on account of disruptions to the Windows Messenger Service used. You can check this with the net send command.

4.10 Making trap settings

If you have selected *Station* for the forwarding, the *New Station Configuration* window opens. In this window you can use the *Station Settings* and *Time Model Settings* tabs to make all necessary settings for trap forwarding.

Station Settings tab

The *Station Settings* tab offers fields for the trap settings, some of which already contain predefined settings.

The input fields in the *Station Settings* window have the following meanings:

Name	Meaning
Station Name	Name of the station to which the traps are to be forwarded. If you want to modify the trap settings for an existing trap forwarding (see *Edit* button, section "Forwarding alarms" on page 51), this field contains the already assigned name and is disabled.
Community	Name of the community to which the traps are to be forwarded. The default value is *public*.
Time Model	Time model indicating when an alarm is to be forwarded. Select a predefined time model from the drop-down list. You can set your own time model via the *Time Model Settings* tab.
IP Address	Internet protocol address

Table 15: Input fields in the Station Settings window

Name	Meaning
Forwarding Mode	The mode for the forwarding.
Normal	This mode evaluates the alarm and forwards it to the management station.
Pass Through	This mode is available in an original variant and in the variant Transparent. The original variant passes the alarm directly through to the management station. The alarm appears there as if it is coming directly from the server. In this mode the trap is only forwarded once.
Transparent	The *Transparent* variant forwards the trap to the management station exactly as it was received. It is not possible to determine whether the trap was sent by the agent or forwarded by the Event Manager.

Table 15: Input fields in the Station Settings window

Time Model Settings tab

The *Time Model Settings* tab allows you to select, add or modify a time model. You can define hour by hour for the whole week when an alarm is to be forwarded.

4.11 Macros

Below is a list of macros that can be used for the forwarding of alarms (e.g. Mail, Pager).

These macros are replaced by the corresponding information about the servers which are reporting the alarm.

Name	Meaning
$_SRV	Name of the server
$_TRP	Text of the alarm message
$_TYP	Brief description of the alarm
$_IPA	IP address of the server
$_CTY	Community
$_SEV	Severity of the alarm (critical, major, minor, informational, unknown)
$_TIM	Time model (format: yyyy-mm-dd-hh.mm.ss) Local time schedule of the management station according to which an alarm is forwarded.
$_IDN	ID number of the server
$_OMS	Name of management station
$_MIB	MIB file name of the received alarm
$_SPC	Specific number of the received alarm
$_MDL	Fujitsu REMCS ID of a hardware which is reporting the alarm

Table 16: Macros

4.12 Alarm configuration example

This section explains a typical example of alarm configuration.

Purpose

When an event whose severity is critical occurs on the *ALARMTEST* server, a mail is sent to the administrator (*admin@test.co.jp*).

Requirements

– ServerView agent is running on the server, and the server is registered as a management target in ServerView Operations Manager on the same network.

– Test traps from the ServerView agent to ServerView Operations Manager are functioning normally.

– ServerView Operations Manager can access the SMTP server (111.222.3.20) while it is in operation.

Setting procedure

► Perform one of the following operations.

  – When operating from the ServerView Operations Manager start window:

    Click *Alarm Configuration*.

  – When operating from the individual function windows:

    Click *Event Management – Alarm Configuration* in the menu bar at the top of the window.

  The *Manage Alarm Rules* window opens.

► Click *Add*.

  The *New Name* dialog box opens.

► Enter e.g. *CriticalMail* in the *New Name* dialog box and click *OK*.

► Click *Apply*, then click *Next*.

  The *Assign Servers* window opens.

► Select the *ALARMTEST* server in the server list, and click the > button.

► Click *Apply*, then click *Next*.

The *Assign Alarms - Individual Alarms* window opens.

► Click *Next* again.

The *Assign Alarms - Type of Alarms* window opens.

► Check *All alarms of severity critical*.

► Click *Apply*, then click *Next*.

The *Assign Destinations* window opens.

► Click *Add*.

The *Type of new Destination* dialog box opens.

► Select *Mail* and click *OK*.

The *New Mail Configuration* window opens.

► Enter the required item in each field on the *Mail Settings* tab.

Description
In this example: *MailSet* as the destination name

Subject
In this example: *Critical Error occurred*

Mail to
In this example: *admin@test.co.jp* as the administrator

Time Model
In this example: *always*

From
In this example: *ALARMTEST*

Server
In this example: *111.222.3.20*

Configure settings for mail to the administrator (*admin@test.co.jp*) from the *ALARMTEST* server.

- ► Click *Apply*, then click *Test Address*.
- ► Once the test mail is sent successfully, click *OK*. This returns you to the *Assign Destinations* window.
- ► Select the created *MailSet*, then click the > button.
- ► Click *Apply*.

5 Traps

If a special event occurs in a network component, then the SNMP agent can send a message to one or more managers to inform them of the event. Such messages are called traps in SNMP. The manager can react to events in the network based on the incoming trap.

A trap message can be uniquely identified by means of the trap ID and MIB OID.

5.1 Displaying trap information

The Event Manager help system provides detailed information on the default MIBs and traps supported by the Event Manager.

You open the relevant overview window either via the Event Manager start window or via the *Alarm Monitor* window.

– Trap information via Event Manager start window:

  ► Start the Event Manager.

  ► Under *Help*, select *On Suite*.

  ► Then under *Event Management*, select *Alarm Monitor*.

  ► In the window that opens, click the *Event Manager* link.

  ► Under *Alarms*, select the *Agent Alarm Information* option.

– Trap information via *Alarm Monitor* window:

  ► Start the Event Manager.

  ► Under *Event Management*, select *Alarm Monitor*.

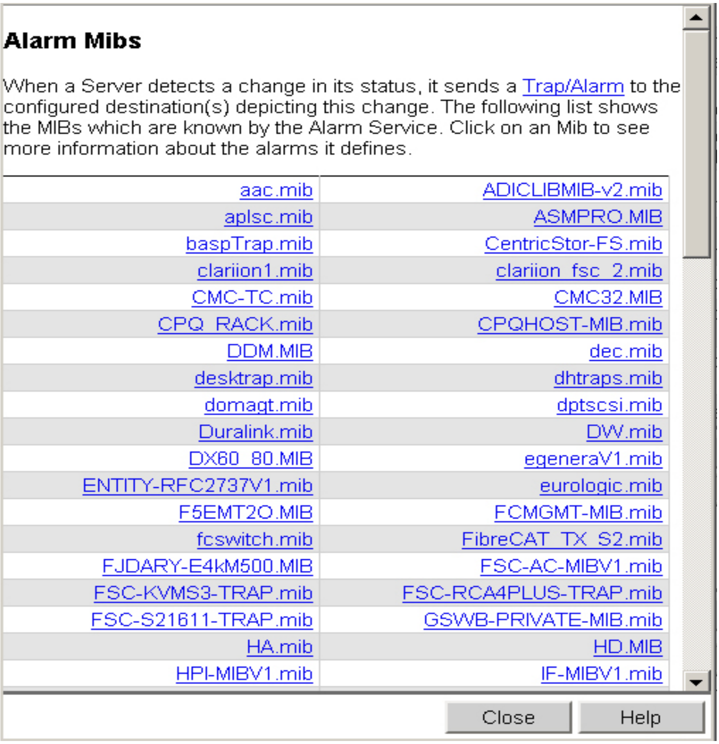
  ► In the *Alarm Monitor* window, select *Help – On Alarm Monitor* from the menu bar.

  ► In the window that opens, click the *Event Manager* link.

  ► Under *Alarms*, select the *Agent Alarm Information* option.

i The trap information can also be called up in the same way via the start window of ServerView Operations Manager.

The *Alarm Mibs* window is displayed:



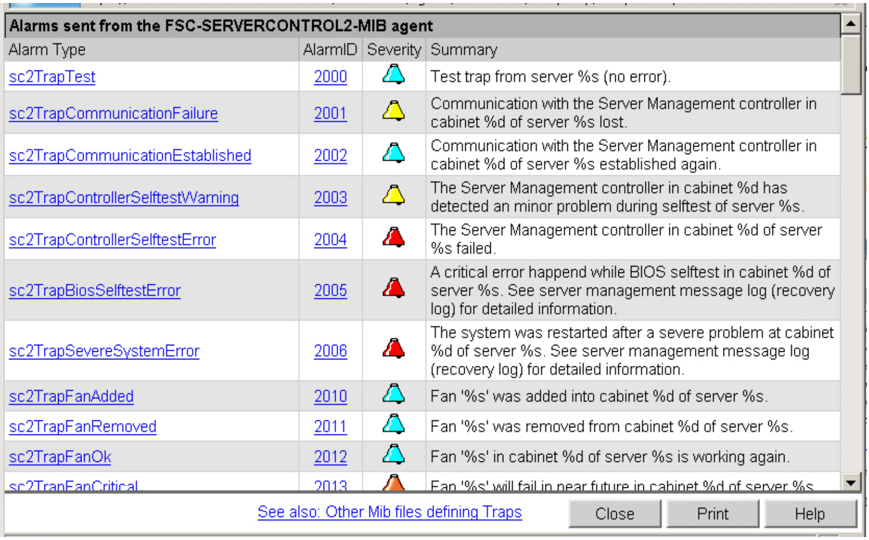
Alarm Mibs

When a Server detects a change in its status, it sends a Trap/Alarm to the configured destination(s) depicting this change. The following list shows the MIBs which are known by the Alarm Service. Click on an Mib to see more information about the alarms it defines.

aac.mib	ADICLIBMIB-v2.mib
aplsc.mib	ASMPRO.MIB
baspTrap.mib	CentricStor-FS.mib
clariion1.mib	clariion_fsc_2.mib
CMC-TC.mib	CMC32.MIB
CPQ_RACK.mib	CPQHOST-MIB.mib
DDM.MIB	dec.mib
desktrap.mib	dhtraps.mib
domagt.mib	dptscsi.mib
Duralink.mib	DW.mib
DX60_80.MIB	egeneraV1.mib
ENTITY-RFC2737V1.mib	eurologic.mib
F5EMT2O.MIB	FCMGMT-MIB.mib
fcswitch.mib	FibreCAT_TX_S2.mib
FJDARY-E4kM500.MIB	FSC-AC-MIBV1.mib
FSC-KVMS3-TRAP.mib	FSC-RCA4PLUS-TRAP.mib
FSC-S21611-TRAP.mib	GSWB-PRIVATE-MIB.mib
HA.mib	HD.MIB
HPI-MIBV1.mib	IF-MIBV1.mib

Figure 15: MIB overview in the Event Manager - example

When you select a MIB, a window with detailed trap information will open; the window will look like this:



Alarms sent from the FSC-SERVERCONTROL2-MIB agent

Alarm Type	AlarmID	Severity	Summary
sc2TrapTest	2000	🟦	Test trap from server %s (no error).
sc2TrapCommunicationFailure	2001	🟨	Communication with the Server Management controller in cabinet %d of server %s lost.
sc2TrapCommunicationEstablished	2002	🟦	Communication with the Server Management controller in cabinet %d of server %s established again.
sc2TrapControllerSelftestWarning	2003	🟨	The Server Management controller in cabinet %d has detected an minor problem during selftest of server %s.
sc2TrapControllerSelftestError	2004	🟥	The Server Management controller in cabinet %d of server %s failed.
sc2TrapBiosSelftestError	2005	🟥	A critical error happend while BIOS selftest in cabinet %d of server %s. See server management message log (recovery log) for detailed information.
sc2TrapSevereSystemError	2006	🟥	The system was restarted after a severe problem at cabinet %d of server %s. See server management message log (recovery log) for detailed information.
sc2TrapFanAdded	2010	🟦	Fan '%s' was added into cabinet %d of server %s.
sc2TrapFanRemoved	2011	🟦	Fan '%s' was removed from cabinet %d of server %s.
sc2TrapFanOk	2012	🟦	Fan '%s' in cabinet %d of server %s is working again.
sc2TrapFanCritical	2013	🟧	Fan '%s' will fail in near future in cabinet %d of server %s.

Figure 16: Detailed information about the traps from a MIB (example)

If you want to print out this information, select the *Print* button in the window.

5.2 Displaying traps in the Windows event log

When you install the Windows agents, you can specify whether the traps from the Fujitsu MIB (e.g. HD.MIB, Mylex.MIB) are also to be written to the Windows event log. The trap ID in the event log is shown increased by 10000 and not as in the subsequent trap descriptions (e.g. the trap *mylexBBUFound* with the trap number 275 is shown in the event log with the trap number 10275).

