NETAPP TECHNICAL REPORT

NetApp Storage Monitoring Using HP OpenView

Vishwas Venkatesh, NetApp

July 2008 | TR-3688

This technical report will briefly explain the integration approaches for monitoring NetApp® storage using HP OpenView software. It will primarily address the discovery and monitoring features provided by HP OpenView and how to integrate them with NetApp storage.

TABLE OF CONTENTS

1 OVERVIEW OF HP OPENVIEW NETWORK NODE MANAGER

HP OpenView Network Node Manager is the market-leading network management solution, providing in-depth views of the network in an intuitive graphical format. Network Node Manager (NNM) discovers network devices and provides a map to illustrate what the network actually looks like. The multilevel map indicates which devices and network segments are healthy and which areas need attention.

Network Node Manager is a manager system. It supplies managers, such as the SNMP MIB (Management Information Base) Browser or the DMI Browser, that monitor and control agent systems on your network. An agent system is a device, such as a host, gateway, server, hub, or bridge, that has interface software called an agent. An agent performs network management tasks at the request of the manager. The SNMP manager and agent communicate using the Simple Network Management Protocol (SNMP). NNM supports SNMP version 1 and Community-based SNMP version 2.

2 PURPOSE AND SCOPE

The main objective of this report is to provide a possible integration path for customers who have NNM as their management solution. This document will discuss some of the integration approaches for managing NetApp storage systems and NetCache® devices under HP OpenView Network Node Manager.

This document provides information only about NetApp Data ONTAP® SNMP information and does not include other NetApp products' SNMP information.

3 MIGRATION PATH

No automated migration path is available. However, customers can follow these approaches:

Approach 1: Customers can download the SNMP MIB from http://now.NetApp.com/NOW/download/tools/mib and can load the MIB in the HP OpenView.

Approach 2: Customers who have Operations Manager can enable trap forwarding and forward SNMP traps to HP OpenView.

4 APPROACH 1

Customers can download the SNMP MIB from http://now.NetApp.com/NOW/download/tools/mib and can load the MIB in HP OpenView.

This section describes how to configure HP OpenView Network Node Manager to manage SNMP devices manufactured by NetApp. It shows where to obtain files such as MIBs and how to integrate these with HP OpenView NNM.

Approach 1 is organized as follows:

- Section 1: Describes how the autodiscovery process within NNM is able to find NetApp devices.

- Section 2: Deals with loading NetApp MIBs.

- Section 3: Describes how to configure NNM to perform customized actions on receipt of NetApp traps.

- Section 4: Describes how to configure NNM to poll NetApp devices and how to configure NNM to perform customized actions depending on the results of the poll.

4.1 SECTION 1: USING THE AUTODISCOVERY PROCESS TO FIND NETAPP DEVICES

The autodiscovery process within NNM will be able to find NetApp devices. NNM performs a first-level discovery of the network—IP and IPX devices. It uses ARP and ping discovery techniques to fill its autodiscovery database with a list of IP and IPX devices. If the device type has a unique SysObjId (part of MIB II) and if it is made available to it, NNM will be able to recognize the manufacturer of the devices. The

NetApp devices would fall into this category. This whole process is considered to be the first level of discovery.

Typically, devices are discovered by NNM depending on the sysObjectID reported by the particular device. Alternatively, devices may be manually added to the NNM map.

The steps involved in configuring NNM to recognize NetApp devices are:

- Prepare the NNM Oid_to_Type File.
- Prepare the NNM Ovw_Fields File.
- Prepare the NNM Snmp_Fields File.

4.2 NNM OID TO TYPE FILE

The NNM Oid_to_Type file is used in NNM to set the value of the vendor and SNMP agent fields for the NetApp device.

Note: The entry made in the Oid_to_Type file must match the entries made in the Ovw_Fields and SNMP_Fields files.

Back up and open the following file:

1. HPOpenview\conf\oid_to_type

Add the required OID entries to the end of the file. A sample addition of NetApp OIDs is shown below:

```
#
# NetApp Agents
#
1.3.6.1.4.1.789.1.5.11.1.3.1:       NetApp aggrFSID
1.3.6.1.4.1.789.1.5.11.1.9.1:       NetApp aggrFlexvollist
1.3.6.1.4.1.789.1.5.11.1.1.1:       NetApp aggrIndex
1.3.6.1.4.1.789.1.5.11.1.2.1:       NetApp aggrName
1.3.6.1.4.1.789.1.5.12.0:            NetApp aggrNumber
1.3.6.1.4.1.789.1.5.11.1.7.1:       NetApp aggrOptions
1.3.6.1.4.1.789.1.5.11.1.4.1:       NetApp aggrOwningHost
1.3.6.1.4.1.789.1.5.11.1.5.1:       NetApp aggrState
1.3.6.1.4.1.789.1.5.11.1.6.1:       NetApp aggrStatus
1.3.6.1.4.1.789.1.5.11.1.10.1: NetApp aggrType
1.3.6.1.4.1.789.1.5.11.1.8.1:       NetApp aggrUUID
1.3.6.1.4.1.789.1.8.2.3.4.1.2.1: NetApp amAddress
1.3.6.1.4.1.789.1.8.2.3.4.1.1.1: NetApp amIndex
1.3.6.1.4.1.789.1.8.2.3.2.0:NetApp amMonitor
1.3.6.1.4.1.789.1.8.2.3.3.0:NetApp amMonitorString
1.3.6.1.4.1.789.1.8.2.3.1.0:NetApp amNumber
1.3.6.1.4.1.789.1.8.2.3.4.1.3.1:    NetApp amPort
1.3.6.1.4.1.789.1.8.2.3.4.1.4.1:    NetApp amStatus
```

4.3 OVW FIELDS FILE

The Ovw fields file contains the values for the vendor fields.

Back up and open the following file:

HPOpenview\fields\C\ovw_fields

Add an entry for NetApp as shown:

```
        Field "vendor" {
                Type    Enumeration;
                Flags   capability, general, locate;
                Enumeration "Unset",
                        "Hewlett-Packard",
                        "HP/Apollo",
                        "3Com",
                        "ACC",
                        "Allied Telesyn",
                        "Axon Networks",
                        "Cayman",
                        "cisco Systems",
                        "CMC",
                        "Data General",
                        "DEC",
                        "Emulex",
                        "Fibronics",
                        "Hughes",
                        "IBM",
                        "Interactive/Lachman",
                        "Microsoft",
                        "Micro Technology",
                        "MIPS",
                        "Mitsubishi Electric",
                        "NCR",
                        "NetWare",
                        "Novell",
                        “NetApp”, --------------------- new entry ---------------------------
                        "NRC",
                        "Plaintree",
                        "SGI",
                        "Sun",
                        "SynOptics",
                        "Ungermann-Bass",
                        "Wellfleet",
                        "XLNT",
                        "Xyplex"
                        ;
                }
```

4.4 SNMP FIELDS FILE

The SNMP fields file contains the values for SNMP agents:

1. Back up and open the following file: HPOpenview\fields\C\snmp_fields.
2. Add the required entries to this file. A sample addition is shown below:

```
Field "SNMPAgent" {
    Type Enumeration;
    Flags    capabilities, general, locate;
    Enumeration
        "Unset",
        "HP 3000/XL",
        "HP 386",
        "MT LANCE/NMS agent",
        "NCR Tower",
        "Netware 386 TCP/IP",
        "NetApp aggrFSID ",      ---------------new entries start------------
        "NetApp aggrFlexvollist ",
        "NetApp aggrIndex ",
        "NetApp aggrName ",
        "NetApp aggrNumber ",
        "NetApp aggrOptions ",
        "NetApp aggrOwningHost ",
        "NetApp aggrState ",
        "NetApp aggrStatus ",
        "NetApp aggrType ",
        "NetApp aggrUUID ",
        "NetApp amAddress ",     ---------------new entries finish--------
        "Novell Lantern",
        "NRC Fusion Xenix agent",
        "Xyplex Terminal Server",
        "Xyplex Remote Ethernet Bridge",
        "4BSD ISODE";
}
```

4.5 INFORM OPENVIEW OF THE UPDATES

Complete the following steps to inform NNM about the changes made:

1. Exit from all NNM sessions.
2. Stop all background processes by typing “ovstop” at the command line.
3. Start the NNM database by typing “ovstart ovd” at the command line.
4. Inform NNM of the changes by typing “ovw -fields” at the command line.
5. Restart the background processes – “ovstart –v | more.”

