NetBackup Appliance SNMP Trap Reference Guide

VERITAS™

Veritas Appliance SNMP Trap Reference Guide

Release 3.0

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

.

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Overview

This chapter includes the following topics:

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It uses either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) for transport, depending on configuration. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager model and agent model. This model consists of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

NetBackup Appliance 3.0 supports SNMP v2.

Example SNMP trap

The following is an example of an SNMP trap that is generated when SNMP is configured on the appliance. This example is for the NetBackup 5230 Appliance RAID group:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0:
TimeTicks:  20 hours, 24 minutes, 41 seconds.:
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.
snmpTrap.snmpTrapOID.0:  Object ID:  .1.3.6.1.4.1.48328.3.9.1.9:
.iso.org.dod.internet.private.enterprises.veritassoftware.products.
applianceMonitoringMib.systems.vrtssystemName:
i89-eng138.cdc.veritas.com:
.iso.org.dod.internet.private.enterprises.veritassoftware.products.
applianceMonitoringMib.systems.vrtsraidgroupTrap:
{"appliance_1_raidgroup_-_enclosure id": "-",
"appliance_1_raidgroup_-_type": "RAID-6","appliance_1_raidgroup_-_wwid"
: "-","appliance_1_raidgroup_-_capacity": "4.54TB",
"appliance_1_raidgroup_-_name": "Controller 0 VD 0",
"appliance_1_raidgroup_-_state": "Warning",
"appliance_1_raidgroup_-_errorstatus": "2",
"appliance_1_raidgroup_-_all hotspares available": "Yes",
"appliance_1_raidgroup_-_status": "Degraded",
"appliance_1_raidgroup_-_disks":
"252: 0 252: 1 252: 2 252: 3 252: 4 252: 5 252: 6 ",
"appliance_1_raidgroup_-_write policy": "Write Back"}:
```

About the Management Information Base (MIB)

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) that is associated with it. Each OID consists of the numbers that are separated by decimal points (for example, 1.3.6.1.4.1.48328.1).

These OIDs form a tree. A MIB associates each OID with a readable label and various other parameters that are related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages. This information is saved as a MIB file.

You can check the details of the SNMP MIB file from the **Settings > Notifications > Alert Configuration** page of the web console. To configure the appliance SNMP manager to receive hardware monitoring related traps, click **View SNMP MIB file** in the **SNMP Server Configuration** page.

You can also view the SNMP MIB file with the `Settings > Alerts > SNMP ShowMIB` command in the Shell Menu of your appliance.

See "The Management Information Base (MIB) file" on page 33.

Settings > Notifications > Alert Configuration

The **Settings > Notifications > Alert Configuration** page provides you with one location from where you can enable SNMP, SMTP, and Call Home alert notifications. The page is divided into three sections each dedicated to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.

Under **Alert Configuration** is the **Notification Interval** field. You must enter the time interval in minutes between two subsequent notifications for the SNMP and the SMTP configurations. The time interval should be in multiples of 15 and it should not be zero.

Configuring SNMP

Table 1-1 lists the fields from the **SNMP** (Simple Network Management Protocol) section.

Table 1-1 SNMP Server Configuration settings

Fields	Description
Enable SNMP Alert	Select this check box to enable SNMP alert configuration.
SNMP Server	Enter the SNMP Server host name. You can enter a host name or an IP address to define this computer. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed. Notification of the alerts or traps that are generated in Appliance are sent to this SNMP manager. **Note:** The NetBackup Appliance supports all the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified for version 2.6.
SNMP Port	Enter the SNMP Server port number. If you do not enter anything for this variable, then the default port is 162. **Note:** Your firewall must allow access from the appliance to the SNMP server through this port.

Table 1-1 SNMP Server Configuration settings *(continued)*

Fields	Description
SNMP Community	Enter the community to which the alerts or traps are sent. For example, Backup Reporting Department. You can enter a value that you configured on your SNMP server. For example, you can enter a company name or a name like, `admin_group`, `public`, or `private`. If you do not enter anything, then the default value is `public`.

