

Symantec NetBackup™ Deduplication Appliance SNMP Trap Reference Guide

Release 1.4.5

NetBackup 5020 and 5030



Symantec NetBackup™ Appliance SNMP Trap Reference Guide

Documentation version: 1.4.5

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, and NetBackup are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan customercare_apj@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

Contents

Technical Support	3	
Chapter 1	Overview	8
	About hardware monitoring and alerts	8
	About non-event-based SNMP traps	16
	Enabling non-event-based SNMP traps for hardware monitoring	19
	Using the command-line shell to enable non-event-based SNMP traps	20
	Using the command-line shell to disable non-event-based SNMP traps	23
	About email notification from the deduplication appliance	24
	Configuring email notifications from the appliance shell menu	27
Chapter 2	SNMP hardware traps	28
	symcadapterTrap	29
	symccpuTrap	29
	symcdiskTrap	30
	symcfanTrap	31
	symcfibrechannelTrap	32
	symcfirmwareTrap	32
	symcnetworkcardTrap	32
	symcpciTrap	33
	symcpowerTrap	33
	symcraidgroupTrap	34
	symcsystemName	36
	symctemperatureTrap	36
	symcenclosurediskTrap	37
	symcenclosurefanTrap	38
	symcenclosurepowerTrap	39
	symcenclosuretemperatureTrap	39

Appendix A	Management Information Base (MIB) file contents	41
	The Management Information Base (MIB) file	41

Overview

This chapter includes the following topics:

- [About hardware monitoring and alerts](#)
- [About non-event-based SNMP traps](#)
- [About email notification from the deduplication appliance](#)

About hardware monitoring and alerts

The deduplication appliance monitors itself for hardware problems. The hardware monitoring information includes the appliance serial number, the appliance model number, and information about the components that is listed in [Table 1-1](#).

You have two ways to configure hardware alerts. First, you can configure alerts by email. Second, you can configure alerts through non-event-based SNMP. More information about these topics is available.

See [“About email notification from the deduplication appliance”](#) on page 24.

See [“About non-event-based SNMP traps”](#) on page 16.

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance

Monitored hardware	Sample of collected data
CPU	<p>Displays the following information about the CPU:</p> <ul style="list-style-type: none"> ■ Status. Can be either Presence detected or Disabled. ■ Voltage. Monitors the voltage to the appliance CPU chip and reports a CPU failure if any of the following conditions occur: <ul style="list-style-type: none"> ■ No voltage ■ The voltage is less than the low watermark. The low watermark is read from the system. ■ The voltage is more than the high watermark. The high watermark is read from the system. ■ State. Any state other than OK indicates a missing CPU or that the voltage for the CPUs is not within the normal range.
Disk	<p>Monitors the boot drive and the storage drives. Reports a disk failure if an internal erroneous state occurs. Displays the following information:</p> <ul style="list-style-type: none"> ■ Slot Number. Slot in the robot that contains the volume. ■ Status. Current status of the media. For example, Online, Spun Up, Unconfigured (bad). ■ Foreign state. Indicates if the disk is foreign. For example, None or Foreign. ■ Capacity. Current capacity of the disk. ■ Type. The disk type. For example, SAS, SATA. ■ Serial Number. The disk's serial number. ■ Enclosure ID. Identification number of the enclosure in which the disk resides. ■ State. If the State is not OK that means: <ul style="list-style-type: none"> ■ The status is either Failure, Unconfigured (bad), Missing, or Offline. ■ The status of the hot spare disk is not Hotspare. ■ There is no disk in the slot.

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance (*continued*)

Monitored hardware	Sample of collected data
RAID	<p>Monitors the RAID status and reports an error if the status changes from optimal. Displays the following information:</p> <ul style="list-style-type: none"> ■ Name. The name of the RAID device. ■ Status. Shows the current status of the device, such as Optimal. ■ Capacity. The capacity of each device. ■ Type. The type of RAID device, such as RAID-1 or RAID-6. ■ Disks. The disks being used. ■ Write Policy. Current write policy of each virtual disk. ■ Check consistency. The RAID is running check consistency or is not running. <ul style="list-style-type: none"> ■ "-" means check consistency is not running. ■ "Complete x%, Taken n min" indicates the progress of check consistency. ■ Enclosure ID. The enclosure ID for the RAID array. ■ Hotspare Available. Indicates the availability of global hot spare disks for the given virtual disk. ■ State. If the State is not OK that means: <ul style="list-style-type: none"> ■ The status is not Optimal. ■ The Write Policy is Write through. ■ The appliance does not contain any hot spare disks if the disk type is RAID-6.
Fan	<p>Monitors the fan units and reports errors. Displays the following information:</p> <ul style="list-style-type: none"> ■ Status. Reports the presence or absence of a fan unit, as follows: Device Present or Device Absent. ■ Speed. Monitors the fan speed and reports a fan failure when the following conditions occur: <ul style="list-style-type: none"> ■ The fan speed drops below the low watermark. The low watermark is read from the system. ■ The fan speed exceeds the high watermark. The high watermark is read from the system. ■ State. If the State is not OK, that indicates a missing fan or that the speed is not within the normal range.