4.6 INTEGRATION OF NETAPP MIBS WITH OPENVIEW

A MIB is used to show the values available for an SNMP agent. The MIB is made up of a number of objects and each object may represent a feature of the agent, for example, a major alarm or an interface status. Objects may have multiple instances to represent multiple occurrences of the same object, for example, an interface status of card 1, an interface status of card 2, through to an interface status of card n.

A MIB definition file is loaded in NNM to define the objects available for a particular agent.

4.7 OBTAINING NETAPP MIBS

The NetApp MIB files, otherwise referred to as MIBs, can be downloaded from the Internet site

http://now.netapp.com/NOW/download/tools/mib.

NetApp suggests that NetApp MIBs be downloaded from http://now.netapp.com/NOW/download/tools/mib to the following NNM directory: HPOpenview\snmp_mibs\Vendor\NetAppfiles.

4.8 SECTION 2: LOADING NETAPP MIBS

After you download the MIBs, you must compile or load them into the NNM by following these steps:

1. Choose Options: Load/Unload Mibs: SNMP to start the NNM MIB compiler.
2. Choose Load.
3. Select the Vendor/NetApp directory.
4. Select the MIB of interest and choose Open or double-click on the file.

4.9 SECTION 3: CONFIGURING OPENVIEW NNM FOR NETAPP TRAP EVENTS

NetApp agents can be configured to send traps to NNM. NNM is capable of receiving SNMP traps and DMI indications from SNMP-capable devices and DMI-capable devices, respectively. NNM processes these traps and indications and displays them in the NNM Event Browser. The status of the symbol representing the device that sent the event can also be changed to reflect the severity of the event.

4.10 SETTING THE TRAP DESTINATION FOR THE STORAGE SYSTEM

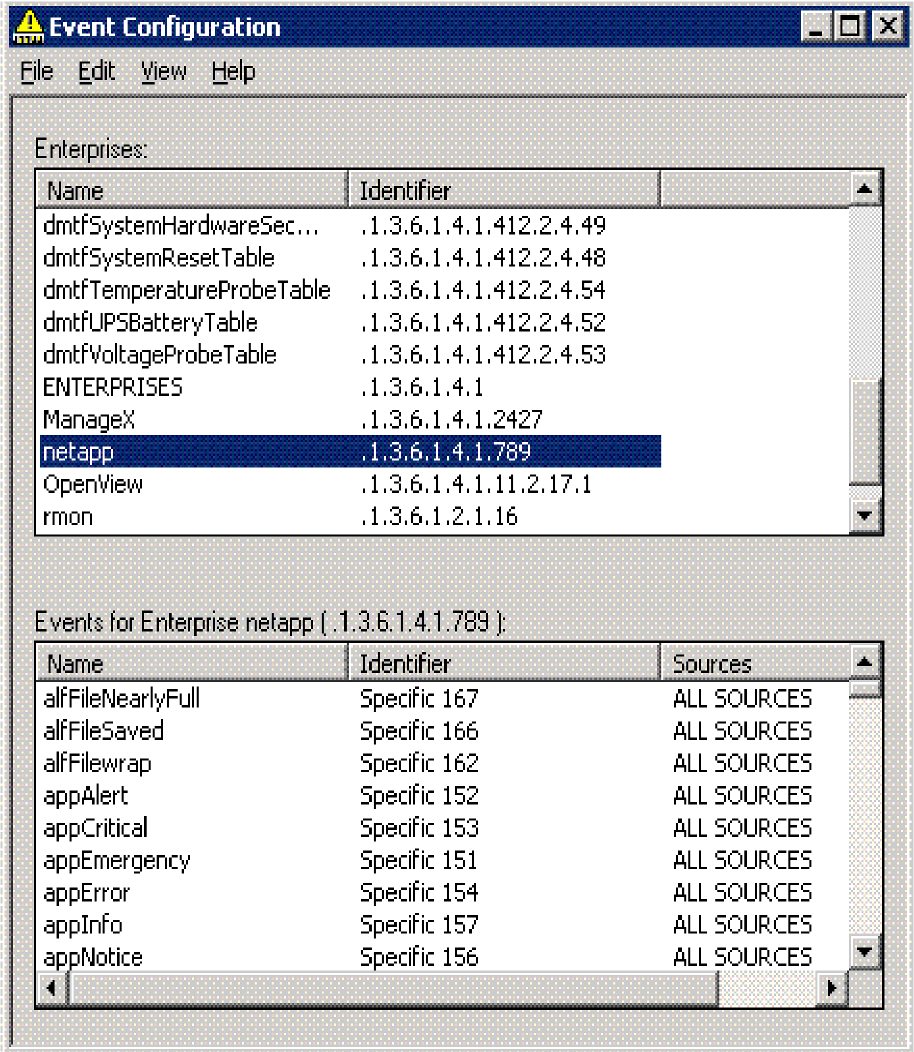
The storage administrator is required to set the trap destination for each storage system. To set the trap destination for a storage system, complete the following steps.

Step	Action
1	To access the storage system for which you want to set the trap destination, right-click the discovered node icon and select Telnet Session. Alternatively, the storage administrator can telnet directly to the IP address of the storage system.
2	Log in to the storage system as root.
3	Enter the following command: snmp traphost add { host_name | ip_address } host_name is the name of the workstation running NNM. ip_address is the IP address of the workstation running NNM.

The steps below discuss the programming of NNM to process the reception of enterprise-specific traps or events from NetApp agents.

1. Choose Options: Event Configuration to start the NNM Event Configuration Manager.

2. In the Enterprises section choose NetApp (Figure 1.0).



Enterprises:

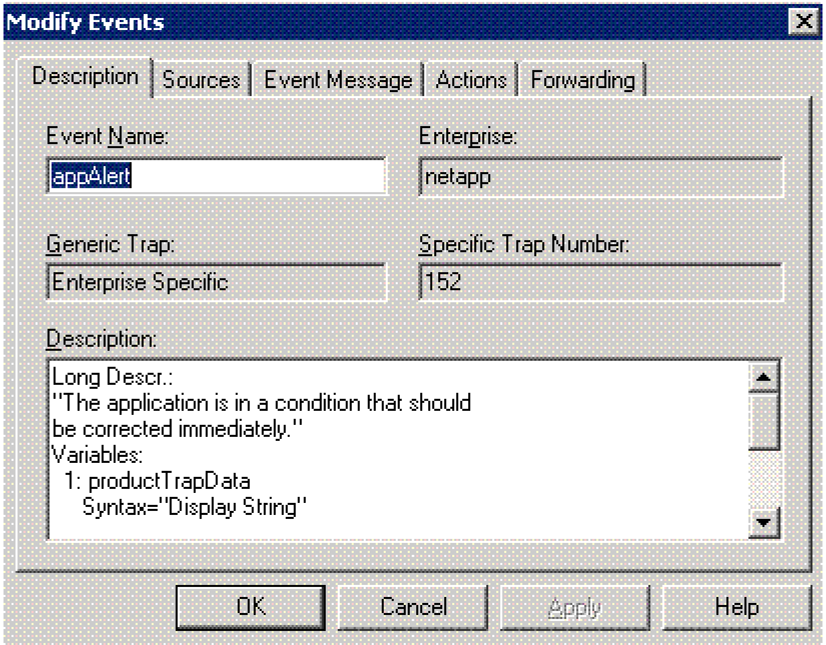
Name	Identifier
dmtfSystemHardwareSec...	.1.3.6.1.4.1.412.2.4.49
dmtfSystemResetTable	.1.3.6.1.4.1.412.2.4.48
dmtfTemperatureProbeTable	.1.3.6.1.4.1.412.2.4.54
dmtfUPSBatteryTable	.1.3.6.1.4.1.412.2.4.52
dmtfVoltageProbeTable	.1.3.6.1.4.1.412.2.4.53
ENTERPRISES	.1.3.6.1.4.1
ManageX	.1.3.6.1.4.1.2427
netapp	.1.3.6.1.4.1.789
OpenView	.1.3.6.1.4.1.11.2.17.1
rmon	.1.3.6.1.2.1.16

Events for Enterprise netapp (.1.3.6.1.4.1.789):

Name	Identifier	Sources
alfFileNearlyFull	Specific 167	ALL SOURCES
alfFileSaved	Specific 166	ALL SOURCES
alfFilewrap	Specific 162	ALL SOURCES
appAlert	Specific 152	ALL SOURCES
appCritical	Specific 153	ALL SOURCES
appEmergency	Specific 151	ALL SOURCES
appError	Specific 154	ALL SOURCES
appInfo	Specific 157	ALL SOURCES
appNotice	Specific 156	ALL SOURCES

Figure 1) Event configuration, NetApp enterprise.

3. In the Events for Enterprises NetApp (.1.3.6.1.4.1.789), select the object generating the enterprise-specific trap, say, appAlert.



Event Name: appAlert

Enterprise: netapp

Generic Trap: Enterprise Specific

Specific Trap Number: 152

Description:

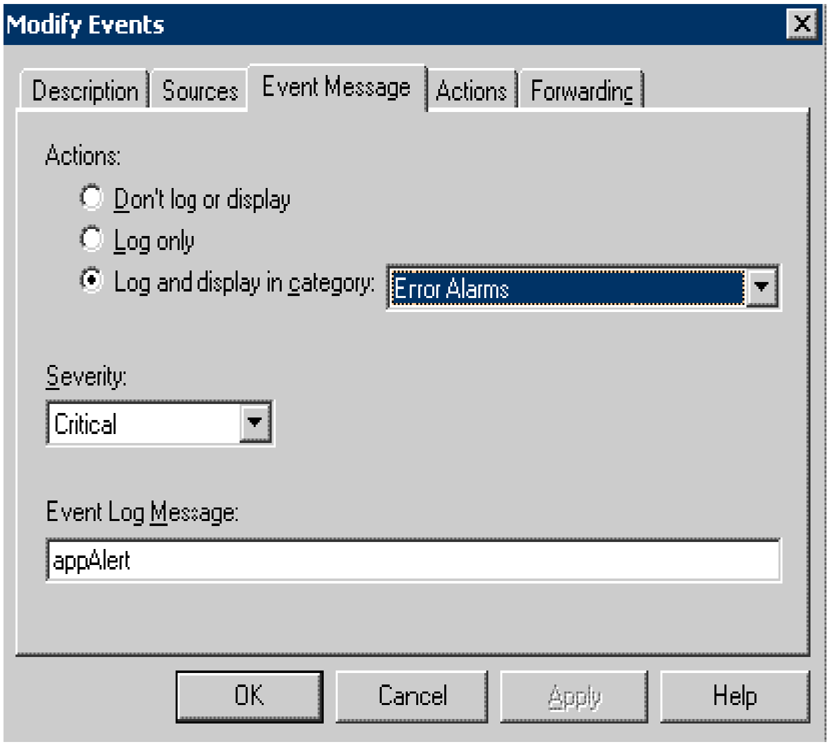
```
Long Descr.:
"The application is in a condition that should
be corrected immediately."
Variables:
  1: productTrapData
     Syntax="Display String"
```

Figure 2) Event configuration, modify events.

This causes the Modify Events Manager to start. The following items can be edited:

• Sources: Choose the source address of the device that can send the trap to activate this event.

• Event Message: Select where in NNM the event will be displayed, the severity of the event, and the event log message.



Actions:

○ Don't log or display

○ Log only

● Log and display in category: Error Alarms

Severity: Critical

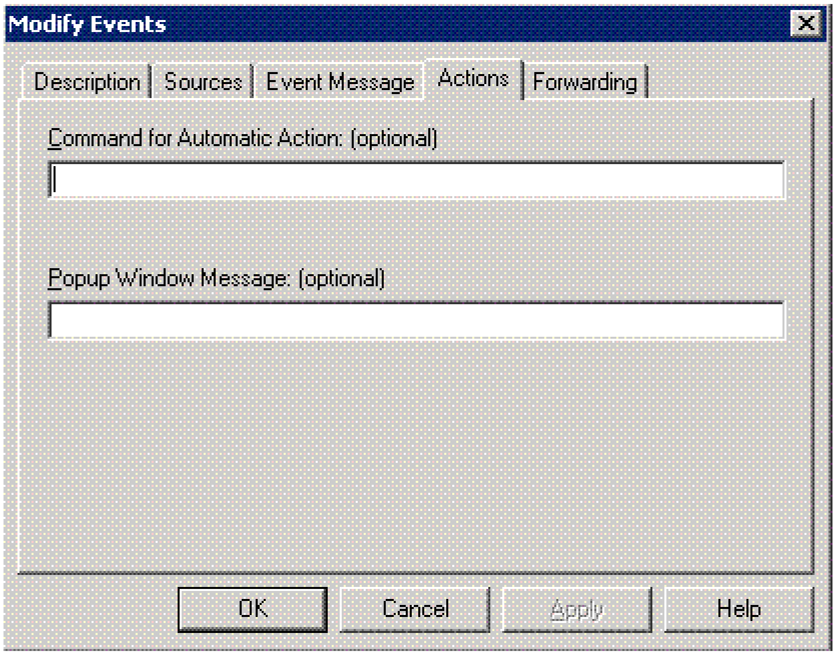
Event Log Message: appAlert

Figure 3) Event configuration, event message.

Event Actions: SNMP events are the building blocks of network management. Thoughtful planning and use of event configuration will allow NNM to monitor your network effectively. To configure an action for specific events, complete the following steps.

Note: The MIB netapp.mib for which you want to configure events must be loaded into NNM's MIB database.

Select what actions NNM will execute when the event is received.