See "Example SNMP trap" on page 7.

The SNMP MIB file serves as a data dictionary that is used to assemble and interpret SNMP messages. If you configure SNMP, you must import the MIB file into the monitoring software so that the software can interpret the SNMP traps. You can check the details of the MIB file from the SNMP Server Configuration pane. To check details about the SNMP MIB file, click **View SNMP MIB file**. An SNMP MIB file opens.

For information on how to send a test SNMP trap after configuration, see the following technical article on the Veritas Support website:

www.veritas.com/docs/TECH208354

Configuring SMTP

The SMTP mail server protocol is used for outgoing email. You can configure SMTP from the NetBackup Appliance Web Console (**Settings > Alert Configuration > SMTP Server Configuration**).

You can also use the following command in the Shell Menu of your appliance to configure the SMTP server and add a new email account:

`Main_Menu > Settings > Alerts > Email SMTP Add` *`Server`* `[Account] [Password]`, where *`Server`* is the host name of the target SMTP server that is used to send emails. `[Account]` and `[Password]` are optional parameters to identify the name of the account and the account password if authentication is required.

For more information, see the related customer documentation of your appliance.

Table 1-2 lists the fields from the **SMTP** section of the NetBackup Appliance Web Console.

Table 1-2 SMTP Server Configuration settings

Fields	Description
SMTP Server	Enter the SMTP (Simple Mail Transfer Protocol) Server host name. Notifications of the alerts that are generated in Appliance are sent using this SMTP server. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.
Software Administrator Email	Enter the email ID of the software administrator, to receive software alerts that are specific to the Veritas NetBackup Appliance software. This email ID that you designate receives alerts for the following software conditions: ■ Host information such as: ■ Disk information. ■ Overall backup status. ■ Results of last seven backups for each client. ■ An email of your catalog backup disaster recovery file. ■ A patch installation success report.
Hardware Administrator Email	Enter the email ID of the hardware administrator, to receive hardware alerts that are specific to the Veritas NetBackup Hardware Appliance. For example, hardwareadmin@usergroup.com for more information about potential hardware alerts.
Sender Email	Enter the email ID to receive any replies to the alerts or the reports that are sent by the Appliance.
SMTP Account	Enter the user name to access the SMTP account. **Note:** You maybe asked to enter a user name as some SMTP servers may require user name and password credentials to send an email.
Password	Enter the password for the above mentioned SMTP user account. **Note:** You maybe asked to enter a password as some SMTP servers may require user name and password credentials to send an email.

You can configure this server to send email reports to a proxy server or to the Veritas Call Home server.

The following describes the supported proxy servers:

- Squid

- Apache
- TMG

Note: NTLM authentication in the proxy configuration is also supported.

Starting with NetBackup Appliance 2.6.1.1, all email notifications that get generated by the appliance use the same SMTP settings. These emails include hardware monitoring notifications and NetBackup job notifications. The configuration settings are located under **Settings > Notification > Alert Configuration** in the NetBackup Appliance Web Console or `Main_Menu > Settings > Alerts` in the NetBackup Appliance Shell Menu. These settings override any previous SMTP setup you may have previously used to send NetBackup job notifications.

Note: If you had already configured the appliance SMTP settings before you upgraded to NetBackup Appliance 2.6.1.1, you may need to re-save the configuration in order for NetBackup to use it. In the NetBackup Appliance Web Console, go to **Settings > Notification > Alert Configuration** and click **Save**. Or in the NetBackup Appliance Shell Menu, go to `Main_Menu > Settings > Alerts` and resubmit the `SMTP` and `SenderID` settings.

Configuring Call Home

Table 1-3 lists the fields from the **Call Home Configuration** section.

Table 1-3 Call Home Configuration settings

Fields	Description
Enable Call Home	Select this check box to enable Call Home alert configuration.
Enable Proxy Server	Select this check box to enable proxy.