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance (*continued*)

Monitored hardware	Sample of collected data
Power Supply	<p>Monitors the power supply wattage. Displays the following information:</p> <ul style="list-style-type: none"> ■ Status. Detects the wattage levels and determines whether the readings are within the limits of the low watermark and the high watermark. The following are the types of status messages displayed: <ul style="list-style-type: none"> ■ Presence detected. Displayed when the power is working as expected. ■ Failure detected. Displayed when the power module is not installed or when the power supply is installed but not connected to the power outlet. ■ Wattage. Monitors the wattage and reports a failure when the following conditions occur: <ul style="list-style-type: none"> ■ The wattage drops below the low watermark. ■ The wattage exceeds the high watermark. ■ State. If the State is not OK, that indicates that the power supply is absent or that the wattage is not within the normal range.
Temperature	<p>Monitors the temperature of the appliance at different points. Displays the following information:</p> <ul style="list-style-type: none"> ■ Type. Location within the appliance at which the temperature was read. This location can be one of the following: <ul style="list-style-type: none"> ■ Intake Vent Temp ■ Outtake Vent Temp ■ Backplane Temp Backplane Temp is only supported on the Deduplication Appliance 5000 and 5020. ■ Power Supply 1 Temp This is only supported for the 5030. ■ Power Supply 2 Temp This is only supported for the 5030. ■ P1 Therm Margin This is only supported for the 5030. ■ P2 Therm Margin This is only supported for the 5030. ■ CPU0_Core_Temp This is only supported for the 5000 and 5020. ■ CPU1_Core_Temp This is only supported for the 5000 and 5020. ■ Temperature. Reports the actual temperature reading and reports a problem when the following conditions occur: <ul style="list-style-type: none"> ■ The temperature drops below the low watermark. The low watermark is read from the system. ■ The temperature exceeds the high watermark. The high watermark is read from the system. <p>Note: For Px Therm Margin and CPUx_Core_Temp the temperature is displayed in a negative value. This value shows how many degrees are remaining before reaching the high temperature threshold.</p> ■ State. If the State is not OK, that indicates that the temperature reading at that location is not within the normal range.

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance (*continued*)

Monitored hardware	Sample of collected data
Fibre Channel HBA	<p>Monitors the fibre card status. Displays the following information:</p> <ul style="list-style-type: none"> ■ Status. Can be either Online, which means that the port is connected to a cable, or LinkDown. ■ Mode. The port's working mode, either Target or Initiator. ■ Port WWN. The unique world-wide name (WWN) for the port. ■ Slot. The physical slot where the fibre card is inserted. You can see the slot number on the rear panel. ■ Speed. The port speed, for example, 2G, 4G, 8G. ■ Remote Ports. Shows the WWNs of the other ports that this port can scan. Displays the WWN of each port that this port can scan remotely. ■ State. If the State is not OK that means the port is not online, linkdown or diagnostics.
Hardware Alerts	<p>Displays the hardware alerts.</p>
PCI	<p>Monitors the peripheral component interconnect (PCI) expansion slots. Displays the following information:</p> <ul style="list-style-type: none"> ■ Slot. The physical slot where the PCI is inserted. You can see the slot number on the rear panel. ■ Details. Information about the PCI card in the slot or the keyword EMPTY. If a card resides in the slot, the information includes the card type and the manufacturer.
Adapter	<p>Monitors the RAID adapter. Displays the following information:</p> <ul style="list-style-type: none"> ■ Adapter model. Includes the type and manufacturer. ■ Adapter Status, which identifies the adapter's working status. ■ Check Consistency, which identifies the current status of Check Consistency. The states can be Stopped or Active. ■ Patrol Read, which identifies the current status of Patrol Read. The states can be Stopped or Active ■ BBU Status, which identifies the BBU's status. ■ BBU Charging Status, which identifies if the BBU is charging, discharging, or none of them. ■ BBU Learn Cycle Active. If the BBU is present and is in Learn Cycle Active state, the RAID's Write Policy is changed to Write Back automatically. This change results in poor write performance. ■ BBU charge. The percentage of charge in the battery. If the appliance uses a supercap instead of a BBU, no value is shown here. ■ State. If the State is not OK that means the BBU is missing, BBU is in Learning Cycle Active state, or BBU Charging is less than 60%.

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance (*continued*)

Monitored hardware	Sample of collected data
Network	<p>Monitors the network cards. Displays the following information:</p> <ul style="list-style-type: none"> ■ Port name. The card's <code>ethx</code> identifier. ■ Card model. The card manufacturer. If Symantec does not support the card, displays the phrase Unsupported Network Card. ■ Serial number. The card serial number. ■ Port speed. ■ MAC address. ■ Link state. Displays Up or Down.
Firmware	<p>Monitors the firmware, including network card firmware and RAID controller firmware. Displays the following information:</p> <ul style="list-style-type: none"> ■ Name. Displays the name of each piece of firmware. ■ Version. Displays the version number of the firmware.

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance (*continued*)

Monitored hardware	Sample of collected data
Enclosure	

Table 1-1 Monitored hardware components in a NetBackup deduplication appliance (*continued*)

Monitored hardware	Sample of collected data
	<pre> -----+-----+-----+-----+----- 4 Device Present Low Speed OK +-----+-----+-----+-----+-----+ Enclosure 41 Power Supply Information +-----+-----+-----+-----+-----+ ID Status State +-----+-----+-----+-----+-----+ 1 Presence detected OK +-----+-----+-----+-----+-----+ 2 Unrecoverable Failure +-----+-----+-----+-----+-----+ Enclosure 41 Temperature Information +-----+-----+-----+-----+-----+ ID Type Temperature HighWaterMark State +-----+-----+-----+-----+-----+ 1 Backplane Temp 1 34 degrees C 51 degrees C OK +-----+-----+-----+-----+-----+ 2 Backplane Temp 2 41 degrees C 51 degrees C OK +-----+-----+-----+-----+-----+ </pre>

After the appliance logs a problem that needs attention, you can retrieve the notice in one of the following ways:

- Through the administrative web UI in the hardware monitoring and alerts panels.
- In an email that is sent from the appliance to the local administrator.
 See [“About email notification from the deduplication appliance”](#) on page 24.
- In a notification that is sent from the appliance to Symantec by the Call Home feature.