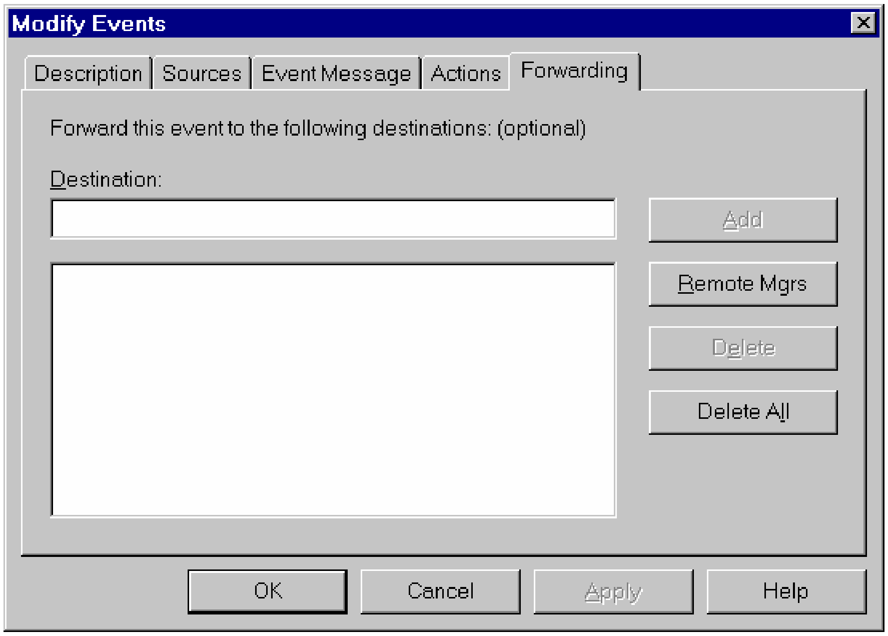


Command for Automatic Action: (optional)

Popup Window Message: (optional)

Figure 4) Event configuration, actions.

Event Forwarding: Select the management stations to forward the event to.



Forward this event to the following destinations: (optional)

Destination:

Figure 5) Event configuration, forwarding.

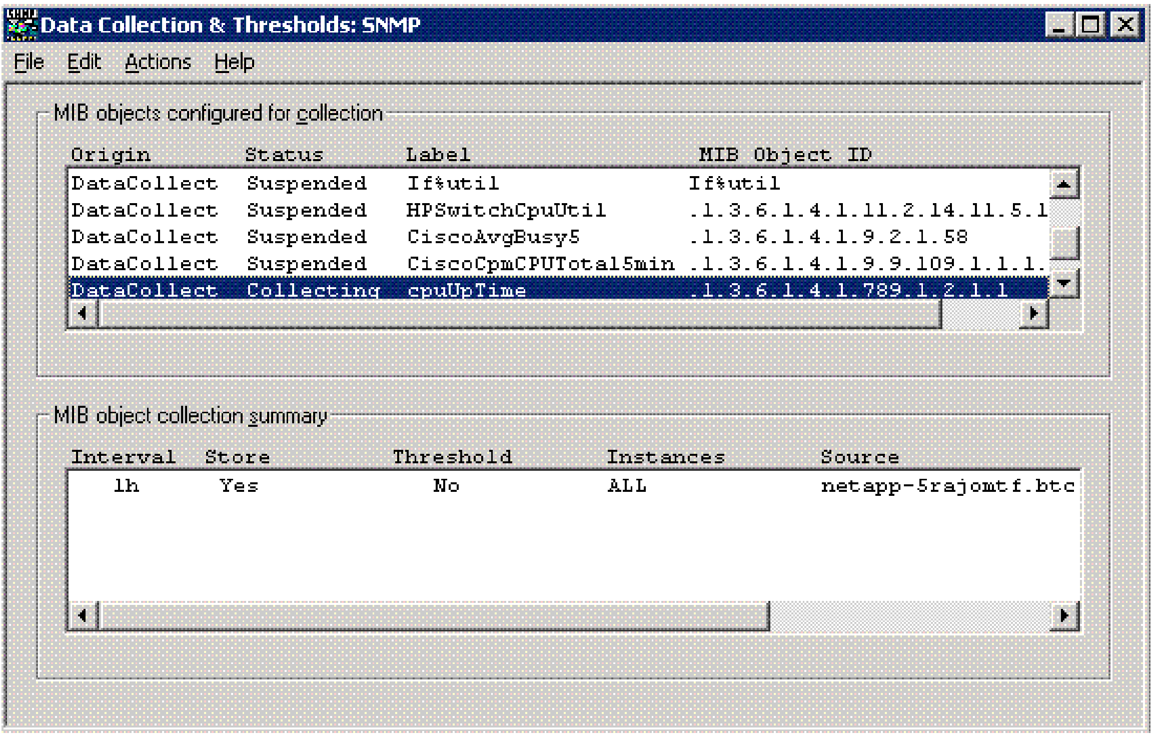
4.11 SECTION 4: CONFIGURING OPENVIEW NNM TO POLL FOR NETAPP EVENTS

NNM can be configured to periodically poll NetApp agents for the status of particular objects. This section discusses the programming of NNM to poll agents and the configuration of events based on the results of the poll.

Choose Options: Data Collection & Thresholds: SNMP.

Choose Edit: Mib Object: New.

Select the desired object, say, private.enterprises.NetApp1.sysStat.cpu.cpuUpTime.



MIB objects configured for collection

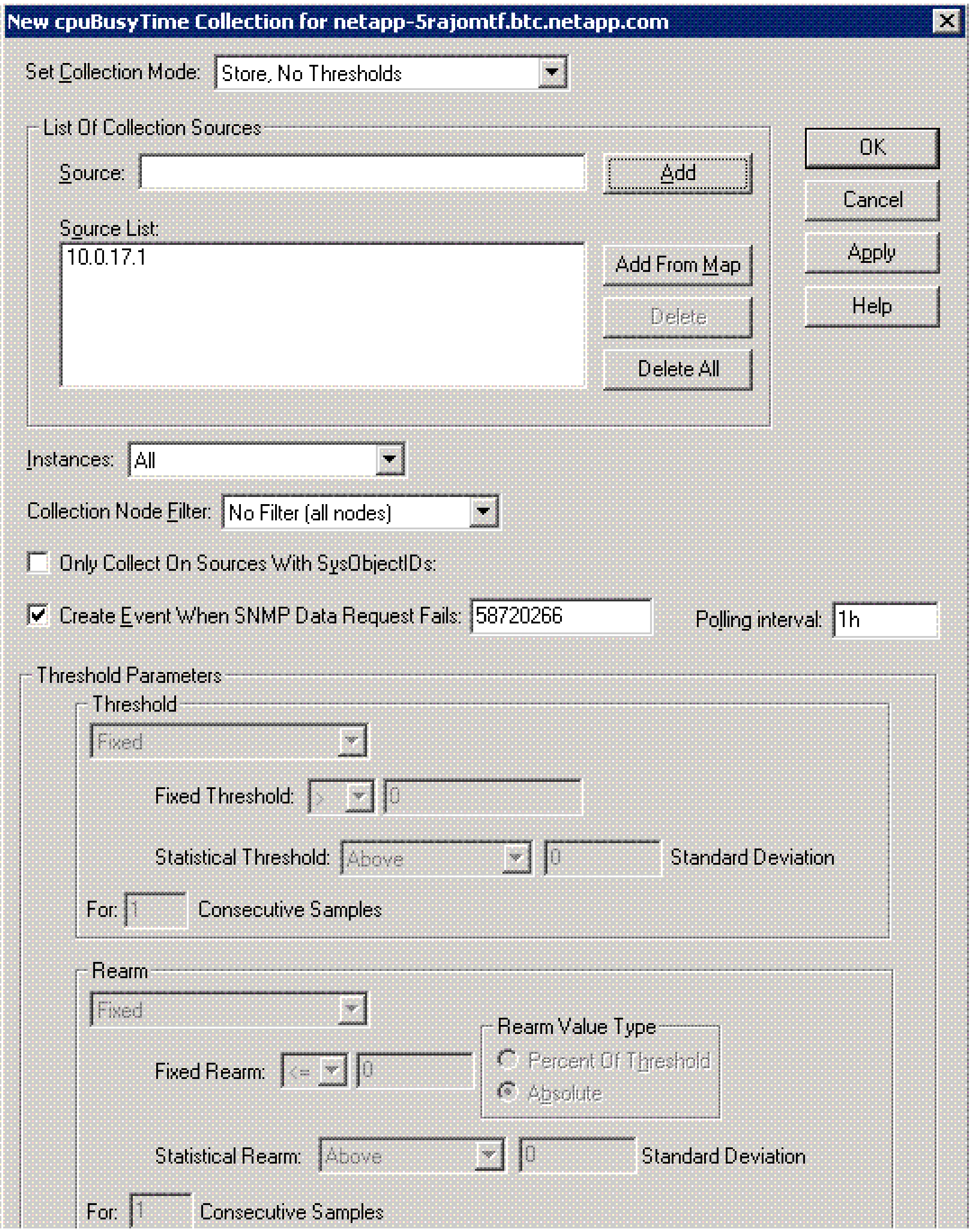
Origin	Status	Label	MIB Object ID
DataCollect	Suspended	If%util	If%util
DataCollect	Suspended	HPSwitchCpuUtil	.1.3.6.1.4.1.11.2.14.11.5.1
DataCollect	Suspended	CiscoAvgBusy5	.1.3.6.1.4.1.9.2.1.58
DataCollect	Suspended	CiscoCpmCPUTotal5min	.1.3.6.1.4.1.9.9.109.1.1.1.
DataCollect	Collecting	cpuUpTime	.1.3.6.1.4.1.789.1.2.1.1