Enable Proxy Tunneling	Select this check box if your proxy server supports SSL tunneling.
Proxy Server	Enter the name of the proxy server.
Proxy Port	Enter the port number of the proxy server.
Proxy Username	Enter the user name to log into the proxy server.
Proxy Password	Enter the password for the user name to log into the proxy server.

When Call Home is enabled, you can test whether or not Call Home is working correctly by clicking the **Test Call Home** option that is available below the Call Home configuration settings.

Note: The **Test Call Home** option is active on the NetBackup Appliance Web Console only when Call Home is enabled.

The following describes the supported proxy servers:

- Squid
- Apache
- TMG

NTLM is the supported authentication method for Call Home proxy settings.

Configuring Alert Configuration settings

This section provides the procedure to configure the SNMP, SMTP, and Call Home server settings using the **Settings > Notification > Alert Configuration** page.

To configure the SNMP, SMTP, and Call Home server settings

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Notification > Alert Configuration**.

   The system displays the **Alert Configuration** page.

   The **Alert Configuration** page is divided into three sections to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.
3. In the **Notification Interval** field enter the time interval in minutes between two subsequent notifications, for **SNMP**, **SMTP**, and **Call Home** alert configurations.
4. Enter the SNMP settings in the provided fields. A description of the SNMP parameters is available in Table 1-1.
5. Enter the SMTP settings in the provided fields. A description of the SMTP parameters is available in Table 1-2.

   The appliance uses the global server settings to send email notifications to the SMTP server that you specify.
6. Enter the Call Home settings in the provided fields. A description of the Call Home parameters is available in Table 1-3.
7. Click **Save**, to save the SNMP, SMTP, and Call Home settings.

About email notification

An Appliance has the ability to send an email to a local administrator when a hardware failure is detected. You can use the **Settings > Notification > Alert Configuration** page of the NetBackup Appliance Web Console to configure the email address that you want to use for hardware failure notifications. You can also use the command from the NetBackup Appliance Shell Menu. The contents of the email identifies the type of hardware failure that occurred and the status of the failure.

For complete information about how to configure email addresses using the NetBackup Appliance Shell Menu, refer to the related customer documentation for your appliance.

The following is an example of an email notification that is sent in case of any hardware failures.

About this guide

This guide introduces the SNMP community traps that are used on the Veritas NetBackup Appliances with the software version 3.0.

This guide also provides procedures to troubleshoot some of the hardware SNMP alerts that you receive.

This guide helps you to perform following tasks:

- Locate the hardware trap with the unique Object Identification (OID).
- Configure the appliance to receive SNMP notifications when an error occurs.
- Locate the relevant information to identify the core problem by referencing to the relevant hardware traps.
- Resolve the hardware issues by implementing the procedures.

Note: If you receive alerts from a SNMP trap that is not listed in this guide, contact Veritas Technical Support for assistance.

Chapter 2

SNMP hardware traps

This chapter includes the following topics:

vrtsadapterTrap

OID: 1.3.6.1.4.1.48328.3.9.1.14

Note: The `vrtsadapterTrap` applies only to the NetBackup 52xx Appliance.

Description

The `vrtsadapterTrap` monitors the status of the NetBackup 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 > Hardware** page of the web console.

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

Table 2-1 Next steps for the `vrtsadapterTrap`

What happened	What to do now
If the **Adapter Status** is **NOT OK**, the adapter has failed.	Contact Veritas 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 Veritas Support for assistance.
5200/5220 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 Veritas Support to replace the adapter BBU.

vrtsbbuTrap

OID: 1.3.6.1.4.1.48328.3.9.1.19

Note: The `vrtsbbuTrap` applies only to the NetBackup 5330 and later appliances.

Description

The `vrtsbbuTrap` monitors the status of the Primary Storage Shelf Battery Backup Unit (BBU) of your appliance. If you receive an alert, it means that the BBU has experienced an error and could cause a performance drop for the storage system.

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 > Hardware** page of the Web Console of your appliance.