With the Event Manager you can use alarm forwarding (*logging*) to specify that traps are to be written to the Windows or LINUX event log. The source name of the events in the event log is *ServerView Services* in both Windows and Linux.

The event type of the log of *UnknownTrap* becomes an *ERROR* level.

5.3 Trap overview

The table below provides an overview of the MIBs which are integrated in the Event Manager. Because these contents are frequently updated, this table and the following trap lists are only a snapshot and do not claim to be complete. You can find out which MIBs are currently integrated in the Event Manager via the *Alarm Configuration* window (in the *MIB* column of the *Alarm Rules - Assign Alarms* dialog box) or via the Event Manager online help.

The sections after the table provide an overview of the main types of trap. In later sections of this chapter, the traps are ordered alphabetically by category. Inside each category the traps are ordered alphabetically by name.

The *Comments* column indicates the number of the page on which the traps are listed. You can also use the Event Manager to print out the trap lists. For more information, see the section "Displaying trap information" on page 83.

MIB	**Traps from**	**Comments**
aac.mib	Adaptec controller	
ADICLIBMIB-v2.mib		see page 119
adptinfo.mib		
Asmpro.mib	ASM PRIVATE COMMIB traps	see page 160
baspCfg.mib		
baspStat.mib		

Table 17: MIB overview

MIB	Traps from	Comments
baspTrap.mib	Broadcom Advanced Server traps	
BIOS.mib		
BUS.mib		
clariion1.mib	FibreCat	
clariion_fsc_2.mib	FibreCat	
Cmc32.mib	Rittal rack monitor	
CMS-TC.mib		
Ddm.mib	DuplexDataManager traps	see page 105
dec.mib	Compaq StorageWorks Enterprise Array Manager	see page 125
desktrap.mib	DeskView traps	
dhtraps.mib		
domagt.mib		
dptscsi.mib	DPT SCSI traps	see page 103
Duralink.mib	ADAPTEC Duralink traps	see page 92
DW.mib	DuplexWrite traps	see page 109
egeneraV1.mib		
Ether.mib		
eurologic.mib	FibreCat	
F5emt2o.mib	HP OpenView Network Node Manager	
fcswitch.mib	Fibre Channel switch	
FSC-AC-MIBV1.mib		
FSC-KVMS3-TRAP.mib		
FSC-RCA4PLUS-TRAP.mib		
FSC-S21611-TRAP.mib		
Hd.mib	ServerView agent: disks	see page 111
HPI-MIBV1.mib		
INTELLAN_V1.mib		
INVENT.mib		
iommib.mib	Adaptec	

Table 17: MIB overview

MIB	Traps from	Comments
Ldcm.mib	LAN Desk Client Manager from Intel traps	see page 162
Ldsm.MIB	LAN Desk Server Manager from Intel traps	see page 162
log3v1.mib	PRIMEPOWER log entries	see page 120
Lsi1030.mib		
LSIRAID-IDE.mib		
Megaraid.mib	RAID adapter from American Mega Trends Inc.	see page 129
Mlxraid.mib	MylexDiskArrayController traps	
MMB-COM-MIB.mib		
MMB-ComTrap-MIB.mib		
mp.mib	MultiPath traps	see page 113
Mylex.mib	RAID controller (Mylex DAC 960)	see page 114
net-snmp.mib		
netapp.mib	Network Appliance traps	
NT.mib		
NTCluster.MIB	Microsoft Cluster	see page 100
NW.mib		
OS2.mib		
pcihotplug.mib	SCSI device hot-plug traps	see page 118
Powernet.mib	American Power Conversion traps	see page 92
Ppc.mib	UPS traps 2	see page 169
primepower_xscf.mib	PRIMEPOWER hardware diagnostics	see page 119
promiseraid.mib		
promisev1.mib	Promise RAID controller traps	
PSA-COM-MIB.mib	PRIMEQUEST traps	
PSA-ComTrap-MIB.mib	PRIMEQUEST traps	
PSA-ExternalFileUnitTrap-MIB.mib	PRIMEQUEST traps	
PSA-LIN-MIB.mib	PRIMEQUEST traps	

Table 17: MIB overview

MIB	Traps from	Comments
PSA-LinBcm5700Trap-MIB.mib	PRIMEQUEST traps	
PSA-LinEmulexTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinGdsTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinGlsTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinGrmpdTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinIntelE1000Trap-MIB.mib	PRIMEQUEST traps	
PSA-LinIntelE100Trap-MIB.mib	PRIMEQUEST traps	
PSA-LinLanComTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinLsiLogicTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinScsiComTrap-MIB.mib	PRIMEQUEST traps	
PSA-LinTg3Trap-MIB.mib	PRIMEQUEST traps	
PSA-WIN-MIB.mib	PRIMEQUEST traps	
PSA-WinBcm5700Trap-MIB.mib	PRIMEQUEST traps	
PSA-WinEmulexTrap-MIB.mib	PRIMEQUEST traps	
PSA-WinIntelE1000Trap-MIB.mib	PRIMEQUEST traps	

Table 17: MIB overview

MIB	Traps from	Comments
PSA-WinIntelE100Trap-MIB.mib	PRIMEQUEST traps	
PSA-WinLsiLogicTrap-MIB.mib	PRIMEQUEST traps	
RAID.mib		
RFC1157.mib		
RFC1213.mib		
RFC1285.mib		
RFC1628.mib		
RMS-C_SNMPv1_contact.mib		
RMS-C_SNMPv1_humid1.mib		
RMS-C_SNMPv1_humid2.mib		
RMS-C_SNMPv1_main.mib		
RMS-C_SNMPv1_output.mib		
RMS-C_SNMPv1_temp2.mib		
Rompilot.mib	RomPilot traps	see page 132
S31.mib	Blade server traps	
SANMgrV1.mib	Pathlight SAN Data Gateway	
SC.mib	ServerControl traps	see page 133
SC2.mib		
SECURITY.mib		
Servervi.mib	FUJITSU ServerVisor traps	

Table 17: MIB overview

MIB	Traps from	Comments
ServerView.mib	ServerView traps	see page 145
Status.mib	ServerView status traps	see page 146
tapealrt.mib	Tape driver traps	see page 147
Threshold.mib		
TOK.mib		
Trap.mib	ServerView traps	see page 163
trap1493.mib	Switch traps	
trap1757.mib	Switch traps	
unicorn-trap.mib		
uniserv.mib	PRIMEPOWER Enterprise Server	see page 121
UNIX.mib		
Upsman.mib	Enterprise Specific Top Level MIB by Quazar GmbH, UPS traps 1	see page 168
v1_fscHaCl.mib	PRIMECLUSTER traps	
VMWARE-TRAPS-MIB.mib		
VV.mib		
WFM.mib	Wired-for-Management traps	
wsatrap.mib	PRIMEPOWER hardware	

Table 17: MIB overview

5.3.1 Adaptec traps (Duralink.mib)

MIB-OID: 1.3.6.1.4.1.795.3.1.2.3

This section lists Adaptec traps in alphabetical order.

Trap name	ID	Meaning	Error class
duralinkStatusTrap	1	The link status has changed.	informational
failoverStatusTrap	1	The failover status has changed.	informational

Table 18: Adaptec traps

5.3.2 APC traps (Powernet.mib)

MIB-OID: 1.3.6.1.4.1.318

This section lists the APC traps in alphabetical order.

Trap name	ID	Meaning	Error class
baseFanFailure	25	The base module bypass power supply is defective.	major
batteryPackComm Established	27	The UPS can communicate with the external battery pack.	informational
batteryPackCommLost	26	Communication with external battery packs interrupted.	major
bypassPowerSupply Failure	24	The base module bypass power supply is defective.	major
calibrationStart	28	A test to determine the battery strength has been initiated by the UPS.	informational
codeAuthentication Done	32	Authentication based on the agent code image has been completed.	informational

Table 19: APC traps

Trap name	ID	Meaning	Error class
communication Established	8	Communication is established between the agent and power supply.	informational
communicationLost	1	Communication between the agent and power supply was interrupted.	major
contactFault	18	One of the contacts on the Measure UPS has changed from its default position.	major
contactFaultResolved	19	An error on one of the Measure UPS contacts has been resolved.	informational
hardwareFailure Bypass	20	The UPS is on bypass due to a hardware failure.	major
lowBattery	7	The UPS system batteries are low and will soon be exhausted. If utility power is not restored the UPS will put itself to *sleep* and immediately cut power to the load.	major
powerRestored	9	Utility power has been restored after the occurrence of an *upsOnBattery* condition.	informational
restartAgent	29	The agent was restarted on the command of the manager.	informational
returnFromBypass	23	The UPS has returned from bypass mode.	informational
returnFromLowBattery	11	The UPS has returned from a *lowBattery* condition.	informational
smartAvrReducing	31	The UPS has enabled SmartAVR voltage reduction.	minor
smartBoostOn	6	The UPS has enabled *SmartBoost*.	minor

Table 19: APC traps

Trap name	ID	Meaning	Error class
softwareBypass	21	The UPS has been set to bypass by a user via software or via the UPS front panel.	minor
switchedBypass	22	The UPS has been set to bypass by a user via the switch on the back.	minor
upsBatteryNeeds Replacement	17	The UPS batteries require immediate replacement.	major
upsDiagnosticsFailed	3	Internal UPS self-test failed.	major
upsDiagnosticsPassed	10	Internal UPS self-test passed.	informational
upsDipSwitchChanged	16	The UPS DIP switch settings have been changed.	minor
upsDischarged	4	The UPS batteries are discharged. If utility power fails an immediate low battery condition will exist. Sufficient runtime for necessary action cannot be guaranteed.	major
upsOnBattery	5	The UPS is now providing battery backup power.	minor
upsOverload	2	The UPS has sensed a load greater than 100% of its rated capacity.	major
upsRebootStarted	15	The UPS has started the reboot sequence. The UPS will reboot itself at this time.	minor
upsSleeping	13	The UPS is entering *sleep* mode.	minor
upsTurnedOff	12	The UPS has been switched off by a management station.	minor
upsTurnedOn	30	The UPS is turned on.	informational
upsWokeUp	14	The UPS has woken up from *sleep* mode. Power to the load has been restored.	informational

Table 19: APC traps

5.3.3 Blade System traps (s31.mib)

MIB-OID: 1.3.6.1.4.1.7244.1.1.1

This section lists the blade system traps in alphabetical order.

Trap name	ID	Meaning	Error class
s31LivetimeError	1644	The lifetime of the blade system has exceeded the limited count.	informational
s31MgmtBladeAdded	1601	A management blade was added to the blade system.	informational
s31MgmtBladeCriticalError	1605	The management blade status at the blade system is critical.	critical
s31MgmtBladeError	1604	The management blade status at the blade system is error.	major
s31MgmtBladeOk	1603	The management blade status at the blade system is ok.	informational
s31MgmtBladeRemoved	1602	A management blade was removed from the blade system.	informational
s31NicDetectionFail	1646	The management blade NIC detection has failed.	informational
s31PowerOverBudget	1645	The server blade at the blade system power on failed because of over power budget.	informational
s31ServerBladeAdded	1606	A server blade was added to the blade system.	informational
s31ServerBladeCritical Error	1610	The server blade status at the blade system is critical.	critical

Table 20: Blade System Traps

Trap name	ID	Meaning	Error class
s31ServerBladeError	1609	The server blade status at the blade system is error.	critical
s31ServerBladeHot Replace	1640	A server blade was added by hot replace.	informational
s31ServerBladeNewAdd	1639	A server blade was added on an empty slot of the blade system.	informational
s31ServerBladeOk	1608	The server blade status at the blade system is ok.	informational
s31ServerBladeRemoved	1607	A server blade was removed from the blade system.	informational
s31ServerBootError	1633	No bootable operating system is found at the server blade of the blade system.	informational
s31ServerBootWatchdog Expired	1636	Boot watchdog at the server blade of the blade system was expired.	informational
s31ServerPostError	1632	The Power On Self Test status of the server blade at the blade system is error.	informational
s31ServerPowerOff	1641	The server blade was powered off.	informational
s31ServerPowerOn	1631	The server blade at the blade system is powered on.	informational
s31ServerShutdown	1634	The server blade at the blade system is shut down.	informational
s31ServerSoftware WatchdogExpired	1635	Software watchdog at the server blade of the blade system was expired.	informational