MIB object collection summary

Interval	Store	Threshold	Instances	Source
1h	Yes	No	ALL	netapp-5rajomtf.btc

Figure 6) Data collection and thresholds.

This starts the NNM Collection Modification Manager.



New cpuBusyTime Collection for netapp-5rajomtf.btc.netapp.com

Set Collection Mode: Store, No Thresholds

List Of Collection Sources

Source:

Source List: 10.0.17.1

Instances: All

Collection Node Filter: No Filter (all nodes)

□ Only Collect On Sources With SysObjectIDs:

☑ Create Event When SNMP Data Request Fails: 58720266

Polling interval: 1h

Threshold Parameters

Threshold

Fixed

Fixed Threshold: > 0

Statistical Threshold: Above 0 Standard Deviation

For: 1 Consecutive Samples

Rearm

Fixed

Fixed Rearm: <= 0

Rearm Value Type

○ Percent Of Threshold

● Absolute

Statistical Rearm: Above 0 Standard Deviation

For: 1 Consecutive Samples

Figure 7) Collection modifications.

The following events can be configured:

- Source: the agent to which the poll will be directed
- Collection Mode: a combination of store or don’t store and check threshold or don’t check threshold
- Polling interval: the period to poll the agent
- Instances: for devices reporting multiple instances of an OID; instances can be included or excluded
- Threshold parameters: the values that will trigger threshold and alarm events
- Configure threshold and alarm events: the events executed when threshold and alarm conditions are satisfied; these actions allow the configuration of events as discussed in section 4

4.12 ACCESSING EXISTING MANAGEMENT TOOLS

The following table lists the storage system tools that are available from NNM.

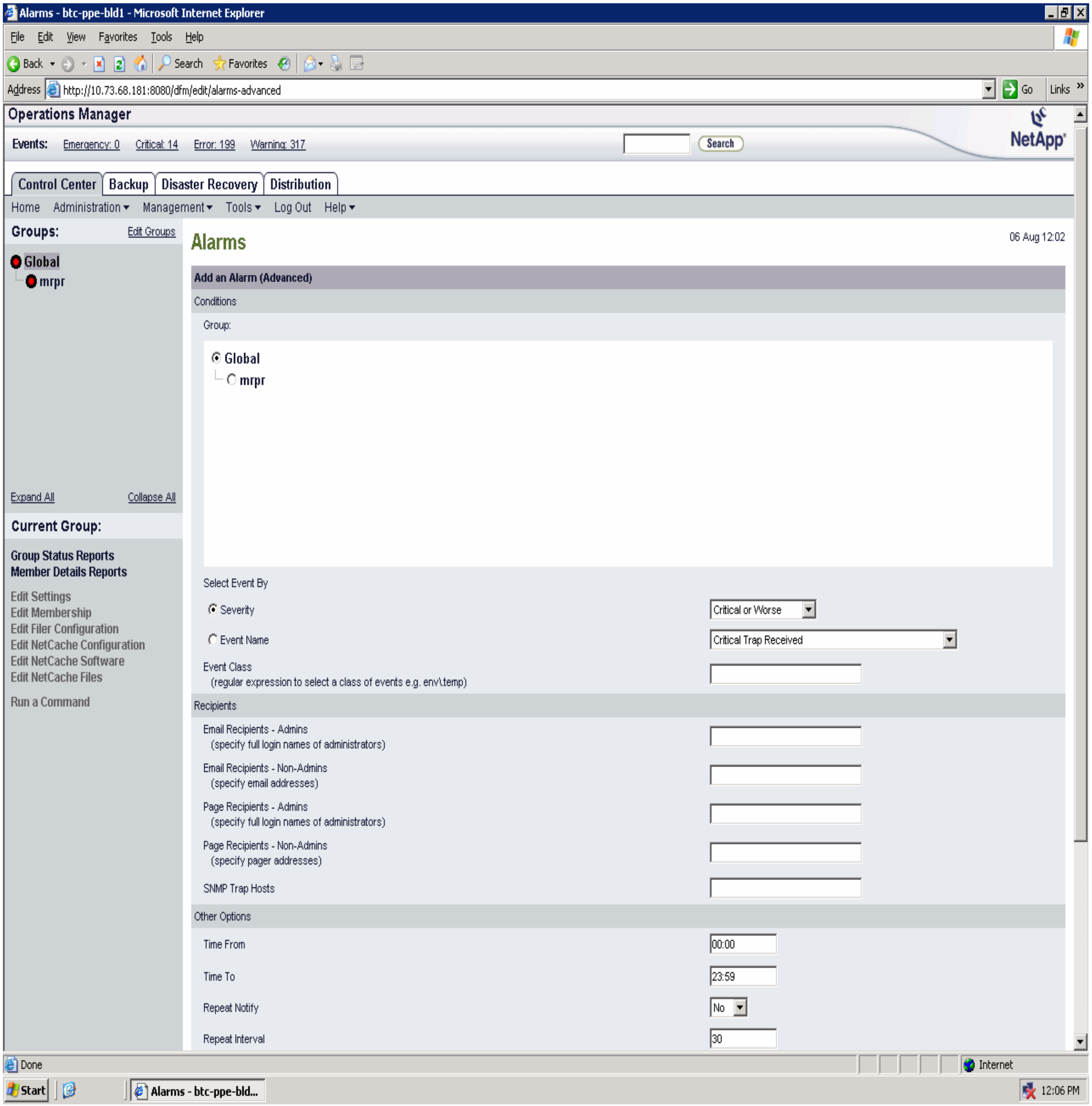
Tool	Description
Manage Storage System	Enables you to access the following storage system management tools: _ FilerView®—A Web-based administration tool. You can use FilerView software to perform tasks that otherwise require you to enter commands at the storage system console or edit configuration files. _ Filer At-A-Glance—A Java™-based monitoring tool. Filer At-A-Glance displays real-time graphs of network traffic and file system operations.
Setup Wizard	Web-based setup tool to configure a storage system for your network environment
Manual Pages	Data ONTAP man pages
Telnet Session	Starts a telnet session

5 APPROACH 2

Customers who have Operations Manager can enable trap forwarding and forward SNMP traps of their storage system to HP OpenView.