Symantec recommends that you check for hardware alert messages on a daily basis.

About non-event-based SNMP traps

The NetBackup deduplication appliance enables you to send non-event-based SNMP traps.

The deduplication appliance can send an SNMP trap to notify you of the following types of non-event-based system activity:

- Disks reaching their hard limit or their soft limit
- Job failures
- Stopped services
- Hardware monitoring

In addition to sending an SNMP trap, the deduplication appliance logs all traps in the following files:

- `/Storage/log/NonEventBasedSNMP.log`
- `/Storage/log/pdhwmon.log`

The deduplication appliance sends traps of the following format:

```
Storagepool: storagepoolid (storagepoolname,SPA:spahostname)
Agent: agentid ([alias, ][hostname, ][ipaddress[, PDserver])
[Dataselection: dsid (dataselectionname)]
[Job: jobid (workflowname)]
[Jobstep: jobstepid (workflowstepname)]
ErrID: errorid
Descr: errordescription
```

The following notes apply to the SNMP trap format:

- The deduplication appliance omits *alias* if it is empty or equal to *hostname*.
- The deduplication appliance omits *hostname* if it is empty or equal to *ipaddress*.
- The deduplication appliance includes *PDserver* only if the agent is a PureDisk server. The deduplication appliance omits *PDserver* if the error message applies to a client agent.
- If a field does not pertain to a specific trap, the deduplication appliance omits the field. This situation can occur, for example, with the `Dataselection`, `Job`, or `Jobstep` fields.

You can use the Web UI to change the following values:

- The *alias* and *hostname* values for an agent.
 To change these values for client agents, complete the following steps:
 - Select **Manage > Agents**.
 - Select a client agent in the left pane.
 - Edit the information in the right pane.
 - Click **Save**.

To change these values for server agents, complete the following steps:

- Select **Settings > Topology**.
- Select a server agent in the left pane.
- Edit the information in the right pane.
- Click **Save**.
- The *storagepoolname*.
 To change this value for a storage pool, complete the following steps:
 - Select **Settings > Topology**.
 - Select a storage pool in the left pane.
 - Edit the information in the right pane.
 - Click **Save**.

The following is an SNMP trap example for software traps:

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (5604365) 15:34:03.65
SNMPv2-MIB::snmpTrapOID.0 = OID:
VERITAS-COMMAND-CENTRAL-MIB::ccCritical
VERITAS-COMMAND-CENTRAL-MIB::alertDescription = STRING: Storagepool:
771 (birdie,SPA:acme.com)Agent: 771000000 (acme.com, PDserver)ErrID:
1001Descr: Service 'Controller' (pdctrl) is currently not running
```

The following is an SNMP trap example for deduplication appliance hardware traps:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 150 days, 0 hours,
26 minutes, 6 seconds.:
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0:
Object ID: .1.3.6.1.4.1.393.3.9:
.iso.org.dod.internet.private.enterprises.symantecsoftware.products.applianceMonitoringMib.
systems.systemName: test_system_name:
.iso.org.dod.internet.private.enterprises.symantecsoftware.products.applianceMonitoringMib.
systems.powerTrap: POWER 1 status : Failure detected:
POWER 1 wattage : 0 Watts:
POWER 1 lowwatermark : 0:
POWER 1 highwatermark : 700 Watts:
.iso.org.dod.internet.private.enterprises.symantecsoftware.products.applianceMonitoringMib.
systems.cpuTrap: CPU 2 status : Disabled:
CPU 2 voltage : -:
CPU 2 lowwatermark : -:
CPU 2 highwatermark : -:
```

Note: Some lines in the preceding example were wrapped and indented for inclusion in this topic.

The following topics contain information about SNMP traps on the deduplication appliance:

- See [“Enabling non-event-based SNMP traps for hardware monitoring”](#) on page 19.
- See [“Using the command-line shell to enable non-event-based SNMP traps”](#) on page 20.
- See [“Using the command-line shell to disable non-event-based SNMP traps”](#) on page 23.

The information in this guide that describes SNMP traps supplements the information about how to enable the SNMP traps that is included in the following manual:

PureDisk Backup Operator’s Guide

Enabling non-event-based SNMP traps for hardware monitoring

The following procedure describes how to enable the SNMP software.

To configure the SNMP software

- 1 Obtain the following files from the storage pool authority node and install them on your site's SNMP manager server:

```
/opt/pdinstall/snmp/VERITAS-REG.mib
/opt/pdinstall/snmp/VERITAS-TC.mib
/opt/pdinstall/snmp/VRTS-cc.mib
/opt/pdinstall/snmp/SYMANTEC-APPLIANCE-MONITORING.mib
```

In the preceding list, the first three files constitute the NetBackup MIB and are used for monitoring software events. The last file is used for monitoring hardware events.

- 2 Perform one of the following procedures:
 - The procedure called "Enabling the non-event-based SNMP trap feature" in the online Help or in the following manual:
PureDisk Backup Operator’s Guide
 - Using the command-line shell:
See [“Using the command-line shell to enable non-event-based SNMP traps”](#) on page 20.
 - Using Configure Alert in the Configuration Wizard:

See [“About non-event-based SNMP traps”](#) on page 16.

