Data ONTAP® SNMP Trap Management

M. Ravi Prakash Reddy, Network Appliance, Inc.

August 2007 | TR-3608

Executive Summary

Data ONTAP SNMP Traps provide a standard mechanism for monitoring the health and state of various components of the NetApp storage system. The Data ONTAP SNMP agent supports different types of traps like Standard SNMP traps, NetApp Specific Built-in Traps, and User-defined Traps. This document provides all the details of the supported Trap types including trap severity conventions, configuring trap settings, adding customized traps, and different ways of receiving traps.

Table of Contents

1. Introduction

1.1 Background

The *Simple Network Management Protocol (SNMP)* is an application layer protocol that facilitates exchange of management information between network devices. SNMP is defined in RFC 1157.

SNMP is based on a manager/agent model. The agent resides on the managed device and provides two types of events to the manager on the management system.

- Responses – These are the events sent as responses to the get/set requests from the SNMP manager.
- Traps – These are asynchronous events sent to the management system following such occurrences as a threshold that exceeds a predetermined value.

SNMP manager/agent gets the properties of managed objects within the managed device from Management Information Bases (MIBs). Every managed device keeps a database of values for each of the definitions written in the MIB. The latest Internet MIB is given in RFC 1213, sometimes called the MIB-II.

At present three versions of SNMP exist: SNMP version 1 (SNMPv1, basic version), SNMP version 2 (SNMPv2, provides additional protocol operations), and SNMP version 3 (SNMPv3, provides a new security model).

1.2 SNMP Support on NetApp Storage Systems

NetApp storage systems support the SNMP version 1 compatible agent. This agent supports both MIB-II and the Network Appliance™ custom MIB.

If SNMP is enabled in Data ONTAP, SNMP managers can query the storage system's SNMP agent for information (specified in your storage system's MIBs or the MIB-II specification). In response, the SNMP agent gathers information and forwards it to the SNMP managers using the SNMP protocol. The SNMP agent also generates trap notifications whenever specific events occur and sends these traps to the SNMP managers. The SNMP managers can then carry out actions based on information received in the trap notifications.

The latest versions of the Data ONTAP MIB files are available online on the NetApp on the Web (NOW™) site.

1.3 Purpose and Scope

The purpose of this document is to provide all the information about Data ONTAP SNMP traps to help the developers and users of SNMP management applications for NetApp Storage systems to properly understand and manage the Data ONTAP SNMP traps.

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

2. Basics of SNMP Traps

SNMP agents use Traps as a mechanism to send asynchronous events to the Management system on the occurrence of a particular event on the managed system. A trap can be used to check periodically for different operational properties' thresholds or operational failures defined in the MIB on the managed device; if a threshold or failure is detected, the SNMP agent sends a message to the trap hosts alerting them to the event.

SNMP defines (RFC 1215) a few standardized traps and provides a means for management enterprises to define enterprise-specific traps using the 'TRAP_TYPE' macro.

The typical definition of enterprise-specific traps is shown below:

<Trap Name> TRAP-TYPE
ENTERPRISE *<Enterprise OID>*
VARIABLES *<MIB objects to be sent in the Trap Protocol Data Unit (PDU)>*
DESCRIPTION
<"Description of the Trap">

::= <Trap Code>

Traps are generated when a condition has been met on the SNMP agent. These conditions are defined in the Management Information Base (MIB) provided by the vendor. The administrator then defines thresholds, or limits to the conditions, that are to generate a trap. Conditions range from preset thresholds to a restart. After the condition has been met the SNMP agent forms an SNMP trap packet with the following format:

SNMP Trap Packet Format:

Version	Community	Trap PDU

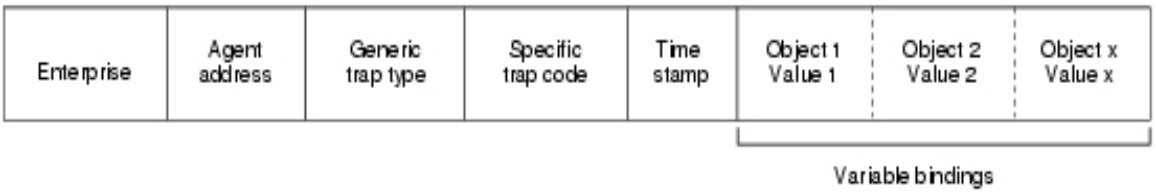
***Version**: SNMP Version (v1, v2 or v3)*

***Community**: Community name of the SNMP agent (defined on the agent)*

***Trap PDU**: SNMPvX PDU of type Trap-PDU*

SNMP Trap PDU Format:

Trap PDU contains the six fields shown below:



***Enterprise**: Corporation or organization that originated the trap, such as .1.3.6.1.4.1.x*

***Agent Address**: IP address of the SNMP agent.*

***Generic Trap Type**: One of the generic SNMP trap types (Cold Start, Warm Start, Link Up, Link Down, Authentication Failure, EGP Neighbor Loss, Enterprise Specific).*

***Specific Trap code**: When Generic trap type is set to 'Enterprise Specific,' a unique ID is provided that identifies the Trap.*

***Timestamp**: Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.*

***Object x Value x**: The data field of the Trap PDU. Each variable binding associates a particular object instance with its current value.*

The above packet is sent to an SNMP trap host, or manager, through UDP port 162. The trap-hosts list specifies network management stations that receive trap information. Third-party SNMP applications on the network management station can be used to process the trap information.

3. Data ONTAP SNMP Traps

3.1 Trap Types

The Data ONTAP SNMP agent supports 3 types of SNMP traps.

1. **SNMP Standard Traps**:
   These are standard SNMP traps defined in the MIB-II specification (RFC 1215). These traps define the different operation states of the SNMP agent, like agent is reinitializing, agent communication link is down, etc.

   Data ONTAP provides a mechanism to suppress or enable the standard SNMP trap 'authenticationFailure.'

   '***Appendix 1a***' lists the details of the SNMP Standard Traps.

2. **NetApp Specific Built-in Traps**:

   NetApp storage systems have a number of built-in traps for the convenience of SNMP users. The bottom of the management information base file (/etc/mib/netapp.mib) has a list of all the built-in traps.

   The trap code provided in the trap definition in MIB is the unique identifier for the Built-in Trap. The '*Specific Trap code'* field in the Trap PDU of the SNMP packet is set to this trap code. The Trap code numbers are used in blocks of ten [0..9]; which number to actually use should follow the trap's severity convention as described in section '***3.2 Trap Severity.***'

   '***Appendix 1b***' lists the details of the NetApp Built-in Traps.

3. **User defined Traps**:

   Data ONTAP provides a mechanism to add customized user-defined traps. Users can set traps on any numeric variable in the MIB. Section '3.3.2 Adding Traps' provides the details on how to add a user defined Trap on Data ONTAP.

   Data ONTAP provides certain Built-in Traps in the MIB to facilitate the standard way for retrieving the different severity level user defined Traps. Appendix 1c lists the details of these Built-in Traps.

User defined Traps are persistent. After a trap is created and set, it remains across reboots until it is specifically removed or modified.

All user-defined traps are sent with a variable binding to the 'userDefined' trap in the Data ONTAP MIB, which has the OID of 1.3.6.1.4.1.789.0.2. The trap itself contains the source entity (the storage system). The trap data contains a string of the following form: *name == value*

name is the name specified by the user.
value is the value of its MIB object at the time the trap fires.