5.1 RECEIVING SNMP TRAPS USING OPERATIONS MANAGER

Operations Manager monitors events from the storage systems managed by it. It provides an option called “Alarm” that can be set for the events it monitors. Data ONTAP SNMP traps are part of the events monitored by Operations Manager. Alarms can be set on the SNMP trap events. Users can configure a simple or an advanced alarm from the Alarms window. When an event occurs that triggers an alarm, a notification is sent to one or more specified recipients: an e-mail address, a pager number, or an SNMP trap host, or the alarm can trigger a user-defined script. By setting the alarm recipient as “SNMP trap host,” SNMP trap events can be received by the trap host.


Alarms - btc-ppe-bld1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.73.68.181:8080/dfm/edit/alarms-advanced
Go Links
Operations Manager
NetApp
Events: Emergency: 0 Critical: 14 Error: 199 Warning: 317
Search
Control Center Backup Disaster Recovery Distribution
Home Administration Management Tools Log Out Help
Groups: Edit Groups
Global
mrpr
Expand All Collapse All
Current Group:
Group Status Reports
Member Details Reports
Edit Settings
Edit Membership
Edit Filer Configuration
Edit NetCache Configuration
Edit NetCache Software
Edit NetCache Files
Run a Command
Done
Internet
Start
Alarms - btc-ppe-bld...
12:06 PM

Alarms

06 Aug 12:02

Add an Alarm (Advanced)

Conditions

Group:

- ● Global
  - ○ mrpr

Select Event By

● Severity	Critical or Worse
○ Event Name	Critical Trap Received
Event Class (regular expression to select a class of events e.g. env\.temp)	

Recipients

Email Recipients - Admins (specify full login names of administrators)	
Email Recipients - Non-Admins (specify email addresses)	
Page Recipients - Admins (specify full login names of administrators)	
Page Recipients - Non-Admins (specify pager addresses)	
SNMP Trap Hosts	

Other Options

Time From	00:00
Time To	23:59
Repeat Notify	No
Repeat Interval	30

Figure 8) Setting alarms in Operations Manager.

5.2 SNMP TRAP LISTENER CONFIGURATION REQUIREMENTS

The following configuration requirements must be met to enable reception of SNMP traps from managed storage systems.

On DataFabric® Manager: No configuration is needed to start the SNMP trap listener on DataFabric Manager (the trap listener is automatically started after installation). The SNMP trap global options are also configured with default settings, although you might want to modify these settings. For information about modifying the SNMP trap global settings, refer to the Operations Manager admin guide available at http://now.netapp.com/NOW/knowledge/docs/.

On Managed Storage Systems: You must manually add the DataFabric Manager server as a trap destination on all supported systems to be monitored. The traps must be sent to the DataFabric Manager server over UDP port 162.

5.3 STARTING AND STOPPING THE SNMP TRAP LISTENER ON DATAFABRIC MANAGER

The SNMP trap listener is enabled on DataFabric Manager by default. If you want to stop the SNMP trap listener, use the CLI command ***dfm option set snmpTrapListenerEnabled="No."*** You can also reenable the SNMP trap listener using the CLI command ***dfm option set snmpTrapListenerEnabled="Yes."***

Note: DataFabric Manager Service—"Server" needs to be restarted once this option is set.

5.4 MODIFYING THE SNMP TRAP GLOBAL OPTIONS

Configuration of the SNMP trap global options is not necessary at startup. However, you might want to modify the global default settings. The following global default settings can be modified:

- Enable SNMP Trap Listener

Use this option to enable or disable the SNMP trap listener.

- SNMP Trap Listener Port

Use this option to specify the UDP port on which the SNMP Manager Trap Listener receives traps. Currently, supported storage systems can send SNMP traps only over UDP port 162.

- SNMP Maximum Traps Received per Window and SNMP Trap Window Size

Use these two options to limit the number of SNMP traps that can be received by the Trap Listener within a specified period of time.

For more details on changing these settings, refer to the Operations Manager admin guide available at http://now.netapp.com/NOW/knowledge/docs/ and refer to SNMP Trap Listener options and the Event and Alert options on the Options page.

Further information about Operations Manager can be found at http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml.

6 APPENDICES

Appendix 1a—Standard SNMP Traps (RFC 1215)

TRAP NAME	TRAP CODE	DESCRIPTION
coldStart	0	A coldStart trap signifies that the protocol entity is reinitializing itself such that the agent's configuration or protocol entity implementation may be altered.
warmStart	1	A warmStart trap signifies that the protocol entity implementation is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.
linkDown	2	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.
linkUp	3	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.
authenticationFailure	4	An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated.
egpNeighborLoss	5	An egpNeighborLoss trap signifies that an EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer obtains.

6.1.1 Appendix 1b—NetApp Specific Built-in SNMP Traps

The following list may not be exhaustive or the most recent. The actual list of NetApp Specific Built-in Data ONTAP SNMP Traps that is applicable to your storage system can be found in the MIB file ***/etc/MIB/netapp.mib*** on your storage system.

TRAP NAME	TRAP CODE	Severity	DESCRIPTION
dhmNoticeDegradedIO	6	Notification	Disk Health Monitor—Reported a Disk Degraded-I/O Event
dhmNoticePFAEvent	7	Information	Disk Health Monitor—Reported a Disk Predictive-Failure Event
diskFailedShutdown	21	Emergency	System is shutting down because it has been running in degraded mode for 24 hours. The trap includes a string describing the failed disk.
diskFailed	22	Alert	One or more disks failed. The trap includes a string describing the failed disk(s).
diskRepaired	26	Notification	The failed disks have been repaired. This trap is a placeholder—it is not currently sent by Data ONTAP.
fanFailureShutdown	31	Emergency	Critical chassis or CPU fans have failed and the system is shutting down.
fanFailed	33	Critical	One or more chassis fans failed. The trap includes a string describing the failed fan(s).
fanWarning	35	Warning	One or more chassis or CPU fans are in the warning state. The trap includes a string describing the fan(s) in the warning state.