Using the command-line shell to enable non-event-based SNMP traps

The following procedure explains how to use the deduplication appliance's command-line shell to enable non-event-based SNMP traps. This procedure has the same effect as the SNMP enablement procedure in the following manual:

PureDisk Backup Operator's Guide

To enable non-event-based SNMP traps

- 1 Start a command-line shell session on the storage pool authority node.

Perform the following steps:

- Connect to the storage pool authority node through an SSH connection.
- Type the user name and password for the deduplication appliance shell menu.
By default, the user name is `sysadmin`, and the password is `P@ssw0rd`. In the preceding password, the sixth character is the numeral zero (0).
- After the welcome information appears, press `q` to display the root mode menu.
- Type `support` at the shell menu prompt and press Enter.

For example:

> **support**

- 2 Type the following `snmp add` command to specify one or two SNMP server names and (optionally) your SNMP community:

```
> snmp add server1 [community]
```

For *server*, specify the IP address, host name, or FQDN of your site's primary SNMP server. The deduplication appliance must be able to contact this server.

For *community*, specify the community name. This argument is optional. Default is `public`.

The following example specifies the primary SNMP server:

```
> snmp add 100.100.100.101
```

```
Successfully updated SNMP SERVER to 100.100.100.101
```

If you want to add a secondary SNMP server, type the following `snmp add` command:

```
> snmp add server1 [community] server2
```

```
> snmp add 100.100.100.101 public 100.100.100.102
```

3 (Optional) Type the following command to verify the SNMP server:

```
> snmp show
```

The following output shows one SNMP server:

```
> snmp show
SERVER                : snmpserver.yourcompany.com
PORT                  : 162
COMMUNITY              : public
ENABLE HARDWARE       : 0
ENABLE SOFTWARE EVENT : 0
ENABLE SOFTWARE NONEVENT : 0
SOFTWARE EVENT ALERT LEVEL : <not configured>
```

The following output shows two SNMP servers:

```
> snmp show
SERVER                : snmpserver.yourcompany.com
SERVER2               : snmpserver2.yourcompany.com
PORT                  : 162
COMMUNITY              : public
ENABLE HARDWARE       : 0
ENABLE SOFTWARE EVENT : 0
ENABLE SOFTWARE NONEVENT : 0
SOFTWARE EVENT ALERT LEVEL : <not configured>
```

4 Type the following command to enable SNMP:

```
> snmp enable
```

If you want to enable hardware SNMP, type the following **snmp enable** command:

```
snmp enable hardware
```

If you want to enable software SNMP, type the following **snmp enable** command:

```
snmp enable software
```

Note: You will be prompted to select `event` or `nonevent` when enabling software SNMP.

5 (Optional) Type the following command to verify that SNMP is enabled:

```
> snmp show
```

The following example shows the output from the `snmp show` command after you enable SNMP. Note the line that reads `SNMP ENABLE HARDWARE : 1`, which indicates that SNMP is enabled. It also shows that event based and non-event based SNMP is enabled.

```
> snmp show
```

```
SERVER                : snmpserver.yourcompany.com
SERVER2               : snmpserver2.yourcompany.com
PORT                  : 162
COMMUNITY              : public
ENABLE HARDWARE       : 0
ENABLE SOFTWARE EVENT : 0
ENABLE SOFTWARE NONEVENT : 0
SOFTWARE EVENT ALERT LEVEL : <not configured>
```

6 Type the following command to return to the main shell menu:

```
> exit
```

7 Type the following command to exit the shell menu:

```
> logout
```

See [“About non-event-based SNMP traps”](#) on page 16.

Using the command-line shell to disable non-event-based SNMP traps

The following procedure explains how to disable non-event-based SNMP traps.

To disable non-event-based SNMP traps

1 Start a command-line shell session on the storage pool authority node.

Perform the following steps:

- Connect to the storage pool authority node through an SSH connection.
- Type the user name and password for the deduplication appliance shell menu.

By default, the user name is `sysadmin`, and the password is `P@ssw0rd`.

In the preceding password, the sixth character is the numeral zero (0).

- After the welcome information appears, press `q` to display the root mode menu.
 - Type `support` at the shell menu prompt and press Enter.
 For example:
 > `support`
- 2 Type the following command to disable SNMP:
 > `snmp disable hardware`
 - 3 (Optional) Type the following command to verify that SNMP is disabled:
 > `snmp show`

```

SERVER                               : snmpserver.yourcompany.com
SERVER2                               : snmpserver2.yourcompany.com
PORT                                  : 162
COMMUNITY                             : public
ENABLE HARDWARE                       : 0
ENABLE SOFTWARE EVENT                 : 0
ENABLE SOFTWARE NONEVENT             : 0
SOFTWARE EVENT ALERT LEVEL           : <not configured>

```
 - 4 Type the following command to return to the main shell menu:
 > `exit`
 - 5 Type the following command to exit the shell menu:
 > `logout`

See [“About non-event-based SNMP traps”](#) on page 16.

About email notification from the deduplication appliance

The deduplication appliance has the ability to send an email to a local administrator when a hardware failure is detected. The following table lists the hardware failures that prompt an email notification. It also contains an example of the contents that would appear in the email for each failure.