Based on the information from the SNMP trap and the email alert, take one of the following actions:

Table 2-2 Next steps for the `vrtsbbuTrap`

What happened	What to do now
If the BBU **Status** is **Battery expired** or **Near expiration**, the BBU has expired or is about to expire.	Contact Veritas Support to replace the BBU.
If the BBU **Status** is **Battery over temperature**, the BBU has exceeded the maximum temperature threshold.	Contact Veritas Support for assistance.
If the BBU **State** is **Warning**, and the **Status** is **Battery learning** or **Battery maintenance charging**, the BBU is in a learn cycle or a maintenance charge cycle.	Wait for the learn cycle or the maintenance charge cycle to complete. If the warning persists, contact Veritas Support for assistance.
If the BBU **State** is **Failed**, and the **Status** is **Failed** or **Battery replacement required**, the BBU is not functional.	Contact Veritas Support to replace the BBU.
If the BBU **State** is **Failed**, and the **Status** is **Removed**, the BBU is not present.	Contact Veritas Support for assistance.

Table 2-2 Next steps for the `vrtsbbuTrap` *(continued)*

What happened	What to do now
If the BBU **State** is **Failed**, and the **Status** is **Not authorized** or **Battery settings mismatch**, an issue exists with the configuration.	Contact Veritas Support for assistance.
If the BBU **State** is **Failed**, and the **Status** is **Not available**, the firmware was unable to report the current status.	Wait 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 Veritas Support for assistance.

vrtsconnectionTrap

OID: 1.3.6.1.4.1.48328.3.9.1.20

Note: The `vrtsconnectionTrap` applies only to the NetBackup 5330 and later appliances.

Description

The `vrtsconnectionTrap` monitors the status of the connections between the appliance, the Primary Storage Shelf, and the Expansion Storage Shelf. If you receive an alert, it means that one or more of the cables is not installed correctly or is not functional.

Resolution

Check the Fibre Channel connections between the appliance and the primary shelf and the SAS connections between the primary shelf and the expansion shelf. If all cables are installed correctly and are functional, contact Veritas Support for assistance.

vrtscpuTrap

OID: 1.3.6.1.4.1.48328.3.9.1.7

Description

The `vrtscpuTrap` 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 > Hardware** page of the Web Console of your appliance.

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

Table 2-3 Next steps for the `vrtscpuTrap`

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 Veritas Support for assistance.
If the CPU **State** is **Failed**, and the **Status** is anything other than **OK** or **ProcPresent**, the status of the CPU is unknown.	Contact Veritas Support for assistance.
5230 and 5330 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 Veritas Support for assistance.
5230 and 5330 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 Veritas Support for assistance.

vrtsdiskTrap

OID: 1.3.6.1.4.1.48328.3.9.1.8

Description

The `vrtsdiskTrap` 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 > Hardware** page of the Web Console of your appliance.

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

Table 2-4 Next steps for the `vrtsdiskTrap`

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 Veritas Support. Let them know of the error, with the following message: Import foreign configuration
5220 and 5230 only: If the **State** of disk 7 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 Veritas 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 Veritas Support to replace the faulty disk.
If the disk **State** is **Failed**, and the **Status** is **Offline**, the disk is offline.	Contact Veritas 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.
5330 only: If the disk **State** is **Failed**, and the **Status** is **Unresponsive**, the disk is present but unresponsive.	Contact Veritas Support for assistance.
5330 only: If the disk **State** is **Failed**, and the **Status** is **Incompatible**, the disk is not compatible with the appliance.	Replace the disk with a compatible disk. If you need assistance, contact Veritas Support for assistance.
5330 only: If the disk **State** is **Failed**, and the **Status** is **Loss of redundancy**, the disk does not have redundant access.	Contact Veritas Support for assistance.

vrtsfanTrap

OID: 1.3.6.1.4.1.48328.3.9.1.3

Description

The `vrtsfanTrap` 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 > Hardware** page of the Web Console of your appliance.