fanRepaired	36	Notification	All fans are repaired.
powerSupplyFailureShutdown	41	Emergency	Critical power supplies or power rails failed and the system is shutting down.
powerSupplyFailed	43	Critical	One or more redundant power supplies failed. Includes in the trap a string describing the failed power supply(ies).
powerSupplyWarning	45	Warning	One or more power supplies or power rails are in the warning state. Includes in the trap a string describing the power supply(ies) or the power rail(s) in the warning state.
powerSupplyRepaired	46	Notification	Previously failed power supplies or power rails have been repaired.
cpuTooBusy	55	Warning	CPU utilization exceeds 90%. This trap is not enabled by default. To enable this trap set the registry entry options.monitor.cpu.enable to on. Note that as the threshold for this trap is checked once a minute it is possible to receive multiple instances of this trap in a short time.
cpuOk	56	Notification	CPU utilization has dropped back below 90%. This trap is a placeholder—it is not currently sent by Data ONTAP.
nvramBatteryDischarged	62	Alert	The NVRAM battery is fully discharged.
nvramBatteryLow	63	Critical	The charge in the NVRAM battery is low.
clusterNodeFailed	72	Alert	A node in a Cluster Failover configuration failed. Its partner will assume service for the failed node.
clusterNodeTakenOver	75	Warning	The partner has taken over for a failed cluster node.
clusterNodeRepaired	76	Notification	A cluster node has resumed operation.
volumeFull	82	Alert	At least one volume is more than 98% full. The string sent with the trap gives the name of the volume or volumes that exceed the threshold.
volumeNearlyFull	85	Warning	At least one volume is more than 95% full. The string sent with the trap gives the name of the volume or volumes that exceed the threshold.
volumeRepaired	86	Notification	All volumes are now under 95% full.
overTempShutdown	91	Emergency	System temperature is too high to continue operating. The system is shutting down.
overTemp	95	Warning	System temperature is too high and in the warning level.
overTempRepaired	96	Notification	System temperature has returned to an acceptable value.
shelfFault	103	Critical	A disk storage shelf reported a fault, probably due to a problem with drive placement, fans, power, or temperature.
shelfRepaired	106	Notification	A previously reported shelf fault is now corrected.
globalStatusNonRecoverable	111	Emergency	The appliance's overall status changed to “nonRecoverable,” indicating a problem so severe that the appliance is shutting down.
globalStatusCritical	113	Critical	The appliance's overall status changed to “critical,” indicating a problem that needs immediate attention.
globalStatusNonCritical	115	Warning	The appliance's overall status changed to “noncritical,” indicating a problem that needs attention.

globalStatusOk	116	Notification	The appliance's overall status returned to normal.
softQuotaExceeded	126	Notification	A user has exceeded his or her soft quota limit.
softQuotaNormal	127	Information	A user is safely back under his or her soft quota limit.
autosupportSendError	134	Error	Unable to send AutoSupport. The trap includes a string describing the reason for the failure.
autosupportConfigurationError	135	Warning	AutoSupport may be configured incorrectly. The trap includes a string describing the misconfiguration.
autosupportSent	136	Notification	AutoSupport was sent successfully.
upsLinePowerOff	142	Alert	UPS: Input line power has failed and UPS is now on battery.
upsBatteryCritical	143	Critical	UPS: Battery is nearly exhausted, starting graceful shutdown.
upsShuttingDown	144	Error	UPS: Shutting down now: Time left on battery is exhausted.
upsBatteryWarning	145	Warning	UPS: Warning: Time left on battery is getting critical.
upsLinePowerRetored	146	Notification	UPS: Input line power has been restored and UPS is now off battery.
appEmergency	151	Emergency	The application encountered an extremely urgent situation and requires an immediate response.
appAlert	152	Alert	The application is in a condition that should be corrected immediately.
appCritical	153	Critical	The application encountered a critical condition.
appError	154	Error	The application encountered an error condition.
appWarning	155	Warning	The application is in a condition that is not an error, but may require special handling.
appNotice	156	Notification	The application is notifying regarding a certain event.
appInfo	157	Information	The application's message is meant for informational purposes.
appTrap	158	Debug	The application requires debugging.
alfFilewrap	162	Alert	The internal audit file has wrapped. You are currently losing event records. Warning the user.
alfFileSaved	166	Notification	The internal audit log has been autosaved to an external evt file. Notifying the user.
alfFileNearlyFull	167	Information	The internal audit log file is nearly full. The file is going to wrap. Notifying the user.
quotaExceeded	176	Notification	One of the quota limits has been exceeded.
quotaNormal	177	Information	One of the quota limits has gone back down to a normal level.
waflDirFull	187	Information	The directory has been filled to its limit.
eccSummary	192	Alert	Memory ECC: number of new correctable ECC errors.
eccMasked	195	Warning	Memory ECC: high frequency of ECC errors.
ftpdError	204	Error	Ftp daemon: service stopped.
ftpdMaxConnNotice	206	Notification	Ftp daemon: number of connections hits maximum number.
ftpdMaxConnThresholdNotice	216	Notification	Ftp daemon: number of connections nearly hits

			maximum number.
scsitgtFCPLinkBreak	222	Alert	SCSI Target: link break on FCP adapter.
scsitgtPartnerPathMisconfigured	224	Error	SCSI Target: FCP partner path misconfigured.
scsitgtThrottleNotice	226	Notification	SCSI Target: throttle limit event notification.
vifPrimaryLinkFailed	237	Information	The primary interface on a single mode vif has failed.
vifAllLinksFailed	238	Debug	All the links of the vif have failed.
vfStopped	245	Warning	A vFiler™ has stopped.
vfStarted	246	Notification	A vFiler has started.
vscanVirusDetectedError	254	Error	Vscan scanner has detected a virus on the storage.
vscanDisConnection	255	Warning	A connection to the vscan servers has been dropped.
vscanConfigurationChange	256	Notification	There has been a change to the vscan configuration.
vscanServerUpgrade	266	Notification	The vscan server has been upgraded.
volumeRestrictedByMirrorBigIo	272	Alert	A volume that experienced a medium error during reconstruction is restricted and marked wafl-inconsistent, but starting wafliron has failed. This trap is issued to alert the operator that a volume is not accessible and wafliron must be started to allow access to it.
volumeInconsistentUmount	274	Error	This trap is issued when we unmount a volume due to an inconsistency.
volumeStateChanged	275	Warning	Volume is being taken offline or being restricted. The string sent with trap specifies name of affected volume and its state.
volumeOnline	276	Notification	Volume is online now. The string sent with trap specifies name of volume that is online now.
rmcCardNeedsReplacement	283	Critical	Remote Management Controller card needs replacement. The trap includes a string specifying the reason for replacement.
rmcCardMissingCables	284	Error	Remote Management Controller card is missing its internal cable, LAN cable, or power supply cable. The trap includes a string specifying the missing component.
volumeRemoteUnreachable	294	Error	Local volume encountered an error while communicating to remote volume.
volumeRemoteOk	296	Notification	The communication between remote volume and local volume returned to normal.
volumeRemoteRestored	297	Information	The data on remote volume has been fully restored to local volume.
volumeRemoteRestoreBegin	298	Debug	The data on remote volume has started being restored to local volume by Restore-on-Demand.
volumeRestrictedRootConflict	304	Error	Volume is restricted due to a root volume conflict. The string sent with trap specifies name of conflicting volume that is being restricted.
volumeOfflineTooBig	314	Error	Volume cannot be brought online because its raw size is larger than maximum allowed size. The string sent with trap specifies name of affected volume and its raw size, and maximum allowed size.
volumeOffline	324	Error	Volume is being taken offline. The string sent with