**Monitored
Hardware**

Example of the email contents

Adapter

```
ADAPTER 1 Adapter model : Intel (R) RAID Controller RS25SB008
ADAPTER 1 BBU Status : Not OK
ADAPTER 1 ErrorStatus : 2
ADAPTER 1 Adapter Status : OK
ADAPTER 1 BBU Learn Cycle Active : -
ADAPTER 1 BBU charge : -
ADAPTER 1 BBU Charging Status : -
ADAPTER 1 State : Critical Warning
```

CPU

```
CPU 2 ErrorStatus : 1
CPU 2 Status : Disabled
CPU 2 LowWaterMark : 0.530 Volts
CPU 2 Voltage : -
CPU 2 State : Failure
CPU 2 HighWaterMark : 1.760 Volts
```

Monitored Hardware

Example of the email contents

Disk

```

DISK 10 Slot Number : 9
DISK 10 Enclosure ID : -
DISK 10 Status : Not found
DISK 10 Serial Number : -
DISK 10 Capacity : -
DISK 10 State : Failure
DISK 10 Type : -
DISK 10 Foreign state : -
DISK 10 ErrorStatus : 1

DISK 23 Slot Number : 22
DISK 23 Enclosure ID : 8
DISK 23 Status : Unconfigured(good), Spun Up
DISK 23 Serial Number : 9WM1N1EZST32000644NS SN12
DISK 23 Capacity : 1.819 TB [0xe8e088b0 Sectors]
DISK 23 State : Warning
DISK 23 Type : SATA
DISK 23 Foreign state : Foreign
DISK 23 ErrorStatus : 3

DISK 24 Slot Number : 23
DISK 24 Enclosure ID : 8
DISK 24 Status : Unconfigured(good), Spun Up
DISK 24 Serial Number : 9WM1N1H5ST32000644NS SN12
DISK 24 Capacity : 1.819 TB [0xe8e088b0 Sectors]
DISK 24 State : Warning
DISK 24 Type : SATA
DISK 24 Foreign state : Foreign
DISK 24 ErrorStatus : 3

```

Fan

```

FAN 1 ErrorStatus : 1
FAN 1 Speed : -
FAN 1 Status : Device Absent
FAN 1 LowWaterMark : 1974.000 RPM
FAN 1 State : Failure
FAN 1 HighWaterMark : 11468.000 RPM

FAN 2 ErrorStatus : 1
FAN 2 Speed : -
FAN 2 Status : Device Absent
FAN 2 LowWaterMark : 1974.000 RPM
FAN 2 State : Failure
FAN 2 HighWaterMark : 11468.000 RPM

```

Monitored Hardware

Example of the email contents

Power Supply

```
POWER 2 Wattage : -
POWER 2 ErrorStatus : 1
POWER 2 Status : Failure detected
POWER 2 LowWaterMark : 1 Watts
POWER 2 State : Failure
POWER 2 HighWaterMark : 700 Watts
```

RAID Group

```
RAIDGROUP 2 Enclosure ID : 8
RAIDGROUP 2 Status : Optimal
RAIDGROUP 2 Disks : 4,5,6,7,8,10,11,12,13,14,15,16,17,18,19,20
RAIDGROUP 2 Capacity : 27.270 TB
RAIDGROUP 2 State : Warning
RAIDGROUP 2 Type : Primary-6, Secondary-0, RAID Level Qualifie
RAIDGROUP 2 ErrorStatus : 3
RAIDGROUP 2 All HotSpares Available : yes
RAIDGROUP 2 Write Policy : WriteThrough, ReadAheadNone, Direct
RAIDGROUP 2 Name : VD-2
```

For information about how to configure email notifications, see the following:

See [“Configuring email notifications from the appliance shell menu”](#) on page 27.

For general information about hardware notifications, see the following:

See [“About hardware monitoring and alerts”](#) on page 8.

Configuring email notifications from the appliance shell menu

You can use the `support > email hardware` command from the appliance shell menu interface to configure the email address that you want to use to receive the hardware failure notification. The contents of the email identifies the type of hardware failure that occurred and a status of the failure.

For more information about how to configure email notifications from the appliance shell menu, see the following topic:

For more information about email notifications, see the following:

See [“About email notification from the deduplication appliance”](#) on page 24.

SNMP hardware traps

This chapter includes the following topics:

- [symcadapterTrap](#)
- [symccpuTrap](#)
- [symcdiskTrap](#)
- [symcfanTrap](#)
- [symcfibrechannelTrap](#)
- [symcfirmwareTrap](#)
- [symcnetworkcardTrap](#)
- [symcpciTrap](#)
- [symcpowerTrap](#)
- [symcraidgroupTrap](#)
- [symcsystemName](#)
- [symctemperatureTrap](#)
- [symcenclosediskTrap](#)
- [symcenclosurefanTrap](#)
- [symcenclosurepowerTrap](#)
- [symcenclosuretemperatureTrap](#)

symcadapterTrap

OID: 1.3.6.1.4.1.393.3.9.1.14

Description

The `symcadapterTrap` monitors the status of the appliance adapters (RAID controllers). If you receive an alert, it means that one of adapters is not in an optimal state.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-1 Next steps for the `symcadapterTrap`

What happened	What to do now
If the Adapter Status is NOT OK , the adapter has failed.	Contact Symantec Support to replace the adapter.
If the BBU Status is NOT OK , and the current Charge is NULL , the firmware was unable to report the current charge.	Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Symantec Support for assistance.
5020 only: If the BBU Status is NOT OK , and the current Charge is less than 67 or greater than 130, the adapter battery backup unit (BBU) is about to fail.	Contact Symantec Support to replace the adapter BBU.

symccpuTrap

OID: 1.3.6.1.4.1.393.3.9.1.7

Description

The `symccpuTrap` monitors the status of the appliance CPUs. If you receive an alert, it means that a CPU has malfunctioned or that the voltage has crossed the threshold value.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-2 Next steps for the `symccpuTrap`