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

Table 2-5 Next steps for the `vrtsfanTrap`

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 Veritas Support to replace the fan.
If the fan **State** is **Failed**, the fan is missing or has failed.	Contact Veritas Support to replace the fan.

vrtsfirmwareTrap

OID: 1.3.6.1.4.1.48328.3.9.1.15

Description

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

vrtsnetworkcardTrap

OID: 1.3.6.1.4.1.48328.3.9.1.17

Description

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

vrtspartitionTrap

OID: 1.3.6.1.4.1.48328.3.9.1.21

Description

The `vrtspartitionTrap` monitors the status of the appliance storage partitions. If you receive an alert, it means that the partition's disk usage is too high, or it 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 > Hardware** page of the Web Console of your appliance.

Based on the information from the SNMP trap and the email alert, take one of the following actions:

Table 2-6 Next steps for the `vrtspartitionTrap`

What happened	What to do now
The partition usage has exceeded critical threshold: full capacity imminent.	Cleanup the partition and re-check status. If the issue is not resolved, contact Veritas Support for assistance.
The partition usage has exceeded warning threshold and will soon reach full capacity.	Cleanup the partition and re-check status. If the issue is not resolved, contact Veritas Support for assistance.
The partition is degraded.	Check if there are any disk errors or a power supply interruption to one or more storage shelves. If the issue persists, contact Veritas Support for assistance.
The partition is not accessible.	Check if there are any disk errors or a power supply interruption to one or more storage shelves. If the issue persists, contact Veritas Support for assistance.

vrtspowerTrap

OID: 1.3.6.1.4.1.48328.3.9.1.4

Description

The `vrtspowerTrap` 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 > Hardware** page of the web console.

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

Table 2-7 Next steps for the `vrtspowerTrap`

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 Veritas 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 Veritas 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 Veritas 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 Veritas Support for assistance.

vrtsraidgroupTrap

OID: 1.3.6.1.4.1.48328.3.9.1.9

Description

The `vrtsraidgroupTrap` 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 > Hardware** page of the wen console.

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

Table 2-8 Next steps for the `vrtsraidgroupTrap`

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 Veritas 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.	Check the disk status. If a disk has failed, contact Veritas Support to replace the faulty disk. 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 Veritas Support.
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 Veritas Support for assistance.
If the RAID **State** is **Failed**, and the **Status** is also **Failed**, the RAID is offline or is not functional.	Contact Veritas Support for assistance.

Table 2-8 Next steps for the `vrtsraidgroupTrap` *(continued)*

What happened	What to do now
If the RAID **State** is **Failed**, and the **Status** is **Unknown**, 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 Veritas Support for assistance.
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 Veritas 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 Veritas Support for assistance.
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 Veritas Support for assistance.

vrtsstoragestatusTrap

OID: 1.3.6.1.4.1.48328.3.9.1.22

Note: The `vrtsstoragestatusTrap`applies only to the NetBackup 53xx appliances with software release 2.7.1, 2.7.2 or 2.7.3.

Description

The `vrtsstoragestatusTrap` monitors the status of the appliance storage system as a whole. If you receive an alert, it means that the storage system has experienced an error.

Note: A **Storage Status** error or warning cannot be acknowledged to suppress notifications.

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 > Hardware** page of the administrative web UI.

Based on the information from the email alert, take one of the following actions:

To troubleshoot this issue in the shell menu

1. Use the command `Monitor > Hardware ShowHealth`.
2. Browse to the **Primary Storage Shelf** section and **Expansion Storage Shelf** section.
3. Verify the status of all the components.
   - If you locate an error, see the related documentation for your appliance to troubleshoot.
   - If you found no error, while the storage status continues to be not optimal, contact Veritas Technical Support for more assistance.

To troubleshoot this issue in the web console

1. Browse to the **Monitor > Hardware** page.
2. Verify the status of all the components in the Summary of the NetBackup Storage Shelf.
   - If you locate an error, click the hardware component icon for details and find the troubleshooting information in the Veritas Help Center.