Table 20: Blade System Traps

Trap name	ID	Meaning	Error class
s31SwitchBladeAdded	1611	A switch blade was added to the blade system.	informational
s31SwitchBladeCritical Error	1615	The switch blade status at the blade system is critical.	critical
s31SwitchBladeError	1614	The switch blade status at the blade system is error.	major
s31SwitchBladeOk	1613	The switch blade status at the blade system is ok.	informational
s31SwitchBladeRemoved	1612	A switch blade was removed from the blade system.	informational
s31SysFanAdded	1616	A system fan was added to the blade system.	informational
s31SysFanCriticalError	1620	The system fan status at the blade system is critical.	critical
s31SysFanError	1619	The system fan status at the blade system is error.	major
s31SysFanOk	1618	The system fan status at the blade system is ok.	informational
s31SysFanRemoved	1617	A system fan was removed from the blade system.	informational
s31SysPowerSupplyAdded	1626	A power supply unit was added to the blade system.	informational
s31SysPowerSupplyCritical Error	1630	The power supply unit status is critical.	critical
s31SysPowerSupplyError	1629	The power supply unit at the blade system failed.	major
s31SysPowerSupplyOk	1628	The power supply unit at the blade system is working again.	informational

Table 20: Blade System Traps

Trap name	ID	Meaning	Error class
s31SysPowerSupplyRemoved	1627	A power supply unit was removed from the blade system.	informational
s31SysTempCriticalError	1623	The temperature at the system temperature sensor of the blade server has reached the critical level.	critical
s31SysTempError	1622	The temperature at the system temperature sensor of the blade server is out of normal range.	major
s31SysTempOk	1621	The temperature at the system temperature sensor of the blade server is within normal range.	informational
s31SysTempSensorAdded	1642	A system temperature sensor was added to the blade system.	informational
s31SysTempSensorBroken	1625	The system temperature sensor of the blade server is broken or not connected.	major
s31SysTempSensorOK	1624	The system temperature sensor of the blade server is working again.	informational
s31SysTempSensor Removed	1643	A system temperature sensor was removed from the blade system.	informational
s31TestTrap	1600	A test trap was sent from the blade system (no error).	informational

Table 20: Blade System Traps

Trap name	ID	Meaning	Error class
s31TrapEventLog	1638	An error was recorded on the blade system. See the server management event error log (Recovery) for detailed information.	major
s31UserAuthentication Failure	1637	An user authentication failure was detected at the blade system. Performing the protocol.	major

Table 20: Blade System Traps

5.3.4 Cluster traps (NTCluster.mib)

MIB-OID: 1.3.6.1.4.1.231

This section lists cluster traps in alphabetical order.^

Trap name	ID	Meaning	Error class
sniWpChange ClusterActiveAgain	811	The SNMP agent has established the connection with the cluster service.	informational
sniWpChange ClusterNoLonger Active	812	The SNMP agent has lost the connection with the cluster service.	critical
sniWpChange ClusterNotFound Active	810	The SNMP agent has started the cluster service but could not communicate with it.	critical
sniWpChange GroupAdded	851	A new resource group was created.	informational
sniWpChange GroupDeleted	850	A resource group was deleted.	critical
sniWpChange GroupProperty	853	The settings for a resource group have been changed.	major
sniWpChange GroupState	852	A resource group has changed its status.	major
sniWpChange NetInterfaceAdded	921	A new network interface was created.	informational
sniWpChange NetInterfaceDeleted	920	A network interface was deleted.	critical
sniWpChange NetInterfaceProperty	923	The settings for a network interface have been changed.	major
sniWpChange NetInterfaceState	922	A network interface has changed its status.	major
sniWpChange NetworkAdded	911	A network was added to the cluster.	informational

Table 21: Cluster traps

Trap name	ID	Meaning	Error class
sniWpChange NetworkDeleted	910	A network was deleted from the cluster.	critical
sniWpChange NetworkProperty	913	The settings for a network have been changed.	major
sniWpChange NetworkState	912	A network has changed its status.	major
sniWpChange NodeAdded	831	A new node was added to the cluster.	informational
sniWpChange NodeDeleted	830	A node has been permanently deleted from the cluster.	informational
sniWpChange NodeState	832	A cluster node has changed its status.	major
sniWpChange RegistryAttributes	895	The registry attributes of the cluster were changed.	informational
sniWpChange RegistryKey	896	A registry key of the cluster was created or deleted.	informational
sniWpChange RegistryValue	897	A registry value of a cluster was changed or deleted.	informational
sniWpChange ResourceAdded	861	A new resource was created in the cluster.	informational
sniWpChange ResourceDeleted	860	A cluster resource was deleted.	critical
sniWpChange ResourceProperty	863	The settings of a cluster resource have been changed.	major
sniWpChange ResourceState	862	A cluster resource has changed its status.	major
sniWpChange ResourceTypeAdded	841	A new type of resource was created.	informational
sniWpChange ResourceType Deleted	840	A resource type was deleted.	critical

Table 21: Cluster traps

Trap name	ID	Meaning	Error class
sniWpChange Unknown	801	The cluster API has returned a note type that does not have an associated trap definition.	critical

Table 21: Cluster traps

5.3.5 DPT traps (dptscsi.mib)

MIB-OID: 1.3.6.1.4.1.1597

This section lists DPT traps in alphabetical order.

Trap name	ID	Meaning	Error class
dptArrayCfgChangeTrap	12	Configuration of a RAID array changed due to one of the following events: – creating a new array – deleting an existing array – modifying an array (changing stripe size, etc.)	informational
dptDevBlock ReassignedTrap	6	The HBA reassigned a block. *dptScsiDevBadBlockNumber* contains the reassigned block number.	informational
dptDevData InconsistentTrap	7	The RAID verify function found a data inconsistency. *dptScsiDevBadBlockNumber* and *dptScsiDevBadBlockCount* contains the starting block number and the number of blocks affected, respectively.	informational
dptDevError ThresholdHitTrap	8	The status of the particular device changed and the error count crossed the device crash threshold.	informational
dptDevLocking StatusChangedTrap	10	Locking of drive started/stopped.	informational
dptDevReqSenseTrap	11	Request sense information received from the HBA.	informational

Table 22: DPT traps

Trap name	ID	Meaning	Error class
dptDevStatus ChangedTrap	9	Status of the SCSI device changed.	informational
dptHbaCorrected HardRAMErrorTrap	4	The HBA encountered an ECC RAM error and corrected it. *dptScsiHbaBadMemoryAddress* contains the RAM address.	informational
dptHbaSoftRAM ErrorTrap	3	The HBA encountered an ECC RAM error, but the error is not found on the physical disk block. *dptScsiHbaBadMemoryAddress* contains the RAM address.	informational
dptHbaTemperature ChangeTrap	2	Normal temperature restored on the HBA.	informational
dptHbaUnCorrectable HardRAMErrorTrap	5	The HBA encountered an ECC RAM error and could not correct it. *dptScsiHbaBadMemoryAddress* contains the RAM address.	informational
dptHbaVoltage ChangeTrap	1	Low voltage detected on the HBA.	informational
dptUnknownErrorTrap	13	An event has occurred as defined by the value of the object *dptScsiEventInfo*.	informational

Table 22: DPT traps

5.3.6 DuplexDataManager traps (Ddm.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists DuplexDataManager traps in alphabetical order.

Trap name	ID	Meaning	Error class
FscDdmNewConfig	1400	After the driver has created a new DuplexWrite group or has added a new disk to an existing DuplexWrite group as requested by the user.	informational
FscDdmPieceRemoved	1401	After the driver has removed a disk from a DuplexWrite group as requested by the user.	informational
FscDdmConfigRemoved	1402	After the driver has removed a DuplexWrite group as requested by the user.	informational
FscDdmStatusSet	1403	After the driver has set the status of a DuplexWrite disk as requested by the user.	minor
FscDdmUpdateStatus	1404	After the driver has updated the status of a DuplexWrite disk.	minor
FscDdmPieceRecovered	1405	The recovery of a DuplexWrite group has been completed successfully.	informational
FscDdmRecoverAborted	1406	At the request of the user the recovery process of a DuplexWrite group has been aborted.	minor

Table 23: DDM-Traps

Trap name	ID	Meaning	Error class
FscDdmReservationConflict	1407	A reservation conflict has been detected. From now on an entire DuplexWrite group is no longer available. This leads to an error if a conflict of operation (not initialization) occurs in the group.	major
FscDdmConfigChanged	1408	Repeated reading of the configuration by the driver detects a modified configuration.	informational
FscDdmConfigInvalidated	1409	The configuration information of a DuplexWrite group is declared not valid. The configuration information is reread before the next access of the DuplexWrite group on this cluster element.	informational
FscDdmActiveLunChanged	1410	After the driver has selected a specified disk of a DuplexWrite group for read commands.	informational
FscDdmPieceFailed	1411	An error was detected on a DuplexWrite group.	critical
FscDdmRootFlagChanged	1412	The RootDisk behavior of a DuplexWrite group has been modified.	informational
FscDdmForceActive	1413	A disk of a DuplexWrite group has been marked by the driver as forced active at reboot. The partner disk can be used as Snapshot.	informational

Table 23: DDM-Traps

Trap name	ID	Meaning	Error class
FscDdmNameChanged	1414	After the driver has changed the name of a DuplexWrite group.	informational
FscDdmPathFailed	1415	After the driver has detected an error on one path of a MultiPath group.	critical
FscDdmRetry	1416	After the driver has detected an error on one path of a MultiPath group and the retry of the command was successful on another path.	major
FscDdmActivePortChanged	1417	After the driver has changed the active path of a MultiPath group.	informational
FscDdmReconfigured	1418	Change has been detected detected in the MultiPath configuration.	informational
FscDdmStatusChanged	1419	After the driver has changed the status of a MultiPath path.	informational
FscDdmAutoRecovered	1420	After the driver has enabled a path of a MultiPath group (AutoRecovery).	informational
FscDdmErrorCleared	1421	After the driver has cleared the error status of a MultiPath path.	informational
FscDdmPnPRemove	1422	After the driver has detected a Plug and Play Removal.	informational
FscDdmPnPNew	1423	After the driver has detected a Plug and Play Add.	informational

Table 23: DDM-Traps

Trap name	ID	Meaning	Error class
FscDdmDdmCluster	1424	After the DuplexDataManager service has detected a cluster configuration change.	informational

Table 23: DDM-Traps

5.3.7 DuplexWrite traps (DW.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists DuplexWrite traps in alphabetical order.

Trap name	ID	Meaning	Error class
sieDWActiveLunChanged	1310	A user has changed the read path for a DuplexWrite group to a certain disk.	informational
sieDWConfig Changed	1308	The driver has reread the configuration and found a modified configuration.	informational
sieDWConfigInvalidated	1309	The DuplexWrite cluster service has invalidated the configuration information for a disk. The configuration information is reread before the next access of the disk on this cluster element.	informational
sieDWDiskRegistered	1351	A user has locked or released a disk for use with DuplexWrite by changing the registration. This setting has no effect on the driver until the system was restarted.	informational
sieDWConfigRemoved	1302	A user has removed a DuplexWrite group. The action was requested by the configuration utility.	informational
sieDWNewConfig	1300	A user has created a new DuplexWrite group or has added a disk to an existing DuplexWrite group as requested by the configuration utility.	informational

Table 24: DuplexWrite traps

Trap name	ID	Meaning	Error class
sieDWPieceFailed	1311	The driver has detected an error on one of the disks of a DuplexWrite group.	critical
sieDWPieceRecovered	1305	A DuplexWrite group was successfully recovered. Both elements of the DuplexWrite group have the status ONLINE.	informational
sieDWPieceRemoved	1301	A user has removed a disk from a DuplexWrite group. The action was requested by the configuration utility.	informational
sieDWRecoverAborted	1306	A user has aborted the recovery process of a DuplexWrite group.	minor
sieDWRefreshFinished	1350	The driver interface has updated the internal data structures.	informational
sieDWReservationConflict	1307	The driver has detected a reservation conflict. A whole DuplexWrite group is no longer accessible. This is not an error if it occurs during the initialization phase.	major
sieDWStatusSet	1303	A user has modified the status of a disk of a DuplexWrite group. The action was requested by the configuration utility.	minor
sieDWUpdateStatus	1304	The driver has updated the status of a DuplexWrite group.	minor

Table 24: DuplexWrite traps

5.3.8 Hard disk (S.M.A.R.T.) traps (Hd.mib)

This section lists hard disk traps in alphabetical order.