What happened	What to do now
If the CPU Status is NULL , the firmware was unable to report the current status.	Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Symantec Support for assistance.
If the CPU State is Failed , and the Status is Presence detected or Disabled , the status of the CPU is unknown.	Contact Symantec Support for assistance.
5030 only: If the CPU State is Failed , and the current Voltage is greater than the high threshold of 1.51 Volts, the CPU voltage is too high.	Check the status of the appliance power supplies. Check the temperature of the appliance's environment. If both are normal, contact Symantec Support for assistance.
5030 only: If the CPU State is Failed , and the current Voltage is lower than the low threshold of .54 Volts, the CPU voltage is too low.	Check the status of the appliance power supplies. Check the temperature of the appliance's environment. If both are normal, contact Symantec Support for assistance.

symcdiskTrap

OID: 1.3.6.1.4.1.393.3.9.1.8

Description

The `symcdiskTrap` monitors the status of the appliance disks. If you receive an alert, it means that one of the disks has experienced an error.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-3 Next steps for the `symcdiskTrap`

What happened	What to do now
If the disk State is Warning , and the Status is Unconfigured (Good) , the disk is in a foreign, unsupported state. The disk may have been reinserted and caused an error.	Contact Symantec Support. Let them know of the error, with the following message: Import foreign configuration
If the disk State is Failed , and the Status is Unconfigured (Bad) , the disk is no longer functional.	Contact Symantec Support to replace the faulty disk.
If the disk State is Failed , and the Status is Offline , the disk is offline.	Contact Symantec Support for assistance.
If the disk State is Failed , and the Status is Missing, Not Found , or Removed , the disk cannot be detected.	Check to make sure that the disk is installed properly and is fully seated in the appliance.

symcfanTrap

OID: 1.3.6.1.4.1.393.3.9.1.3

Description

The `symcfanTrap` monitors the status of the appliance fans. If you receive an alert, it means that one or more of the system fans has experienced an error. Either a fan has stopped working, or the fan rpm has crossed the threshold value that is required for proper system functioning.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-4 Next steps for the `symcfanTrap`

What happened	What to do now
If the fan State is Warning , the fan is running slower than the low threshold of 1715 rpm.	Check the system temperature. Check the power supply. If both are normal, contact Symantec Support to replace the fan.
If the fan State is Failed , the fan is missing or has failed.	Contact Symantec Support to replace the fan.

symcfibrechannelTrap

OID: 1.3.6.1.4.1.393.3.9.1.5

Description

The `symcfibrechannelTrap` monitors the status of the appliance Fibre Channel links. If you receive an alert, it means that one or more of the Fibre Channel links is not in an optimal state.

Resolution

Check the physical Fibre Channel connections and the Fibre Channel configuration settings. If both are normal, contact Symantec Support. The Fibre Channel card may need to be replaced.

symcfirmwareTrap

OID: 1.3.6.1.4.1.393.3.9.1.15

Description

The `symcfirmwareTrap` is an informational trap that tracks the firmware of the appliance. It does not trigger any alerts.

symcnetworkcardTrap

OID: 1.3.6.1.4.1.393.3.9.1.17

Description

The `symcnetworkcardTrap` is an informational trap that tracks the network cards that are installed in the appliance. It does not trigger any alerts.

symcpciTrap

OID: 1.3.6.1.4.1.393.3.9.1.16

Description

The `symcpciTrap` monitors the appliance PCIe cards. If you receive an alert, it means that one or more of the PCIe cards are not installed in the correct slots, or a PCIe card is not functional.

Resolution

Check to make sure that the PCIe cards are installed in the correct slots. To see the supported PCIe slot configurations, refer to the following documents:

- For the 5030 appliance or the 5000 appliance, refer to the *NetBackup Deduplication Appliance Product Description Guides*.
- For the 5020 appliance, refer to the *NetBackup Deduplication Appliance Getting Started Guide*.

If the PCIe cards are all installed in the correct slots, contact Symantec Support to replace the faulty card(s).

symcpowerTrap

OID: 1.3.6.1.4.1.393.3.9.1.4

Description

The `symcpowerTrap` monitors the status of the appliance power supplies. If you receive an alert, it means that one of the power supplies has experienced an error.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-5 Next steps for the symcpowerTrap

What happened	What to do now
If the power supply Status is Power Supply AC lost , the redundant power supply is not functional. Either the power supply has stopped working, or it is not plugged in to a power source.	Check the power supply cable. If the power supply is plugged in, and the cable is functional, contact Symantec Support to replace the power supply.
If the power supply State is Warning , and the current Wattage is greater than the high threshold of 920 Watts, the power supply is using too much power.	Contact Symantec Support to replace the power supply.
If the power supply State is Warning , and the current Wattage is not defined, the firmware was unable to report the current status.	Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Symantec Support for assistance.
If the power supply State is Failed , the firmware was unable to report the current status.	Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Symantec Support for assistance.

symcraidgroupTrap

OID: 1.3.6.1.4.1.393.3.9.1.9

Description

The `symcraidgroupTrap` monitors the status of the appliance RAID groups in the operating system disks and in the storage disks. If you receive an alert, it means that one of the RAID groups is not in an optimal state. Either the write policy is in write through mode, or one or more of the disks in the RAID group has experienced an error.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-6 Next steps for the symcraidgroupTrap