   - If you found no error, while the storage status continues to be not optimal, contact Veritas Technical Support for more assistance.

vrtssystemName

OID: 1.3.6.1.4.1.48328.3.9.1.1

Description

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

vrtstemperatureTrap

OID: 1.3.6.1.4.1.48328.3.9.1.6

Description

The `vrtstemperatureTrap` 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 > Hardware** page of the web console.

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

Table 2-9 Next steps for the `vrtstemperatureTrap`

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 10 minutes and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Veritas Support for assistance.
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: ■ Intake Vent Temperature: 64 degrees C ■ Outtake Vent Temperature: 85 degrees C ■ P1 and P2 Therm Margins: -15 degrees C	Check the status of the appliance fans. Check the temperature of the appliance's environment. If both are normal, contact Veritas Support for assistance.
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: ■ Intake Vent Temperature: 0 degrees C ■ Outtake Vent Temperature: 0 degrees C ■ P1 and P2 Therm Margins: -128 degrees C	Wait 10 minutes and re-check the status. If the issue is resolved, you can ignore the failure. If the issue is not resolved, contact Veritas Support for assistance.

vrtsvolumeTrap

OID: 1.3.6.1.4.1.48328.3.9.1.18

Note: The `vrtsvolumeTrap` applies only to the NetBackup 53xx Appliance.

Description

The `vrtsvolumeTrap` monitors the status of the appliance volumes. If you receive an alert, it means that the volume is not in an optimal state due to disk errors.

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 > Hardware** page of the web console.

Based on the information from the SNMP trap and the the email alert sent to your configured address, you need to contact technical support for assistance if your appliance encounter any volume related errors.

vrtsenclosurediskTrap

OID: 1.3.6.1.4.1.48328.3.9.1.13

Description

The `vrtsenclosurediskTrap` 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 > Hardware** page of the web console.

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

Table 2-10 Next steps for the `vrtsenclosurediskTrap`

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 Veritas Support. Let them know of the error, with the following message: Import foreign configuration

Table 2-10 Next steps for the `vrtsenclosurediskTrap` *(continued)*

What happened	What to do now
Symantec Storage Shelf (52xx) only: 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 Veritas 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 Veritas Support to replace the faulty disk.
If the disk **State** is **Failed**, and the **Status** is **Offline**, the disk is offline.	Contact Veritas 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.

vrtsenclosurefanTrap

OID: 1.3.6.1.4.1.48328.3.9.1.10

Description

The `vrtsenclosurefanTrap` 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 > Hardware** page of the web console.

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

Table 2-11 Next steps for the `vrtsenclosurefanTrap`

What happened	What to do now
If the fan **State** is **Warning**, the fan is running slower than the low threshold of 2000 rpm. **Note:** The low threshold of 2000 rpm applies to the Veritas Storage Shelf (52xx appliance) only. The `vrtsenclosurefanTrap` does not include a low threshold value for the NetBackup 5330 Appliance Primary or Expansion Storage Shelf.	Check the system temperature. Check the power supply. If both are normal, contact Veritas Support to replace the fan.
If the fan **State** is **Failed**, the fan is missing or has failed.	Contact Veritas Support to replace the fan.

vrtsenclosurepowerTrap

OID: 1.3.6.1.4.1.48328.3.9.1.11

Description

The `vrtsenclosurepowerTrap` 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 Veritas Support to replace the power supply.

vrtsenclosuretemperatureTrap

OID: 1.3.6.1.4.1.48328.3.9.1.12

Description

The `vrtsenclosuretemperatureTrap` 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 > Hardware** page of the web console.

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

Table 2-12 Next steps for the `vrtsenclosuretemperatureTrap`

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 Veritas Support for assistance.