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Trap name	ID	Meaning	Error class
sniSMARTFailure Predicted	750	S.M.A.R.T. is warning that a hard disk may fail.	critical
sniSMARTMonitoring Disabled	751	The S.M.A.R.T. configuration has been changed.	informational

Table 25: Hard disk traps

5.3.9 Generic traps

This section lists generic traps in alphabetical order.

Trap name	ID	Meaning	Error class
coldStart	0	An agent was restarted. MIB view objects may have changed.	minor
egpNeighborLoss	5	An EGP neighbor of the managed node changed from the *UP* to the *DOWN* state.	major
linkDown	2	An interface of the managed node changed from the *UP* to the *DOWN* state.	critical
linkUp	3	One interface of the managed node changed from the *DOWN* to the *UP* state.	minor
warmStart	1	An agent was reinitialized, objects remain unchanged.	minor

Table 26: Generic traps

5.3.10 MultiPath traps (mp.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists MultiPath traps in alphabetical order.

Trap name	ID	Meaning	Error class
sieMP ActivePortChanged	1202	The user has enabled or disabled a path of a MultiPath group.	informational
sieMPAutoRecovered	1205	A path of a MultiPath group, which was in error status, is accessible again due to automatic recovery.	informational
sieMPError	1200	A MultiPath group now consists of only one path, and an error has been detected for this path. The MultiPath group is not operational anymore.	critical
sieMPErrorCleared	1206	A user has cleared the error status for a path of a MultiPath group.	informational
sieMPReconfigured	1203	A path has been removed from or added to a MultiPath group.	informational
sieMPRetry	1201	An error has been detected on a path of a MultiPath group. An attempt is being made to execute the command on another path of the MultiPath group.	critical
sieMPStatusChanged	1204	A user has made a change to a MultiPath group (autorecovery was turned on or off, loadbalancing was turned on or off, or one path was enabled or disabled.	informational

Table 27: MultiPath traps

5.3.11 Mylex traps (Mylex.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists Mylex traps in alphabetical order.

Trap name	ID	Meaning	Error class
mylexAdapterDied	221	Connection to a disk array controller interrupted.	critical
mylexAutoRebuild Started	200	Automatic rebuild of a unit has been started.	critical
mylexAutoRebuild Started2	222	Automatic rebuild of a system drive has been started.	informational
mylexBBUFound	275	Battery Backup Unit found.	informational
mylexBBUPowerLow	276	Battery Backup Unit power is low.	critical
mylexBBUPowerOK	277	Battery Backup Unit power is OK.	informational
mylexGamDriver IncorrectVersion	262	Incorrect version of GAM driver installed.	minor
mylexGamDriverMissing	261	GAM driver is either not installed or has not been started.	minor
mylexInitialization Cancelled	231	Initialization of system drive canceled.	informational
mylexInitializationDone	230	Initialization of system drive completed successfully.	informational
mylexInitializationFailed	232	Initialization of system drive has failed.	major
mylexInitializationStarted	229	Initialization of system drive started.	informational
mylexLogicalDriveCritical	215	A logical drive is in a critical state. One drive in a RAID configuration has failed.	major

Table 28: Mylex traps

Trap name	ID	Meaning	Error class
mylexLogicalDriveOffline	214	Logical drive is offline.	critical
mylexLogicalDriveOnline	216	Logical drive is online.	critical
mylexManualRebuild Started	201	Manual rebuild started.	informational
mylexManualRebuild Started2	223	Manual rebuild started. After the rebuild has finished successfully, *mylexRebuildDone2* will be sent.	informational
mylexParityCheck Cancelled	210	Parity check canceled.	informational
mylexParityCheckDone	209	Parity check completed successfully.	informational
mylexParityCheckError	212	Parity check error detected.	major
mylexParityCheck LogicalDriveFailed	213	Parity check: logical drive has failed.	major
mylexParityCheckStarted	208	Parity check started.	informational
mylexParityCheckStatus	211	Parity check status.	informational
mylexPhysicalDevice Added	257	Physical device added.	informational
mylexPhysicalDevice Alive	218	Physical device online.	informational
mylexPhysicalDevice Died	217	Physical device is off.	critical
mylexPhysicalDevice HardError	251	A permanent error has occurred in the physical device.	minor
mylexPhysicalDevice Hotspare	250	Physical device is now a hot-spare device.	informational
mylexPhysicalDevice MiscError	254	A miscellaneous error has occurred in physical device.	minor
mylexPhysicalDevice ParityError	253	Parity error has occurred in physical device.	minor

Table 28: Mylex traps

Trap name	ID	Meaning	Error class
mylexPhysicalDevice Prefailure	255	Prefailure alert from physical device.	major
mylexPhysicalDevice Removed	258	Physical device has been removed.	major
mylexPhysicalDevice SoftError	252	A normal (soft) error has occurred in physical device.	minor
mylexPhysicalDevice Unconfigured	256	Physical device is unconfigured.	minor
mylexRaidExpansion Done	236	RAID capacity expansion completed successfully.	minor
mylexRaidExpansion Failed	237	RAID capacity expansion failed.	major
mylexRaidExpansion Started	235	RAID capacity expansion started.	informational
mylexRaidTypeChanged	240	RAID type of system drive was changed.	informational
mylexRebuildCancelled	203	Rebuild has been canceled.	informational
mylexRebuildCancelled2	225	Rebuild of system drive has been canceled.	informational
mylexRebuildDone	202	Rebuild has been completed successfully.	informational
mylexRebuildDone2	224	Rebuild of system drive completed successfully.	informational
mylexRebuildError	205	Rebuild error detected.	major
mylexRebuildError2	226	Rebuild error on system drive detected.	major
mylexRebuildLogical DriveFailed	207	Rebuild finished at disk array adapter; bad blocks detected.	major
mylexRebuildLogical DriveFailed2	228	Rebuild of system drive finished; system drive in server has failed.	major

Table 28: Mylex traps

Trap name	ID	Meaning	Error class
mylexRebuildNew DeviceFailed	206	Rebuild finished; new device failed.	major
mylexRebuildNewDevice Failed2	227	Rebuild of system drive; new device has failed.	major
mylexRebuildStatus	204	Rebuild status.	informational
mylexSMART ConfigurationChanged	271	S.M.A.R.T. configuration has been changed.	informational
mylexSMART FailurePredicted	270	Sent if a failure (S.M.A.R.T.) has been predicted on a physical disk.	critical
mylexStateChange TableFull	220	Cache change table full. Too many configuration changes have occurred since last warm start.	major
mylexSystemDriveBad Block	238	Bad block detected in system drive.	minor
mylexSystemDrive Created	233	System drive created.	informational
mylexSystemDrive Deleted	234	System drive deleted.	informational
mylexSystemDrive SizeChanged	239	System drive size changed.	informational
mylexWriteBackError	219	Controller cache write-back error.	major
mylexWriteBackError2	260	Controller cache write-back error.	major

Table 28: Mylex traps

5.3.12 PCI HotPlug traps (pcihotplug.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists PCI HotPlug traps in alphabetical order.

Trap name	ID	Meaning	Error class
sieDeviceHotPlug TrapHotAdd	1022	A SCSI device was added.	informational
sieDeviceHotPlug TrapHotRemoval	1020	A SCSI device was removed.	informational
sieDeviceHotPlug TrapHotReplace	1021	A SCSI device was replaced.	informational
siePciHotPlugTrap EndHotPlugAction	1002	The HotPlug action for the physical slot number held in *pciHotPlugTrapPhysicalSlotNumber* object was finished.	informational
siePciHotPlugTrap HotRemoval	1000	A Hot Removal action has been started.	informational
siePciHotPlugTrap HotReplace	1001	A Hot Replace action has been started.	informational

Table 29: PCI HotPlug traps

5.3.13 PRIMEPOWER traps

This section describes the traps supplied with PRIMEPOWER.

ADICLIBMIB-V2 traps (ADICLIBMIB-v2.mib)

MIB-OID: 1.3.6.1.4.1.3764.3

Trap name	ID	Meaning	Error class
doorStateChange	2	The door state has changed.	informational
error	6	The device has an error. Error code and error data is displayed.	informational
mailboxStateChange	3	The mailbox state has changed.	informational
sac	7	The device has generated a SAC code.	informational
shutdown	5	The device has been shut down. The shutdown state is displayed.	informational
startup	4	The device was started. The shutdown state is displayed.	informational
statusChange	1	The status has changed. Previous status is displayed.	informational

Table 30: ADICLIBMIB traps

DOMAIN-MIB traps (domagt.mib)

MIB-OID: 1.3.6.1.4.1.231.2.41

Trap name	ID	Meaning	Error class
domNodeAdded	52	A client was added to domain.	informational
domNodeDeleted	53	A client was deleted.	informational
domNodeOffline	50	A client went offline.	informational
domNodeOnline	51	A client went online.	informational

Table 31: DOMAIN-MIB traps

Trap name	ID	Meaning	Error class
domNoManagementServer	55	An agent was stopped.	informational
domStartTrap	54	An agent was started.	informational

Table 31: DOMAIN-MIB traps

FSC-LOG3-MIB traps (log3v1.mib)

MIB-OID: 1.3.6.1.4.1.231.2.46.2

Trap name	ID	Meaning	Error class
log3AlertNotice	2	A log3Event has occurred. System, module, error and text is displayed.	critical
log3CriticalNotice	3	A log3Event has occurred. System, module, error and text is displayed.	critical
log3DebugNotice	8	A log3Event has occurred. System, module, error and text is displayed.	informational
log3EmergencyNotice	1	A log3Event has occurred. System, module, error and text is displayed.	critical
log3ErrorNotice	4	A log3Event has occurred. System, module, error and text is displayed.	major
log3InformationalNotice	7	A log3Event has occurred. System, module, error and text is displayed.	informational
log3NoticeNotice	6	A log3Event has occurred. System, module, error and text is displayed.	informational
log3OtherNotice	9	A log3Event has occurred. System, module, error and text is displayed.	informational

Table 32: FSC-LOG3-MIB traps

Trap name	ID	Meaning	Error class
log3WarningNotice	5	A log3Event has occurred. System, module, error and text is displayed.	minor

Table 32: FSC-LOG3-MIB traps

UNISERV-MIB traps (uniserv.mib)

MIB-OID: 1.3.6.1.4.1.231.2.41

Trap name	ID	Meaning	Error class
kaiPartitionOffline	700	A partition was powered off.	minor
kaiPartitionOnline	701	A partition was powered on.	informational

Table 33: UNISERV-MIB traps

PRIMEPOWER-XSCF-MIB traps (primepower_xscf.mib)

MIB-OID: 1.3.6.1.4.1.211.1.15.2.1

Trap name	ID	Meaning	Error class
scfAgentStart	5	XSCF agent has started.	informational
scfHardwareDefectRepair	7	A hardware defect was repaired.	minor
scfHardwareDefectSet	1	A hardware defect has occurred.	critical
scfHardwareDefectUnset	2	A hardware defect was reset.	informational
scfHardwareErrorRepair	6	A hardware error was repaired.	minor
scfHardwareErrorSet	3	A hardware error has occurred.	critical
scfHardwareErrorUnset	4	A hardware error was reset.	informational

Table 34: PRIMEPOWER-XSCF-MIB traps

FSC-HACL-MIB traps (v1_fscHaCl.mib)

MIB-OID: 1.3.6.1.4.1.231.2.42.2.0

Trap name	ID	Meaning	Error class
fscHaClApplicationStateChanged	5	Application state has changed.	major
fscHaClClusterInfAvailable	1	Cluster information is available. InfoOperScope is displayed.	informational
fscHaClClusterInfNotAvailable	2	Cluster information is no longer available. InfoOperScope is displayed.	major
fscHaClMonitorStateChanged	3	Cluster monitoring state has changed.	major
fscHaClResourceStateChanged	6	Resource state has changed.	minor
fscHaClSystemStateChanged	4	System state has changed.	critical

Table 35: FSC-HACL-MIB traps

WSA-TRAP-MIB traps (wsatrap.mib)

MIB-OID: 1.3.6.1.4.1.231.2.41

Trap name	ID	Meaning	Error class
testTrap	600	Test trap from server (no error).	informational
wsaAgentStart	5	WsaAgent has started.	informational
wsaControllerHardwareDefectSet	307	Defect on controller hardware has occurred.	critical
wsaControllerHardwareErrorSet	308	Error on controller hardware has occurred.	critical
wsaControllerRepair	309	Controller was repaired.	minor
wsaDefectRepair	7	A defect was repaired.	minor
wsaDROperationStarted	312	DR operation was started.	informational