What happened	What to do now
If the RAID State is Warning , and the Status is Degraded or Partially Degraded , one or more of the disks in the RAID group has failed.	Contact Symantec Support to replace the faulty disk(s) before additional disk errors destroy the RAID volume.
If the RAID State is Warning , and Hotspare available is No , the hot spare disk or disks are unavailable. Either they have become faulty, or another disk failed, and the hot spare needed to be rebuilt.	<p>Check the disk status. If a disk has failed, contact Symantec Support to replace the faulty disk.</p> <p>If a disk has not failed, but one of the disks has a Status of Unconfigured (Good), start the copyback process on that disk if it did not begin automatically. If you need assistance, contact Symantec Support.</p>
If the RAID State is Warning , and the Write Policy is WriteThrough , caching is disabled. Either the Battery Backup Unit (BBU) relearn cycle is on, the write policy was not set correctly, or the BBU is faulty.	Check the adapter status. If the adapter does not have any warnings or failures, contact Symantec Support for assistance.
If the RAID State is Failed , and the Status is also Failed , the RAID is offline or is not functional.	Contact Symantec Support for assistance.
If the RAID State is Failed , and the Status is Unknown , the firmware was unable to report the current status.	<p>Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure.</p> <p>If the issue is not resolved, contact Symantec Support for assistance.</p>
If the RAID State is Failed , and the Status is Missing , all of the disks in the RAID group have been removed from the array. The RAID group is neither operable nor exportable.	Contact Symantec Support for assistance.
If the RAID State is Failed , and the Status is Contingent - preparing for import , the RAID group is incomplete. The group is likely - but not certain - to become complete and available for import.	Contact Symantec Support for assistance.

Table 2-6 Next steps for the `symcraidgroupTrap` (continued)

What happened	What to do now
If the RAID State is Failed , and the Status is Exported - ready for import or Forced - ready for import , the RAID group is in an exported state and is ready to be imported.	Contact Symantec Support for assistance.

symcsystemName

OID: 1.3.6.1.4.1.393.3.9.1.1

Description

The `symcsystemName` trap is an informational trap that tracks the appliance host name. It does not trigger any alerts.

symctemperatureTrap

OID: 1.3.6.1.4.1.393.3.9.1.6

Description

The `symctemperatureTrap` monitors the temperature of the appliance. If you receive an alert, it means that the temperature has exceeded a threshold value, or one of the sensors has stopped working.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-7 Next steps for the `symctemperatureTrap`

What happened	What to do now
If the temperature State is Warning , and the current temperature reading is 0.000 degrees C , the temperature is lower than the low threshold, or the firmware was unable to report the correct temperature.	<p>Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure.</p> <p>If the issue is not resolved, contact Symantec Support for assistance.</p>

Table 2-7 Next steps for the `symctemperatureTrap` (continued)

What happened	What to do now
<p>If the temperature State is Warning, and the current temperature reading is hotter than the high temperature threshold, the temperature is too high. The following are the high threshold values for the appliance temperature sensors:</p> <ul style="list-style-type: none"> ■ Intake Vent Temperature: 64 degrees C ■ Outtake Vent Temperature: 85 degrees C ■ P1 and P2 Therm Margins: -15 degrees C 	<p>Check the status of the appliance fans. Check the temperature of the appliance's environment. If both are normal, contact Symantec Support for assistance.</p>
<p>If the temperature State is Warning, and the current temperature reading is cooler than the low temperature threshold, the temperature is too low. The following are the low threshold values for the appliance temperature sensors:</p> <ul style="list-style-type: none"> ■ Intake Vent Temperature: 0 degrees C ■ Outtake Vent Temperature: 0 degrees C ■ P1 and P2 Therm Margins: -128 degrees C 	<p>Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure.</p> <p>If the issue is not resolved, contact Symantec Support for assistance.</p>

symcenclosediskTrap

OID: 1.3.6.1.4.1.393.3.9.1.13

Description

The `symcenclosediskTrap` monitors the status of the storage shelf disks. If you receive an alert, it means that one of the disks has experienced an error.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-8 Next steps for the `symcenclosediskTrap`

What happened	What to do now
If the disk State is Warning , and the Status is Unconfigured (Good) , the disk is in a foreign, unsupported state. The disk may have been reinserted and caused an error.	Contact Symantec Support. Let them know of the error, with the following message: Import foreign configuration
If the State of disk 16 is Warning , and the Status is anything other than Hot spare , one of the other disks experienced an error, and the hot spare had to be rebuilt.	Contact Symantec Support to replace the faulty disk.
If the disk State is Failed , and the Status is Unconfigured (Bad) , the disk is no longer functional.	Contact Symantec Support to replace the faulty disk.
If the disk State is Failed , and the Status is Offline , the disk is offline.	Contact Symantec Support for assistance.
If the disk State is Failed , and the Status is Missing or Not Found , the disk cannot be detected.	Check to make sure that the disk is installed properly and is fully seated in the storage shelf.

symcenclosurefanTrap

OID: 1.3.6.1.4.1.393.3.9.1.10

Description

The `symcenclosurefanTrap` monitors the status of the storage shelf fans. If you receive an alert, it means that one or more of the system fans has experienced an error. Either a fan has stopped working, or the fan rpm has crossed the threshold value that is required for proper system functioning.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-9 Next steps for the `symcenclosurefanTrap`

What happened	What to do now
If the fan State is Warning , the fan is running slower than the low threshold of 2000 rpm.	Check the system temperature. Check the power supply. If both are normal, contact Symantec Support to replace the fan.
If the fan State is Failed , the fan is missing or has failed.	Contact Symantec Support to replace the fan.

symcenclosurepowerTrap

OID: 1.3.6.1.4.1.393.3.9.1.11

Description

The `symcenclosurepowerTrap` monitors the status of the appliance power supplies. If you receive an alert, it means that one of the power supplies has experienced an error. Either the power supply has stopped working, or it is not plugged in to a power source.