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 52xx appliance storage shelf temperature sensors: ■ I/O Modules: 75 degrees C ■ Backplanes: 51 degrees C ■ PSUs: 75 degrees C **Note:** The high threshold values apply to the Veritas Storage Shelf (52xx appliance) only. The `vrtsenclosuretemperatureTrap` does not include a high threshold value for the NetBackup 53xx Appliance Primary or Expansion Storage Shelf.	Check the status of the storage shelf fans. Check the temperature of the storage shelf's environment. If both are normal, contact Veritas Support for assistance.

vrtsdimmTrap

OID: 1.3.6.1.4.1.48328.3.9.1.23

Description

The `vrtsdimmTrap` monitors the status of the DIMM (Dual In-line Memory Module). If you receive an alert, it means that one of the DIMM's is not in an optimal state or may not have been in an optimal state previously.

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 > Hardware** page of the web console.

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. (for e.g Slot ID, Uncorrectable error count). You can also check the `Monitor > Hardware ShowHealth Appliance DIMM` command of the shell menu.

Based on the information from the SNMP trap, the email alert, or the `Monitor> Hardware ShowHealth Appliance DIMM` command, take the following actions:

Table 2-13 Next steps for the `vrtsdimmTrap`

What happened	What to do now
If the DIMM **Status** is **Failed**, the DIMM has encountered an uncorrectable error and needs to be replaced.	Contact Veritas Support to replace the DIMM.

vrtsiscsiTrap

OID: 1.3.6.1.4.1.48328.3.9.1.24

Description

The `vrtsiscsiTrap` monitors the iSCSI connections for the NetBackup 5240 appliance. This applies only to configuration H of the NetBackup 5240 appliance. If you receive this alert, it means that one or more iSCSI sessions with the targets got disconnected.

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 run the **Settings > iSCSI > Target Show Connected** command and check the **Status** column and verify if the status is **Offline**.

Based on the information from the SNMP trap, the email alert, or the **Settings > iSCSI > Target Show Connected** command, take the following actions:

Table 2-14 Next steps for the `vrtsiscsiTrap`

What happened	What to do now
One or more iSCSI sessions with the target were lost or disconnected.	Check for any network issues or current statistics. Run the `Settings > iSCSI > Interface Show` command to view the properties of the iSCSI interface. Check if the properties like IP address, Netmask etc. are valid. You can also run the `Settings > iSCSI > Target Show Connected` command to view the connected targets. To connect to a discovered target, run the `Settings > iSCSI > Target Connect` command.

vrtsethernetTrap

OID: 1.3.6.1.4.1.48328.3.9.1.25

Description

The vrtsethernetTrap monitors the 10Gb Ethernet/iSCSI card on the NetBackup appliance for any unsupported Small Form-Factor Pluggable (SFP) modules. If you receive this alert, it means that one or more unsupported SFP modules has been inserted in the 10Gb Ethernet/iSCSI card.

Resolution

Check the SNMP trap or the email alert that you received for additional information to help you determine the exact issue that occurred. Inspect the current SFP's and check if they are manufactured by QLogic. Only QLogic SFP+ modules are supported. Install QLogic SFP+ modules in the 10Gb Ethernet/iSCSI card as needed.

Based on the information from the SNMP trap, the email alert, or after inspecting the physical SFP module, take the following actions:

Table 2-15 Next steps for the `vrtsethernetTrap`

What happened	What to do now
One or more unsupported SFP modules have been inserted in the 10Gb Ethernet/iSCSI card.	Install a supported QLogic SFP+ module in the 10Gb Ethernet/iSCSI card.

Appendix A

Management Information Base (MIB) file contents

This appendix includes the following topics:

The Management Information Base (MIB) file

The Management Information Base (MIB) file on your appliance contains the notification traps that are configured to monitor the appliance.

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

Note: Although the MIB file includes software traps, they are not used. The appliance does not currently send any software traps.

Note: Note the status of the traps, only traps with the "current" status are monitored, traps with the "obsolete" status are not functional for the current appliance release.

The Management Information Base (MIB) file