			trap specifies name of affected volume and reason for being taken offline.
volumeRestricted	334	Error	Volume is being restricted. The string sent with trap specifies name of affected volume and reason for being restricted.
volumeDegradedDirty	344	Error	Volume is degraded and has dirty parity. WAFL_check must be run on this volume before it can be brought online. The string sent with trap specifies name of affected volume.
volumeError	354	Error	This trap is issued when a volume cannot be brought online due to an error. The string sent with trap specifies name of affected volume and error description.
snapmirrorSyncFailed	364	Error	Synchronous SnapMirror® failed and went into asynchronous mode.
snapmirrorSyncOk	366	Notification	Synchronous SnapMirror went into synchronous mode.
chassisTemperatureShutdown	371	Emergency	The chassis temperature is extreme. The appliance has initiated a shutdown to protect itself. The operating environment should be monitored and corrected before restarting the appliance.
chassisTemperatureWarning	372	Alert	The chassis temperature is either too high or too low. The temperature should be monitored and, if possible, corrected.
chassisTemperatureUnknown	375	Warning	The chassis temperature is unknown, because a reading can't be obtained from the chassis temperature sensor.
chassisTemperatureOk	376	Notification	The chassis temperature is OK.
chassisCPUFanStopped	381	Emergency	One or more CPU fans have stopped. The appliance has initiated a shutdown to protect itself. A new motherboard may be required to correct the fan.
chassisCPUFanSlow	383	Critical	A CPU fan is spinning too slowly. A new motherboard may be required to correct the fan.
chassisCPUFanOk	386	Notification	All CPU fan(s) are properly functioning.
chassisPowerSuppliesFailed	391	Emergency	Multiple chassis power supplies failed.
chassisPowerSupplyDegraded	392	Alert	One or more chassis power supplies are degraded. A description of the degraded state is logged to the console and message log file.
chassisPowerSupplyFailed	393	Critical	One chassis power supply failed.
chassisPowerSupplyRemoved	394	Error	One or more chassis power supplies are removed.
chassisPowerSupplyOff	395	Warning	One or more chassis power supplies are off.
chassisPowerSuppliesOk	396	Notification	The chassis power supplies are all functioning properly.
chassisPowerSupplyOk	397	Information	This chassis power supply is functioning properly.
chassisPowerDegraded	403	Critical	The power within the chassis is degraded.
chassisPowerOk	406	Notification	The power within the chassis is functioning properly.
chassisFanDegraded	412	Alert	A chassis fan has been degraded.
chassisFanRemoved	413	Critical	A chassis fan FRU has been removed.
chassisFanStopped	414	Error	One or more chassis fans have stopped.

chassisFanWarning	415	Warning	One or more chassis fans are spinning slowly or too fast.
chassisFanOk	416	Notification	All chassis fans are functioning properly.
writeVerificationFailed	424	Error	A write has failed a verification test on a SnapValidator®-enabled volume.
domainControllerDisconnect	435	Warning	A CIFS domain controller connection to the storage has failed.
plexFailed	444	Error	Indicates one plex of a mirrored traditional volume or aggregate has failed. The string sent with this trap specifies name of affected plex or mirrored traditional volume or aggregate.
plexOffline	454	Error	Indicates a plex has gone offline. The string sent with this trap specifies name of affected plex or mirrored traditional volume or aggregate.
shelfSESElectronicsFailed	464	Error	One or more of the enclosure services devices in a disk shelf has failed. Some shelf designs combine the enclosure-monitoring hardware function into the module that provides the storage interface to the shelf. A failure in the enclosure-monitoring section of these combined modules does not necessarily indicate a failure in disk or loop or bus operation, which may be able to continue.
shelfSESElectronicsInfo	467	Information	A previously reported failure of an enclosure services device in a disk shelf has been corrected, or the device has reported information that does not necessarily require customer action.
shelfIFModuleFailed	473	Critical	One or more of the storage interface modules in a disk shelf have failed. Some shelf designs combine the enclosure monitoring hardware function into the module that operates the Fibre Channel loop or SCSI in the shelf. This failure is of the storage interface itself, not a failure of the enclosure monitoring, which may be able to continue. This failure may make one or more disks in the shelf or in the loop or bus unavailable.
shelfIFModuleInfo	477	Information	A previously reported failure of a disk shelf interface module has been corrected, or the module has reported information that does not necessarily require customer action.
maxDirSizeAlert	482	Alert	A directory has reached its maxdirsize limit. Either increase the maxdirsize or clean up the directory.
maxDirSizeWarning	485	Warning	A directory is getting close to its maxdirsize limit. Either increase the maxdirsize or clean up the directory.
takeoverAlert	490	NA	The partner RLM thinks the partner should be taken over.

6.1.2 Appendix 1c—Generic User-Defined SNMP Traps

All user-defined traps with the same severity use the trap for that severity level. The following table lists the built-in traps that are used for the user-defined traps of the same severity level.

TRAP NAME	TRAP CODE	Severity	DESCRIPTION
userDefined	2	Unprioritized	A polling-style trap built using the “snmp traps” command on the storage.
emergencyTrap	11	Emergency	Indicates an extremely urgent situation, usually indicating that the system has failed and is shutting down.
alertTrap	12	Alert	Indicates a condition that should be corrected immediately.
criticalTrap	13	Critical	Indicates a critical condition, such as a hard device error.
errorTrap	14	Error	Indicates an error condition, such as a mistake in a configuration file.
warningTrap	15	Warning	Indicates a condition that is not an error, but may require special handling.
notificationTrap	16	Notification	Trap meant to provide notification, such as an hourly uptime message.
informationalTrap	17	Information	Used for informational purposes.
dbgTrap	18	Debug	Used for debugging purposes.

Appendix 2—User-Defined Traps’ Configurable Parameters

The Data ONTAP command for defining or changing a user-specified trap is:

```
$snmp traps trapname.parm value
```

Valid parameters for the above command, with a description of each, are as follows:

PARAMETER	DESCRIPTION
Var	The MIB variable that is queried to determine the trap’s value. All MIB variables must be specified in the form snmp.oid, where oid is an OID (Object Identifier). A list of OIDs in the Data ONTAP MIB is in the traps.dat file in the same directory as the MIB (/etc/MIB/traps.dat).
trigger	Determines whether the trap should send data. The following triggers are available: single-edge-trigger sends data when the trap’s target MIB variable’s value crosses a value that you specify. double-edge-trigger enables you to have the trap send data when an edge is crossed in either direction (the edges can be different for each direction). level-trigger sends data whenever the trap’s value exceeds a certain level.
edge-1 edge-2	A trap’s edges are the threshold values that are compared against during evaluation to determine whether to send data. The default for edge-1 is the largest integer and the default for edge-2 is 0.
edge-1-direction edge-2-direction	Edge-triggered traps only send data when the edges are crossed in one direction. By default, this is up for the first edge and down for the second edge. The direction arguments let you change this default.

interval	The number of seconds between evaluations of the trap. A trap can only send data as often as it is evaluated.
interval-offset	The amount of time in seconds until the first trap evaluation. Setting it to a nonzero value will prevent too many traps from being evaluated at once (at system startup, for example). The default is 0.
backoff-calculator	After a trap sends data, you might not want it to be evaluated so often. For example, you might want to know within a minute of when a file system is full, but only want to be notified every hour that it is still full. There are two kinds of backoff calculators: step-backoff and exponential-backup in addition to no-backoff.
backoff-step	The number of seconds to increase the evaluation interval if you are using a step backoff. If a trap's interval is 10 and its backoff-step is 3590, the trap is evaluated every 10 seconds until it sends data, and once an hour thereafter. The default is 3600.
backoff-multiplier	The value by which to multiply a trap's evaluation interval each time it fires. If you set the backoff calculator to exponentialbackoff and the backoff multiplier to 2, the interval doubles each time the trap fires. The default is 1.
rate-interval	If this value is greater than 0, the samples of data obtained at the interval points (set using the interval parameter) for a trap variable are used to calculate the rate of change. If the calculated value exceeds the value set for edge-1 or edge-2 parameters, the trap is fired. The default is 0.
priority	In descending order of severity: emergency or alert or critical or error or warning or notification (default) or informational or debug.
message	Message associated with the trap. The message could be a string or of the form snmp.oid. If an OID is specified, the result of evaluating that OID is sent. The default message is a string that shows the OID value that triggered the trap.

Note: For the supported params on your storage system, check the *Data ONTAP Command Reference Manual* version that maps to the version of Data ONTAP on your storage system.

7 REFERENCE

ApplianceWatch 1.2 for HP OpenView
Operations Manager Administration Guide
Data ONTAP TRAP Management Technical Report