Resolution

Check the power supply cable. If the power supply is plugged in, and the cable is functional, contact Symantec Support to replace the power supply.

symcenclosuretemperatureTrap

OID: 1.3.6.1.4.1.393.3.9.1.12

Description

The `symcenclosuretemperatureTrap` monitors the temperature of the appliance storage shelf. If you receive an alert, it means that the temperature has exceeded a threshold value, or one of the sensors has stopped working.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. You can also check the **Monitor > System** page of the administrative web UI.

Based on the information from the SNMP trap, the email alert, or the **Monitor > System** page, take one of the following actions:

Table 2-10 Next steps for the `symcenclosuretemperatureTrap`

What happened	What to do now
If the temperature State is Warning , and the current temperature reading is 0.000 degrees C , the temperature is lower than the low threshold, or the firmware was unable to report the correct temperature.	Wait 15 minutes for the next Call Home interval and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Symantec Support for assistance.
If the temperature State is Warning , and the current temperature reading is hotter than the high temperature threshold of 51 degrees C, the temperature is too high.	Check the status of the storage shelf fans. Check the temperature of the storage shelf's environment. If both are normal, contact Symantec Support for assistance.

Management Information Base (MIB) file contents

This appendix includes the following topics:

- [The Management Information Base \(MIB\) file](#)

The Management Information Base (MIB) file

The NetBackup Deduplication Appliance Management Information Base (MIB) file contains the notification traps that are configured to monitor the appliance.

You can view the contents of the MIB file with the `Support > SNMP ShowMIB` command in the appliance shell menu.

Note: Although the MIB file includes software traps, they are not used. NetBackup Deduplication Appliance does not currently send any software traps.

The following is a copy of the NetBackup Deduplication Appliance 1.4.5 MIB file:

```
SYMANTEC-APPLIANCE-MONITORING-MIB DEFINITIONS ::= BEGIN

IMPORTS
    DisplayString, mib-2 FROM RFC1213-MIB
    enterprises, OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY FROM
        SNMPv2-SMI;

applianceMonitoringMib MODULE-IDENTITY
    LAST-UPDATED "201309240000Z"
```

```

ORGANIZATION "Symantec Corporation"
CONTACT-INFO "350 Ellis Street
              Mountain View, CA 94043 US
              Subject: appliance.mib"
DESCRIPTION  "The MIB module for Symantec Appliance Monitoring"

REVISION     "201309240000Z"
DESCRIPTION  "Removed systemLocation object from list since it was
              not used or sent in trap."

 ::= { products 9 }

symantecsoftware      OBJECT IDENTIFIER ::= { enterprises 393 }
products              OBJECT IDENTIFIER ::= { symantecsoftware 3 }

systems              OBJECT IDENTIFIER ::= { applianceMonitoringMib 1 }
software             OBJECT IDENTIFIER ::= { applianceMonitoringMib 2 }

-- system traps

symcsystemName OBJECT-TYPE
    SYNTAX DisplayString (SIZE(0..80))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "System Name"
 ::= { systems 1 }

symcfanTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps fan failures"
 ::= { systems 3 }

symcpowerTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps power failures"
 ::= { systems 4 }

symcfibrechannelTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps FibreChannel failures"

```

```
::= { systems 5 }

symctemperatureTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps temperature failures"
::= { systems 6 }

symccpuTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps cpu failures"
::= { systems 7 }

symcdiskTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps disk failures"
::= { systems 8 }

symcraidgroupTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps raid failures"
::= { systems 9 }

symcenclosurefanTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps enclosure fan failures"
::= { systems 10 }

symcenclosurepowerTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps enclosure power failures"
::= { systems 11 }

symcenclosuretemperatureTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps enclosure temperature failures"
```

```

 ::= { systems 12 }

symcenclosureDiskTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps enclosure disk failures"
 ::= { systems 13 }

symcadapterTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps adapter failures"
 ::= { systems 14 }

symcfirmwareTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps firmware failures"
 ::= { systems 15 }

symcpciTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps pci failures"
 ::= { systems 16 }

symcnetworkcardTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps network card failures"
 ::= { systems 17 }

symcvolumeTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps volume failures"
 ::= { systems 18 }

symcbbuTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps BBU failures"
 ::= { systems 19 }

```

```
symcconnectionTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Traps connection failures"
    ::= { systems 20 }

-- software traps

symcfailedJobsTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Job failures Trap"
    ::= { software 1 }

symcprocessTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Processes stopped traps"
    ::= { software 2 }

symcdiskSpaceTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Low disk space traps"
    ::= { software 3 }

symcsoftwareUpdateSuccessTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Software update success trap"
    ::= { software 4 }

symcsoftwareUpdateFailedRollbackSuccessTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Software update failed but rollback was successful trap"
    ::= { software 5 }

symcsoftwareUpdateFailedRollbackFailedTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Software update and rollback failed trap"
```

```
::= { software 6 }

symcrollbackSuccessTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Software rollback success trap"
::= { software 7 }

symcrollbackFailedTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Software rollback failed trap"
::= { software 8 }

symcclusterStateTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Cluster node failed trap"
::= { software 9 }

symcdiskPerfTrap NOTIFICATION-TYPE
    OBJECTS { symcsystemName }
    STATUS current
    DESCRIPTION "Disk performance alert trap"
::= { software 10 }

END
```