Table 36: WSA-TRAP-MIB traps

Trap name	ID	Meaning	Error class
wsaDROperationFinished	313	DR operation was terminated.	informational
wsaEnvironmentHardwareDefectSet	301	Defect on environment hardware has occurred.	critical
wsaEnvironmentHardwareErrorSet	302	Error on environment hardware has occurred.	critical
wsaEnvironmentRepair	303	Environment component was repaired.	minor
wsaErrorRepair	6	An error was repaired.	minor
wsaGenLogMessage	900	Error in one module on server has occurred.	informational
wsaGenLogMessageInfo	910	Error in one module on server has occurred.	informational
wsaGenLogMessageCritical	913	Error in one module on server has occurred.	critical
wsaGenLogMessageMajor	912	Error in one module on server has occurred.	major
wsaGenLogMessageMinor	911	Error in one module on server has occurred.	minor
wsaHardwareActiveSet	315	Hardware active was set.	informational
wsaHardwareDeactiveSet	314	Hardware deactive was set.	critical
wsaHWComponentAttached	316	Hardware component has been attached.	informational
wsaHWComponentDetached	317	Hardware component has been detached.	informational
wsaLarHardwareDefectSet	1	A hardware defect has occurred.	critical
wsaLarHardwareDefectUnset	2	A hardware defect was repaired.	informational
wsaLarHardwareErrorSet	3	A hardware error has occurred.	critical

Table 36: WSA-TRAP-MIB traps

Trap name	ID	Meaning	Error class
wsaLarHardwareErrorUnset	4	A hardware error was repaired.	informational
wsaLUNStateChanged	101	State of LUN has changed.	critical
wsaMonitoringRuleInitialized	311	EEM rule was initialized.	minor
wsaMonitoringRuleMatched	310	EEM rule was matched.	informational
wsaNodeStatusIntegrated	24	A node was integrated.	informational
wsaNodeStatusNotavail	25	A node is not available.	critical
wsaNodeStatusNotrunning	26	A node is not running.	critical
wsaRAIDControllerDefect	102	Defect on RAID controller has occurred.	critical
wsaRAIDDiskDefect	103	Defect on RAID disk has occurred.	critical
wsaStorageHardwareDefectSet	304	Defect on storage hardware has occurred.	critical
wsaStorageHardwareErrorSet	305	Error on storage hardware has occurred.	critical
wsaStorageRepair	306	Storage component was repaired.	minor

Table 36: WSA-TRAP-MIB traps

5.3.14 PXRE traps (dec.mib)

MIB-OID: 1.3.6.1.4.1.36.2.15.21

This section lists PXRE traps in alphabetical order.

Trap name	ID	Meaning	Error class
cacheBatteryFailureTrap	7	A controller cache battery has failed. Replace cache battery or replenish charge.	major
cacheBattery InformationTrap	9	A controller cache battery has *GOOD* state.	informational
cacheBatteryLowTrap	8	A controller cache battery has *LOW* state. Replace cache battery or replenish charge.	minor
communication FailureTrap	12	Communication with the subsystem has failed. The Possible causes are data path interruption, communication LUN failure, 2 or more power supplies failed, 2 or more fans failed, temperature over limit, both controllers failed.	critical
communicationInformationTrap	13	Communication with the subsystem has recovered.	informational
controllerFailureTrap	14	The Secondary Controller in the subsystem has failed. Replace controller. Possible causes are PCMCIA memory card ejected, controller physically removed, actual hardware failure.	major
controllerInformationTrap	15	The Secondary Controller in the subsystem has recovered.	informational

Table 37: PXRE traps

Trap name	ID	Meaning	Error class
diskFailureTrap	1	A disk drive has failed. The location of the disk is indicated by the disk name. Replace the disk device. The numbers in the name indicate Port, Target, Lun behind the controller pair. Examples: – DISK10100 is disk location Port 1, Target 01, Lun 00. – DISK30300 is disk location Port 3, Target 03, Lun 00.	major
diskInformationTrap	2	A disk drive has recovered. The location of the disk is indicated by the disk name. The numbers in the name indicate Port, Target, Lun behind the controller pair. Examples: – DISK10100 is disk location Port 1, Target 01, Lun 00. – DISK30300 is disk location Port 3, Target 03, Lun 00.	informational
externalInputFailureTrap	20	The user-defined External Input to the EMU indicates a failure. If the state of the is *FAILURE*, then one of the user-defined external input devices is reporting a problem.	major
externalInput InformationTrap	21	The user-defined External Input to the EMU indicates a recovery.	informational

Table 37: PXRE traps

Trap name	ID	Meaning	Error class
fanFailureTrap	5	The fan in the specified location has failed. Replace fan.	major
fanInformationTrap	6	The fan in the specified location was recovered.	informational
lunFailureTrap	16	The LUN has failed and is off-line. Possible cause is too many failed disk drives that make up the LUN, the OS can no longer communicate with the LUN for other reasons.	critical
lunInformationTrap	19	A LUN has become optimal due to successful completion of the reconstruction process.	informational
lunReconstructTrap	17	The LUN has started the reconstruction process but is available for normal use. Possible causes are an available disk drive was created as a spare to be inserted into the set, an existing spare was automatically added to the set for reconstruction upon failure of a member disk device.	minor
lunReducedTrap	18	A LUN has become degraded due to a member disk device failure. Replace the failed disk device; add a spare to the system to cause a reconstruct.	major

Table 37: PXRE traps

Trap name	ID	Meaning	Error class
powerSupplyFailureTrap	3	The power supply in the specified location has failed. Replace power supply.	major
powerSupply InformationTrap	4	Power supply was recovered.	informational
temperature InformationTrap	11	A temperature sensor indicates temperature below *WARNING* threshold limit.	informational
temperatureOver ThresholdTrap	10	A temperature sensor has exceeded *WARNING* threshold limit. Lower environmental temperature or raise internal threshold limit depending upon application.	major

Table 37: PXRE traps

5.3.15 RAID Adapter traps (Megaraid.mib)

MIB-OID: 1.3.6.1.4.1.16.1.1.200

This section lists RAID Adapter traps in alphabetical order.

Trap name	ID	Meaning	Error class
rtBatteryMissing	9020	Adapter-*%d*: Battery Module is missing.	informational
rtBattery TemperatureHigh	9022	Adapter-*%d*: Battery Module temperature exceeded Danger Threshold.	informational
rtBatteryVolatageLow	9021	Adapter-*%d*: Battery Module voltage is low.	informational
rtCheck ConditionStatus	9018	Adapter-*%d*, Channel-*%d*, Target-*%d*: Command completed with Sense_Key-*0x%x* ASC-*0x%x* ASCQ-*0x%x*.	informational
rtCheck ConsistencyAborted	9010	Adapter-*%d*, Logical Drive-*%d*: Check consistency aborted by user.	informational
rtCheck ConsistencyCompleted	9009	Adapter-*%d*, Logical Drive-*%d*: Check Consistency completed. No inconsistencies found.	informational
rtCheck ConsistencyFailed	9012	Adapter-*%d*, Logical Drive-%d: Check consistency failed.	informational
rtCheck ConsistencyStarted	9008	Adapter-*%d*, Logical Drive-*%d*: Check consistency started.	informational
rtConfigUpdated	9001	Adapter-*%d*: A new configuration has been written.	informational

Table 38: RAID Adapter traps

Trap name	ID	Meaning	Error class
rtConsistencyCorrected	9011	Adapter-*%d*, Logical Drive-*%d*: Check consistency operation completed. Inconsistencies have been cured.	informational
rtInitializeAborted	9006	Adapter-*%d*, Logical Drive-*%d*: Initialization aborted by user.	informational
rtInitializeCompleted	9005	Adapter-*%d*, Logical Drive-*%d*: Initialization completed successfully.	informational
rtInitializeFailed	9007	Adapter-*%d*, Logical Drive-*%d*: Initialization failed.	informational
rtInitializeStarted	9004	Adapter-*%d*, Logical Drive-*%d*: Initialization started.	informational
rtLogicalDriveStateChange	9003	Adapter-*%d*, Logical Drive-*%d*: State changed from *%s* to *%s.*	informational
rtNewDriveInserted	9019	Adapter-*%d*, Channel-*%d*, Target-*%d*: New device inserted.	informational
rtPhysicalDriveStateChange	9002	Adapter-*%d*, Channel-*%d*, Target-*%d*: Drive state changed from %s to *%s*.	informational
rtPredictiveFailuresExceeded	9016	Adapter-*%d*, Channel-*%d*, Target-*%d*: Reported predictive failure. Drive identification string = *%s* Sense Key = *0x%x*, ASC = *0x%x*, ASCQ = *0x%x*.	informational

Table 38: RAID Adapter traps

Trap name	ID	Meaning	Error class
rtPredictiveFailures False	9017	Adapter-*%d*, Channel-*%d*, Target-*%d*: Reported failure prediction threshold exceeded [*FALSE*]. Drive identification string = *%s* Sense Key = *0x%x*, ASC = *0x%x*, ASCQ = *0x%x*.	informational
rtReconstruction Completed	9014	Adapter-*%d*, Logical Drive-*%d*: Reconstruction completed successfully.	informational
rtReconstructionFailed	9015	Adapter-*%d*, Logical Drive-*%d*: Reconstruction failed.	informational
rtReconstruction Started	9013	Adapter-*%d*, Logical Drive-*%d*: Reconstruction started.	informational

Table 38: RAID Adapter traps

5.3.16 RomPilot traps (Rompilot.mib)

MIB-OID: 1.3.6.1.4.1.2487

This section lists RomPilot traps in alphabetical order.

Trap name	ID	Meaning	Error class
RomPilotColdReset	258	Phoenix RomPilot was loaded after a cold system reset.	informational
RomPilot DiagnosticReset	259	Phoenix RomPilot was loaded after a diagnostic system reset.	informational
RomPilotFatalError	769	Phoenix RomPilot detected a fatal error.	informational
RomPilotGenericBoot	512	Phoenix RomPilot announces a generic boot (about to load OS).	informational
RomPilotIDEBootReset	260	Phoenix RomPilot was loaded after an IDE Boot system reset.	informational
RomPilotOSStarted	1280	Phoenix RomPilot announces, that the OS has been started.	informational
RomPilot PostWarningError	771	Phoenix RomPilot detected a post warning error.	informational
RomPilotPressF1	770	Phoenix RomPilot is running and needs a F1 key press to continue.	informational
RomPilot UnspecifiedReset	256	Phoenix RomPilot was loaded after an unspecified system reset (assume cold reset).	informational
RomPilotWarmReset	257	Phoenix RomPilot was loaded after a warm system reset.	informational

Table 39: ROMPilot traps

5.3.17 ServerControl traps (SC.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists ServerControl traps in alphabetical order.

Trap name	ID	Meaning	Error class
cabinetNotConfigured	623	Cabinet is not configured.	informational
cabinetSwitchedOff	617	Cabinet was switched off.	informational
cabinetSwitchedOn	618	Cabinet was switched on.	informational
correctableMemError	643	Correctable memory error.	minor
correctableMemError Addr	637	Correctable memory error at *address*.	minor
correctableMemError Bank	639	Correctable memory error in *bank*.	minor
correctableMemError Module	641	Correctable memory error in *module*.	minor
fanCriticalError	622	A fan is critical and will fail soon.	informational
fanError	601	Fan failed.	critical
fanOk	629	Fan is OK.	informational
frontDoorStatusChanged	646	Status of front door changed.	informational
housingOpenStatus Changed	647	Status of housing changed.	informational
internalError	620	Internal error in server management controller software.	informational
memErrorModuleFailing	669	A memory module is failing.	major
memErrorModule Prefailure	668	A memory module is predicted to fail (prefailure).	major
memErrorModule Replaced	670	A memory module had failed and was replaced by a hot-spare module.	major

Table 40: ServerControl traps (SC.mib)

Trap name	ID	Meaning	Error class
notEnoughCabinets	615	The actual number of storage extensions is lower than number stored in the configuration.	major
powerOffTimeReached	645	Power off time has been reached.	informational
powerSupplyAdded	625	A power supply was added.	informational
powerSupplyFailed	626	A power supply has failed.	major
powerSupplyOk	627	The power supply is working again.	informational
powerSupplyRemoved	624	The power supply has been removed.	informational
powerSupplyStatus Critical	628	Not enough power supplies are operating.	critical
scbBBUNotdetected	614	A BBU is configured but no BBU was detected.	informational
scbUnconfiguredBBU Detected	613	A BBU is detected but no BBU was configured.	informational
scbUnconfiguredUPS Detected	611	A UPS is detected but no UPS was configured.	informational
scbUPSNotdetected	612	A UPS is configured but no UPS was detected.	major
selftestError	609	The server management controller has failed.	critical
selftestWarning	608	The server management controller has detected a minor problem during its self-test.	minor
serverManagement Disabled	631	Server Management BIOS is disabled.	informational
serverShutdown	621	Server has been shut down.	informational
sieScBootCountZero	666	Boot retry counter gets zero on power up.	major

Table 40: ServerControl traps (SC.mib)

Trap name	ID	Meaning	Error class
sieScBootError	661	No bootable operating system can be found.	informational
sieScBootWatchdogExpired	662	Boot watchdog expires.	informational
sieScCpuPrefailure	673	A CPU is predicted to fail (prefailure).	major
sieScDiagnosticBoot	665	Server is reset and diagnostic boot is enabled.	informational
sieScMessageLogFull	667	System Event Log is full. No more message can be logged. Trap will not occur on wrap-around log types.	minor
sieScMessageLog Warning	672	The warning threshold for the number of System Event Log entries has been exceeded.	minor
sieScNoBootCpu	658	The system boot fails, because no valid boot CPU has been found.	informational
sieScPostError	659	System boot fails, because the power on self test (POST) has reported an error.	informational
sieScPowerFail	674	DC power failed in the specified cabinet. System may stop when this condition occurs.	critical
sieScPowerOn	657	A server is powered on.	informational
sieScSetupEntered	660	BIOS setup has been entered.	informational
sieScSoftwareWatchdog Expired	663	Software watchdog expires.	informational

Table 40: ServerControl traps (SC.mib)

Trap name	ID	Meaning	Error class
sieScUserAuthenticationFailure	664	User authentication failure is detected via PPP, FTP, HTTP or telnet.	major
sniScCpuSpeedChanged	656	CPU speed has changed because of temperature problems.	informational
sniScFanAdded	653	The indicated hot-plug fan was inserted.	informational
sniScFanRemoved	654	The indicated hot-plug fan was removed.	informational
sniScPowerSupplyRedundancyLost	671	Power supply redundancy no longer available.	minor
sniScRedundantFanFailed	648	The indicated redundant fan failed.	major
sniScRedundantPowerSupplyFailed	649	One redundant hot-replace power supply failed.	major
sniScShutdownCancelled	655	A pending server shutdown was canceled by the user.	informational
sniScVoltageOk	650	Power supply voltage is within normal range again.	informational
sniScVoltageTooHigh	652	Power supply voltage is too high.	critical
sniScVoltageTooLow	651	Power supply voltage is too low.	critical
svCommunicationEstablished	636	Communication with the server management controller was established.	informational
svCommunicationFailure	610	Communication with the server management controller was interrupted.	critical
tempCritical	604	The temperature has reached a critical level.	critical
tempOk	602	The temperature is within normal range.	informational

Table 40: ServerControl traps (SC.mib)

Trap name	ID	Meaning	Error class
tempSensorBroken	630	The temperature sensor is defective or not connected.	major
tempSensorOk	635	The temperature sensor is working again.	informational
tempWarn	603	The temperature has reached the warning level.	major
testTrap	600	Test trap sent to verify trap connection.	informational
tooManyCabinets	616	The actual number of storage subsystems is higher than the number stored in the configuration.	minor
trapAcFail	632	AC power has failed.	critical
trapDuplicateCabinetId	633	Two or more cabinets (server or storage subsystems) have the same ID number.	major
trapEventLog	634	An error was recorded. See the server management event / error log (recovery) for detailed information. This could have happened when an error occurred before the agent was running or any error without a specific trap.	major

Table 40: ServerControl traps (SC.mib)

Trap name	ID	Meaning	Error class
trapOnBattery	606	AC power failure. Cabinet is running on battery power. The UPS is operating on battery power or the power supply is drawing current from the backup battery unit (BBU). This trap is persistent and is resent at one minute intervals until the mains returns or the system is switched off.	critical
trapOnMains	607	AC power OK.	informational
uncorrectableMemError	644	Uncorrectable memory error.	critical
uncorrectableMemErrorAddr	638	Uncorrectable memory error at *address*.	critical
uncorrectableMemErrorBank	640	Uncorrectable memory error in *bank*.	critical
uncorrectableMemErrorModule	642	Uncorrectable memory error in *module*.	critical

Table 40: ServerControl traps (SC.mib)

5.3.18 ServerControl traps (SC2.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2.2.10.20

This section lists ServerControl traps in alphabetical order.

Trap name	ID	Meaning	Error class
sc2TrapAcFail	2040	Mains failed in the specified cabinet. This trap occurs only in storage extension cabinets without UPS or BBU. A server has no time to send this trap.	critical
sc2TrapBatteryVoltage Prefail	2054	Battery is predicted to fail.	major
sc2TrapBiosSelftest Error	2005	A critical error occurs while BIOS selftest. Take notice of this error to clear the error condition.	critical
sc2TrapBootMessage LogEntry	2102	An error message was written into the systemboard's message log. This could have happened when an error occurred before the server management agents were running or any error without a specific trap. See server management message log for detailed error description.	major
sc2TrapBootRetryCount Zero	2095	This trap will be sent when a boot retry counter gets zero on power up.	major

Table 41: ServerControl traps (SC2.mib)

Trap name	ID	Meaning	Error class
sc2TrapCabinetSwitchedOff	2090	This trap will be sent when a cabinet is switched off. For obvious reasons it cannot be sent when the main cabinet is switched off.	informational
sc2TrapCabinetSwitchedOn	2091	This trap will be sent when a cabinet is switched on.	informational
sc2TrapCommunicationEstablished	2002	The communication with the management controller was reestablished.	informational
sc2TrapCommunicationFailure	2001	The communication with management controller failed.	minor
sc2TrapControllerSelftestError	2004	Controller selftest error.	critical
sc2TrapControllerSelftestWarning	2003	Controller selftest warning.	minor
sc2TrapCorrectableMemErrorAddr	2060	A correctable memory error at specified address was detected.	informational
sc2TrapCorrectableMemErrorBank	2062	A correctable memory error at specified bank was detected.	informational
sc2TrapCorrectableMemErrorModule	2064	A correctable memory error at specified module was detected.	informational
sc2TrapCorrectableMemError	2066	A correctable memory error at unknown location was detected.	informational
sc2TrapCpuPrefail	2081	A CPU is predicted to fail (prefailure).	major
sc2TrapCpuSpeedChanged	2080	This trap will be sent if the CPU clock frequency was changed because of a temperature problem.	informational

Table 41: ServerControl traps (SC2.mib)

Trap name	ID	Meaning	Error class
sc2TrapDcFail	2041	DC power failed in the specified cabinet. This is the result of the systems power-good sensor monitoring. The system stops if this error occurs.	critical
sc2TrapFanAdded	2010	The indicated hot-plug fan was inserted.	informational
sc2TrapFanCritical	2013	The indicated fan became critical.	major
sc2TrapFanFailed	2014	The indicated fan failed.	critical
sc2TrapFanOk	2012	The indicated fan is OK again.	informational
sc2TrapFanRemoved	2011	The indicated hot-plug fan was removed.	informational
sc2TrapIntrusionAssertion	2110	The front door or housing was opened.	major
sc2TrapIntrusionChanged	2112	The front door or housing was opened or closed.	major
sc2TrapIntrusionDeassertion	2111	The front door or housing was closed.	informational
sc2TrapMemErrorModuleFailing	2069	A memory module failed.	major
sc2TrapMemErrorModulePrefail	2068	A memory module is predicted to fail (prefailure).	major
sc2TrapMemErrorModuleReplaced	2070	A memory module failed and was replaced by a hot-spare module.	major

Table 41: ServerControl traps (SC2.mib)

Trap name	ID	Meaning	Error class
sc2TrapMessageLogFull	2100	The System Event Log (message log) is full. No more messages can be logged. This trap will not occur on wrap-around log types.	minor
sc2TrapMessageLogWarning	2101	The warning threshold for the number of System Event Log entries has been exceeded.	minor
sc2TrapOnBattery	2042	The UPS is operating on battery power or the power supply is drawing current from the backup battery unit (BBU). This trap is persistent and is resent at one minute intervals until the mains returns or the system is switched off.	critical
sc2TrapOnMains	2043	The mains voltage returned after a power failure.	informational
sc2TrapPowerOffTimeReached	2092	Power off time reached.	informational
sc2TrapPowerSupplyAdded	2030	One hot-replace power supply was added.	informational
sc2TrapPowerSupplyCritical	2033	Power supply status became critical.	critical
sc2TrapPowerSupplyFailed	2034	One hot-replace power supply failed.	major
sc2TrapPowerSupplyOk	2032	Power supply is working again.	informational
sc2TrapPowerSupplyRedundancyLost	2036	Power supply redundancy id no longer available.	minor
sc2TrapPowerSupplyRemoved	2031	One hot-replace power supply was removed.	informational

Table 41: ServerControl traps (SC2.mib)

Trap name	ID	Meaning	Error class
sc2TrapRedundantFanFailed	2015	The indicated redundant fan failed.	major
sc2TrapRedundantPowerSupplyFailed	2035	One redundant hot-replace power supply failed.	major
sc2TrapServerShutdown	2093	This trap will be sent before a server will switch off.	informational
sc2TrapSevereSystemError	2006	The system was restarted after a severe problem. See server management message log (recovery log) for detailed information.	critical
sc2TrapShutdownCancelled	2094	This trap will be sent if a pending server shutdown was canceled by the user.	informational
sc2TrapTempCritical	2022	The temperature of the indicated sensor is out of tolerance range. The system will shut down and power off if shutdown is enabled.	critical
sc2TrapTempOk	2020	The temperature of the indicated sensor has decreased to the normal level.	informational
sc2TrapTempSensorOk	2023	The indicated broken temperature sensor is OK again.	informational
sc2TrapTempSensorBroken	2024	The indicated temperature sensor is broken.	major
sc2TrapTempWarning	2021	The temperature of the indicated sensor has reached the warning level.	major
sc2TrapTest	2000	Test trap to verify trap connection.	informational

Table 41: ServerControl traps (SC2.mib)

Trap name	ID	Meaning	Error class
sc2TrapUncorrectableMemError	2067	A uncorrectable memory error at unknown location was detected.	critical
sc2TrapUncorrectableMemErrorAddr	2061	An uncorrectable memory error at specified address was detected.	critical
sc2TrapUncorrectableMemErrorBank	2063	An uncorrectable memory error at specified bank was detected.	critical
sc2TrapUncorrectableMemErrorModule	2065	A correctable memory error at specified module was detected.	critical
sc2TrapVoltageOk	2050	Power supply voltage is within normal range again.	informational
sc2TrapVoltageFailed	2053	Power supply voltage is out of range.	critical
sc2TrapVoltageTooHigh	2052	Power supply voltage is too high.	critical
sc2TrapVoltageTooLow	2051	Power supply voltage is too low.	critical
sc2TrapDrvMonEventMessage	2150	Driver Monitoring detected an informational event.	informational
sc2TrapDrvMonEventWarning	2151	Driver Monitoring detected a warning event.	minor
sc2TrapDrvMonEventError	2152	Driver Monitoring detected an error event.	major

Table 41: ServerControl traps (SC2.mib)

5.3.19 ServerView traps (ServerView.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists ServerView traps in alphabetical order.

Trap name	ID	Meaning	Error class
sniSvGenericTrap Forward	700	A ServerView alarm signal has been received.	informational
sniSvPagerOff	701	The pager should be switched off.	informational
sniSvPassThrough TrapForward	703	Forwarded if the Event Manager receives a trap to be forwarded. The original server name and severity is retained.	informational
sniSvServerState Changed	702	Generated by Operations Manager if server changes state (manageable/not manageable).	informational

Table 42: ServerView traps

5.3.20 ServerView status traps (Status.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

This section lists ServerView status traps in alphabetical order.

Trap name	ID	Meaning	Error class
sieStTrapStatusChanged	1100	System status has changed at server.	informational

Table 43: ServerView status trap

5.3.21 Tape drive traps (tapealrt.mib)

MIB-OID: 1.3.6.1.4.1.11.2.3.9.7.1

This section lists tape drive traps in alphabetical order.

Trap name	ID	Meaning	Error class
tapeAlertTrap1	1	The tape drive is having problems reading data. No data has been lost, but there has been a reduction in the performance of the tape.	minor
tapeAlertTrap2	2	The tape drive is having problems writing data. No data has been lost, but there has been a reduction in the capacity of the tape.	minor
tapeAlertTrap3	3	The operation has stopped because an error has occurred while reading or writing data which the drive cannot correct.	minor
tapeAlertTrap4	4	Your data is at risk: 1. Copy any data you require from this tape. 2. Do not use this tape again. 3. Restart the operation with a different tape.	critical
tapeAlertTrap5	5	The tape is damaged or the drive is faulty. Call the tape drive supplier helpline.	critical

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap6	6	The tape is from a faulty batch or the tape drive is faulty: 1. Use a good tape to test the drive. 2. If the problem persists, call the tape drive supplier helpline.	critical
tapeAlertTrap7	7	The tape cartridge has reached the end of its calculated useful life: 1. Copy any data you need to another tape 2. Discard the old tape.	minor
tapeAlertTrap8	8	The tape cartridge is not data-grade. Any data you back up to the tape is at risk. Replace the cartridge with a data-grade tape.	minor
tapeAlertTrap9	9	You are trying to write to a write-protected cartridge. Remove the write-protection or use another tape.	critical
tapeAlertTrap10	10	You cannot eject the cartridge because the tape drive is in use. Wait until the operation is complete before ejecting the cartridge.	informational
tapeAlertTrap11	11	The tape in the drive is a cleaning cartridge. If you want to back up or restore, insert a data-grade tape.	informational

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap12	12	You have tried to load a cartridge of a type which is not supported by this drive.	informational
tapeAlertTrap13	13	The operation has failed because the tape in the drive has snapped: 1. Discard the old tape. 2. Restart the operation with a different tape.	critical
tapeAlertTrap14	14	The operation has failed because the tape in the drive has snapped: 1. Do not attempt to extract the tape cartridge. 2. Call the tape drive supplier helpline.	critical
tapeAlertTrap15	15	The memory in the tape cartridge has failed, which reduces performance. Do not use the cartridge for further backup operations.	minor
tapeAlertTrap16	16	The operation has failed because the tape cartridge was manually ejected while the tape drive was actively writing or reading.	critical
tapeAlertTrap17	17	You have loaded a cartridge of a type that is read-only in this drive. The cartridge will appear as write-protected.	minor
tapeAlertTrap18	18	The directory on the tape cartridge has been corrupted. File search performance will be degraded.	minor

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap19	19	The tape cartridge is nearing the end of its useful life. It is recommended that you: 1. Use another tape cartridge for your next backup. 2. Store this tape cartridge in a safe place in case you need to restore data from it.	informational
tapeAlertTrap20	20	The tape drive needs cleaning: 1. If the operation has stopped, eject the tape and clean the drive. 2. If the operation has not stopped, wait for it to finish and then clean the drive.	critical
tapeAlertTrap21	21	The tape drive is due for routine cleaning: 1. Wait for the current operation to finish. 2. Then use a cleaning cartridge.	minor
tapeAlertTrap22	22	The last cleaning cartridge used in the tape drive has worn out: 1. Discard the worn out cleaning cartridge. 2. Wait for the current operation to finish. 3. Then use a new cleaning cartridge.	critical

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap23	23	The last cleaning cartridge used in the tape drive was an invalid type: 1. Do not use this cleaning cartridge in this drive. 2. Wait for the current operation to finish. 3. Then use a valid cleaning cartridge.	critical
tapeAlertTrap29	29	Preventive maintenance of the tape drive is required. Check the tape drive users manual for device specific preventive maintenance tasks or call the tape drive supplier helpline.	minor
tapeAlertTrap30	30	The tape drive has a hardware fault: 1. Eject the tape or magazine. 2. Reset the drive. 3. Restart the operation.	critical
tapeAlertTrap31	31	The tape drive has a hardware fault: 1. Turn the tape drive off and then on again. 2. Restart the operation. 3. If the problem persists, call the tape drive supplier helpline.	critical

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap32	32	The tape drive has a problem with the host interface: 1. Check the cables and cable connections. 2. Restart the operation.	minor
tapeAlertTrap33	33	The operation has failed: 1. Eject the tape or magazine. 2. Insert the tape or magazine again. 3. Restart the operation.	critical
tapeAlertTrap34	34	The firmware download has failed because you have tried to use the incorrect firmware for this tape drive. Obtain the correct firmware and try again.	minor
tapeAlertTrap35	35	Environmental conditions inside the tape drive are exceeding the humidity specifications.	minor
tapeAlertTrap36	36	Environmental conditions inside the tape drive are exceeding the temperature specifications.	minor
tapeAlertTrap37	37	The voltage supply to the tape drive exceeds specifications.	minor
tapeAlertTrap38	38	A hardware failure of the tape drive is predicted. Call the tape drive supplier helpline.	critical

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap39	39	The tape drive may have a hardware fault. Run extended diagnostics to verify and diagnose the problem. Check the tape drive users manual for device specific instructions on running extended diagnostic tests.	minor
tapeAlertTrap40	40	The changer mechanism is having difficulty communicating with the tape drive: 1. Turn the autoloader off then on. 2. Restart the operation. 3. If problem persists, call the tape drive supplier helpline.	critical
tapeAlertTrap41	41	A tape has been left in the autoloader by a previous hardware fault: 1. Insert an empty magazine to clear the fault. 2. If the fault does not clear, turn the autoloader off and then on again. 3. If the problem persists, call the tape drive supplier helpline.	critical
tapeAlertTrap42	42	There is a problem with the autoloader mechanism.	minor

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap43	43	The operation has failed because the autoloader door is open: 1. Clear any obstructions from the autoloader door. 2. Eject the magazine and then insert it again. 3. If the fault does not clear, turn the autoloader off and then on again. 4. If the problem persists, call the tape drive supplier helpline.	critical
tapeAlertTrap44	44	The autoloader has a hardware fault: 1. Turn the autoloader off and then on again. 2. Restart the operation. 3. If the problem persists, call the tape drive supplier helpline.	critical
tapeAlertTrap45	45	The autoloader cannot operate without the magazine. 1. Insert the magazine into the autoloader. 2. Restart the operation.	critical
tapeAlertTrap46	46	A hardware failure of the changer mechanism is predicted. Call the tape drive supplier helpline.	minor

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap256	256	The library mechanism is having difficulty communicating with the drive: 1. Turn the library off then on. 2. Restart the operation. 3. If problem persists, call the library supplier helpline.	critical
tapeAlertTrap257	257	There is a problem with the library mechanism. If problem persists, call the library supplier helpline.	minor
tapeAlertTrap258	258	The library has a hardware fault: 1. Reset the library. 2. Restart the operation. Check the library users manual for device specific instructions on resetting the device.	critical
tapeAlertTrap259	259	The library has a hardware fault: 1. Turn the library off and then on again. 2. Restart the operation. 3. If the problem persists, call the library supplier helpline. Check the library users manual for device specific instructions on turning the device power on and off.	critical

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap260	260	The library mechanism may have a hardware fault. Run extended diagnostics to verify and diagnose the problem. Check the library users manual for device specific instructions on running extended diagnostic tests.	minor
tapeAlertTrap261	261	The library has a problem with the host interface: 1. Check the cables and cable connections. 2. Restart the operation.	critical
tapeAlertTrap262	262	A hardware failure of the library is predicted. Call the library supplier helpline.	minor
tapeAlertTrap263	263	Preventative maintenance of the library is required. Check the library users manual for device specific preventative maintenance tasks, or call your library supplier helpline.	minor
tapeAlertTrap264	264	General environmental conditions inside the library have exceeded the humidity specifications.	critical
tapeAlertTrap265	265	General environmental conditions inside the library have exceeded the temperature specifications.	critical

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap266	266	The voltage supply to the library exceeds specifications. There is a potential problem with the power supply or failure of a redundant power supply.	critical
tapeAlertTrap267	267	A cartridge has been left in a drive inside the library by a previous hardware fault: 1. Insert an empty magazine to clear the fault. 2. If the fault does not clear, turn the library off and then on again. 3. If the problem persists, call the library supplier helpline.	critical
tapeAlertTrap268	268	There is a potential problem with a drive ejecting cartridges short or with the library mechanism picking a cartridge from a slot. If the problem persists, call the library supplier helpline.	minor
tapeAlertTrap269	269	There is a potential problem with the library mechanism placing a cartridge into a slot. If the problem persists, call the library supplier helpline.	minor
tapeAlertTrap270	270	There is a potential problem with a drive or the library mechanism loading cartridges, or an incompatible cartridge.	minor

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap271	271	The operation has failed because the library door is open: 1. Clear any obstructions from the library door. 2. Close the library door. 3. If the problem persists, call the library supplier helpline.	critical
tapeAlertTrap272	272	There is a mechanical problem with the library media import/export mailslot.	critical
tapeAlertTrap273	273	The library cannot operate without the magazine. 1. Insert the magazine into the library. 2. Restart the operation.	critical
tapeAlertTrap274	274	Library security has been compromised.	minor
tapeAlertTrap275	275	The security mode of the library has been changed. The library has either been put into secure mode, or the library has exited the secure mode.	informational
tapeAlertTrap276	276	The library has been manually turned offline and is unavailable for use.	informational
tapeAlertTrap277	277	A drive inside the library has been taken offline.	informational

Table 44: Tape traps

Trap name	ID	Meaning	Error class
tapeAlertTrap278	278	There is a potential problem with the barcode label or the scanner hardware in the library mechanism. If the problem persists, call the library supplier helpline.	minor
tapeAlertTrap279	279	The library has detected a inconsistency in its inventory. 1. Redo the library inventory to correct inconsistency. 2. Restart the operation Check the applications users manual or the hardware users manual for specific instructions on redoing the library inventory.	critical
tapeAlertTrap280	280	A library operation has been attempted that is invalid at this time.	minor

Table 44: Tape traps

5.3.22 Team Server traps (Fujitsu)

This section describes the traps supplied with the Fujitsu Team Server.

ASM PRIVATE COMMIB traps (Asmpro.mib)

MIB-OID: 1.3.6.1.4.1.3764.3

Trap name	ID	Meaning	Error class
trapACFail	13	AC Power failed.	major
trapAssetChange	23	Asset is changed.	major
trapBatteryFail	15	UPS battery fails.	major
trapBusUtilization	8	Percent bus utilization exceeds the threshold value.	major
trapBiosEventLog	20	BIOS has new event log.	major
trapBiosEventLog Utlization	21	BIOS event log utilization exceeds threshold.	major
trapChassisIntrusion	16	Chassis intrusion occurs.	major
trapCPUAbnormal	22	CPU has internal error.	major
trapCPUUtilization	7	Percent CPU utilization exceeds the threshold value.	major
trapECC1BitError	3	An EEC 1-bit error occurs.	major
trapECCMBitError	4	An EEC multi-bit error occurs.	critical
trapFanStop	5	Any fan stops functioning.	major
trapFuseFail	17	Fuse failed.	major
trapMemoryUtilization	9	Percent memory utilization exceeds the threshold value.	major
trapNICCounter	11	NIC statistical counter exceeds the threshold value.	major

Table 45: ASM PRIVATE MIB traps

Trap name	ID	Meaning	Error class
trapPowerFanFail	14	Any power subsystem fan fails.	major
trapPSFail	12	Any power supply fails.	major
trapRPSFail	18	Redundant power supply is failed.	major
trapRPSFanFail	19	Redundant power supply fan is failed.	major
trapTemperatureCritical	2	Temperatures exceed the second level threshold value.	critical
trapVoltage	6	Any voltage reading exceeds the save operating range.	major
trapVolumeUtilization	10	Percent volume utilization exceeds the threshold value.	major

Table 45: ASM PRIVATE MIB traps

LDCM MIB traps (Ldcm.mib)

MIB-OID: 1.3.6.1.4.1.343.2.5.1.2

Trap name	ID	Meaning	Error class
ldcmCriticalTrap	5	Manager has reported a severity Critical event.	critical
ldcmFatalTrap	6	Manager has reported a severity Fatal event.	critical
ldcmInfoTrap	2	Manager has reported an Informational event.	informational
ldcmOkTrap	3	Manager has reported a severity OK event.	informational
ldcmUnknownTrap	1	Manager has reported an Unknown event.	informational
ldcmWarningTrap	4	Manager has reported a severity Warning event.	minor

Table 46: LDCM MIB traps

LDSM MIB traps (Ldsm.mib

MIB-OID: 1.3.6.1.4.1.343.2.5.1.3

Trap name	ID	Meaning	Error class
ldsmCriticalTrap	4	Manager has reported a “critical” error class event.	critical
ldsmInformationalTrap	2	Manager has reported an “informational” error class event.	informational
ldsmOkTrap	1	Manager has reported an “OK” error class event.	informational
ldsmWarningTrap	3	Manager has reported a “warning” error class event.	minor

Table 47: LDSM MIB traps

5.3.23 Threshold traps (Trap.mib)

MIB-OID: 1.3.6.1.4.1.231

This section lists threshold traps in alphabetical order.

Trap name	ID	Meaning	Error class
sniInvDeltaTrap Underflow	131	DELTA threshold underflow. This trap indicates, that one of the polled variables has left the interval specified by the user. The variable will be given in the sniInvPollAlarm field.	informational
sniInvPollDeltaExceed	130	DELTA threshold exceeded. This trap indicates, that one of the polled variables has left the interval specified by the user. The variable will be given in the sniInvPollAlarm field.	informational
sniInvPollTrapExceed	128	Threshold exceeded. This trap indicates, that one of the polled variables has left the interval specified by the user. The variable will be given in the sniInvPollAlarm field.	informational
sniInvPollTrapUnderflow	129	Threshold underflow. This trap indicates, that one of the polled variables has left the interval specified by the user. The variable will be given in the sniInvPollAlarm field.	informational
sniInvTrapInvalid	132	Threshold has become invalid.	informational

Table 48: Threshold traps

Trap name	ID	Meaning	Error class
sniInvTrapValid	133	Threshold has become valid.	informational
sniNTAlert	304	NT alert message was written to the event log.	informational
sniNTChangeSecurity	302	Security change has occurred.	informational
sniNTChangeTime	305	Time has changed or a nonuniform time adjustment has occurred.	informational
sniNTDownServer	300	Server is going down.	informational
sniNTEventLogError	330	Error entry was written to event log.	informational
sniNTEventLogFailure	334	Failure audit entry was written to event log.	informational
sniNTEventLog Information	332	Information entry was written to event log.	informational
sniNTEventLogSuccess	333	Success audit entry was written to event log.	informational
sniNTEventLogWarning	331	Warning entry was written to event log.	informational
sniNTFileChangeAttr	322	File or directory attributes have been changed.	informational
sniNTFileChange DirName	321	Directory name has been changed, created or deleted.	informational
sniNTFileChangeLast Write	324	Last write time on a file has been changed.	informational
sniNTFileChangeName	320	File name has been changed, created or deleted.	informational
sniNTFileChange Security	325	Security on a file has been changed.	informational
sniNTFileChangeSize	323	File size has been changed.	informational

Table 48: Threshold traps

Trap name	ID	Meaning	Error class
sniNTLoginUser	301	User logged into server.	informational
sniNTRegChangeAttr	311	Attributes for a key or its subtree in registry has been changed.	informational
sniNTRegChangeLast Write	312	Last write time for a key or its subtree in registry has been changed.	informational
sniNTRegChangeName	310	Keyname in registry has been changed.	informational
sniNTRegChange Security	313	Security for a key or its subtree in registry has been changed.	informational
sniNTTrusteeChange	303	Trustee is changed on server.	informational
sniNWActivateScreen	014	Screen is activated on server.	informational
sniNWAlert	044	Netware alert message is written to the console.	informational
sniNWAllocate Connection	037	A connection is allocated.	informational
sniNWChangeSecurity	013	Security change has occurred on server.	informational
sniNWChangeTime	051	Nonuniform time adjustment has occurred.	informational
sniNWClearConnection	009	Connection is cleared.	informational
sniNWCloseFile	050	File is closed.	informational
sniNWCloseScreen	021	Screen is closed on server.	informational
sniNWCreateBinderyObj	011	Bindery object was created (NetWare).	informational
sniNWCreateObject	046	Directory Service (NetWare) object was created.	informational
sniNWCreateProcess	028	Process was created.	informational

Table 48: Threshold traps

Trap name	ID	Meaning	Error class
sniNWDataMigration	041	A files data has been migrated.	informational
sniNWDataDeMigration	042	Migration of file has been withdrawn.	informational
sniNWDeactivateScreen	018	Screen is deactivated on server.	informational
sniNWDeleteBinderyObj	012	Bindery object was deleted (NetWare).	informational
sniNWDeleteObject	047	Directory Service (NetWare) object was deleted.	informational
sniNWDestroyProcess	029	Process was destroyed.	informational
sniNWDownServer	004	Server is going down.	critical
sniNWExitToDos	007	Server exits to DOS.	critical
sniNWKeyWasPressed	017	Key was pressed on server.	informational
sniNWLoginUser	010	User logged into server.	informational
sniNWLogoutConnection	038	User has logged out.	informational
sniNWMLIDDeRegister	040	Multiple Link Interface Driver (MLID) was checked out on server.	informational
sniNWMLIDRegister	039	Multiple Link Interface Driver (MLID) was registered on server.	informational
sniNWModifyDirEntry	022	Directory entry was changed on server.	informational
sniNWModule Loaded	027	Module (e.g. NLM) was loaded.	informational
sniNWModuleUnloaded	009	Module (e.g. NLM) was unloaded.	informational
sniNWNewPublic	032	New public symbol was registered.	informational

Table 48: Threshold traps

Trap name	ID	Meaning	Error class
sniNWNoRelinquish Control	023	NLM-Module has not relinquished control.	critical
sniNWOpenScreen	020	Screen was opened on server.	informational
sniNWProtocolBind	033	A Protocol is bound to a MLID.	informational
sniNWProtocolUnbind	034	A Protocol is unbound from a MLID.	warning
sniNWQueueAction	043	A queue was activated, deactivated, created or deleted.	informational
sniNWRenameObject	048	Directory Service (NetWare) object was renamed.	informational
sniNWSysVolume Dismounted	001	SYS volume was dismounted on server.	critical
sniNWThreadSwitch	025	Thread Switch occurs.	informational
sniNWTrusteeChange	019	Trustee was changed on server.	informational
sniNWUpdateCursor	016	Cursor position was updated.	informational
sniNWUpdateScreen	015	Screen was updated on server.	informational
sniNWValueChanged	049	Value was changed for Directory Service (NetWare) object.	informational
sniNWVolSysMounted	000	SYS volume was mounted.	informational
sniNWVolume Dismounted	003	Volume was dismounted on server.	informational
sniNWVolumeMounted	002	Volume was mounted.	informational

Table 48: Threshold traps

5.3.24 UPS traps (Upsman.mib)

MIB-OID: 1.3.6.1.4.1.1356

This section lists UPS traps in alphabetical order.

UPS traps 1

Trap name	ID	Meaning	Error class
communication Established	4	The connection with the UPS was established.	informational
communicationLost	1	The connection with the UPS was lost.	critical
powerRestored	5	Normal power has been restored to the UPS.	informational
testCompleted	8	The UPS test was completed.	informational
testStarted	7	The UPS test was started.	informational
upsOnBattery	6	The UPS has switched to the battery supply.	major
upsOverload	2	The UPS detected a load exceeding 100% of its capacity.	critical
upsTurnedOff	3	The UPS was turned off by the manager.	major

Table 49: UPS traps 1

UPS traps 2

Trap name	ID	Meaning	Error class
boostOn	6	The UPS has turned on the booster.	major
communication Established	8	The connection with the UPS was established.	informational
communicationLost	1	The connection with the UPS was lost.	critical
lowBattery	7	The batteries are low and will soon be empty.	critical
powerRestored	9	Normal power has been restored to the UPS.	informational
returnFromLowBattery	11	The UPS has returned from the low battery state; the batteries are OK.	informational
upsDiagnosticsFailed	3	The UPS failed its internal diagnostics check.	critical
upsDiagnosticsPassed	10	The UPS has passed its internal diagnostics check.	informational
upsDischarged	4	The UPS has just discharged.	critical
upsOnBattery	5	The UPS has switched to the battery supply.	major
upsOverLoad	2	The UPS detected a load exceeding 100% of its capacity.	critical
upsRebootStarted	15	The UPS has started the reboot.	major
upsSleeping	13	The UPS has switched to sleep mode.	major
upsTurnedOff	12	The UPS was turned off by the manager.	major
upsWokeUp	14	The UPS has returned from sleep mode (woken up).	informational

Table 50: UPS traps 2

6 MIB integration

The Web-based *MIB Manager* tool is installed automatically when you install the Event Manager under Windows and Linux.

This tool is used to integrate private MIBs into the Event Manager, so that ServerView can detect the traps for this type of MIB. Then if an event occurs, ServerView can take the necessary action.

The following example shows the format for a description of TRAP-Type, where TRAP-Type must have the format SMIv1.

```
testTrap TRAP-TYPE
ENTERPRISE sniServerMgmt
VARIABLES {
trapServerName,
trapTime
}
DESCRIPTION
"Test trap to verify trap connection."
--#TYPE "Test trap"
--#SUMMARY "Test trap from server %s (no error)."
--#ARGUMENTS { 0 }
--#SEVERITY INFORMATIONAL
--#TIMEINDEX 1
--#HELP "Note: This is no error condition."
--#HELPTAG
--#STATE OPERATIONAL
::= 600
```

For the MIB file shown, only one enterprise string is supported.

Please note:

- The name extension of the MIB file must be *.mib*.
- You cannot remove integrated MIB files.
- MIB files which contain multi-byte characters are not supported.

Starting MIB Manager

The *MIB Manager* tool is started as follows:

▶ On the *EVENT MANAGEMENT* menu, select the *MIB INTEGRATOR* entry.

The tool starts up and the following window is displayed:

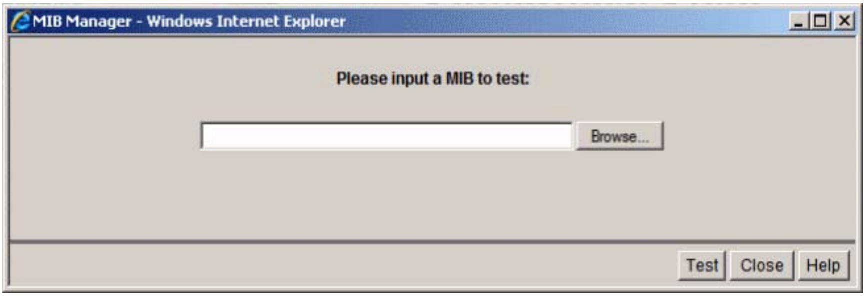

MIB Manager - Windows Internet Explorer
Please input a MIB to test:
Browse...
Test
Close
Help

Figure 17: “MIB Manager” tool

To integrate private MIBs, proceed as follows:

- ► Select the relevant directory using the *Browse...* button.
- ► Select the MIB and then click the *Upload* button. The tool then checks the MIB for correct syntax. In the next window a message shows the status.
- ► Click the *Save parsed MIB* button to integrate the MIB.
- ► In the next window, select *Close* to close the tool.

i After a third-party MIB has been integrated, the Java plug-in cache must be cleared. Under Windows the *ServerView Services* must be restarted. Under Linux it is sufficient just to restart the *SVForwardServer* with: `/etc/init.d/sv_fwdserver restart`.

Additional MIB integration under Linux

Beside the tool private MIBs can also be integrated under Linux operating systems as follows:

- ► Stop the *SVForwardServer* service:
  `/etc/init.d/sv_fwdserver stop`
- ► Copy the MIB to the directory
  `/opt/fujitsu/ServerViewSuite/web/cgi-bin/ServerView/common/mibs`.
- ► Then restart the *SVForwardServer* service:
  `/etc/init.d/sv_fwdserver start`

Viewing integrated MIB files

You can find out which MIBs are integrated in the Event Manager via the *Alarm Configuration* window (in the *MIB* column of the *Alarm Rules - Assign Alarms* dialog box) or via the Event Manager online help.

For a more detailed explanation of how to access the MIB overview window via help, see section "Displaying trap information" on page 83.

Updating integrated MIB files

You can update integrated MIB files. The name of the updated integrated MIB file must be the same as that of the integrated MIB file.

ℹ Please note that the MIB Integrator distinguishes between upper and lower case.