3.2 Trap Severity

NetApp Specific SNMP Traps can have the following levels of severity:

TRAP SEVERITY	SEVERITY DESCRIPTION
emergency	Indicates an extremely urgent situation, usually indicating that the system has failed and is shutting down
alert	Indicates a condition that should be corrected immediately
critical	Indicates a critical condition, such as a hard device error
error	Indicates an error condition, such as a mistake in a configuration file
warning	Indicates a condition that is not an error, but may require special handling
notification	Indicates notification, such as an hourly uptime message
information	Used for informational purposes
debug	Used for debugging purposes

Table 1) SNMP Traps Severity Levels

Built-in Traps' Severity:

The severity level of a built-in trap can be found by inspecting the ones digit of the specific trap code sent to the trap host, or in the trap definition in the Data ONTAP MIB. The following table shows the built-in trap severity convention:

LAST DIGIT OF TRAP CODE	IMPLIED SEVERITY
1	Emergency
2	Alert
3	Critical
4	Error
5	Warning
6	Notification
7	Information
8	Debug

Table 2) Mapping of Trap Code to Trap Severity Level

Examples:

i. The trap code for the built-in trap 'diskFailedShutdown' is 21 – The ones digit is '1' so the severity of this Trap is '*Emergency.*'

ii. The trap code for the built-in trap 'diskRepaired' is 26 – The ones digit is '6' so the severity of this Trap is '*Notification.*'

User defined Traps' Severity:

The User defined Trap severity can be set using the Data ONTAP command 'snmp' as shown below:

Storage system> snmp trapname.priority <priority level>

The <*priority level*> could be one of the following (in descending order of severity):

emergency, or *alert*, or *critical*, or *error*, or *warning*, or *notification (default)*, or *informational*, or *debug*

3.3 Configuring Traps

Different configuration settings for the traps like enabling/disabling traps and enabling/disabling 'authentication failure' traps can be performed through the CLI command on the Storage system, or through Manage ONTAP™ SDK API or through the GUI interface of FilerView®.

CONFIGURATION SETTING	CLI	Manage ONTAP SDK API	FilerView NAVIGATION PATH
Enable SNMP Traps	$*snmp traps enable <trapname>*	*snmp-trap-enable*	|--SNMP |--Configure |--Traps Enabled |--Yes
Disable SNMP Traps	$*snmp traps disable <trapname>*	*snmp-trap-disable*	|--SNMP |--Configure |--Traps Enabled |--No
Enable SNMP 'authentication failure' Trap	$*snmp authtrap 1*	*NA*	|--SNMP |--Configure |--AuthTraps |--Yes
Disable SNMP 'authentication failure' Trap	$*snmp authtrap 0*	*NA*	|--SNMP |--Configure |--AuthTraps |--No

Table 3) Configuration settings for Data ONTAP SNMP Traps

3.4 Adding User-defined Traps

Users can add customized SNMP traps to Data ONTAP using CLI on the Storage system or through the GUI of FilerView. Users can set traps on any numeric variable in the MIB. While setting a trap on any Object variable in the MIB, the Object Identifier (OID) of the variable should be specified as an input. The OIDs of all the Object Variables in the NetApp MIB are given in the file ***/etc/MIB/traps.dat*** on the NetApp storage system.

1. **Adding a User-defined Trap using CLI:**

   The following CLI command is used for creating/modifying User-defined traps:

   $**snmp traps** *trapname.parm* value
   trapname – Name of the User-defined trap being added/modified
   parm – Different parameters of the User-defined trap like the object name to be monitored for the trap, trigger options, trigger interval, trap priority, etc.

   The different configurable parameters for User-defined Traps and the values they take are described in '***Appendix 2.***'

   Examples:

   To define the cpuBusyPct trap and set it to point at the MIB object that returns the cumulative CPU busy time percentage of the storage, use the following command:

   $snmp traps *cpuBusyPct.var snmp.1.3.6.1.4.1.789.1.2.1.3.0*

   To set the evaluation interval of cpuBusyPct to one minute, use the following command:

   $snmp traps *cpuBusyPct.interval 60*

2. **Adding a User-defined Trap using FilerView:**

   Navigate to the page |--SNMP
   |--Manage
   |--Traps
   |--Add

The Page is shown below:

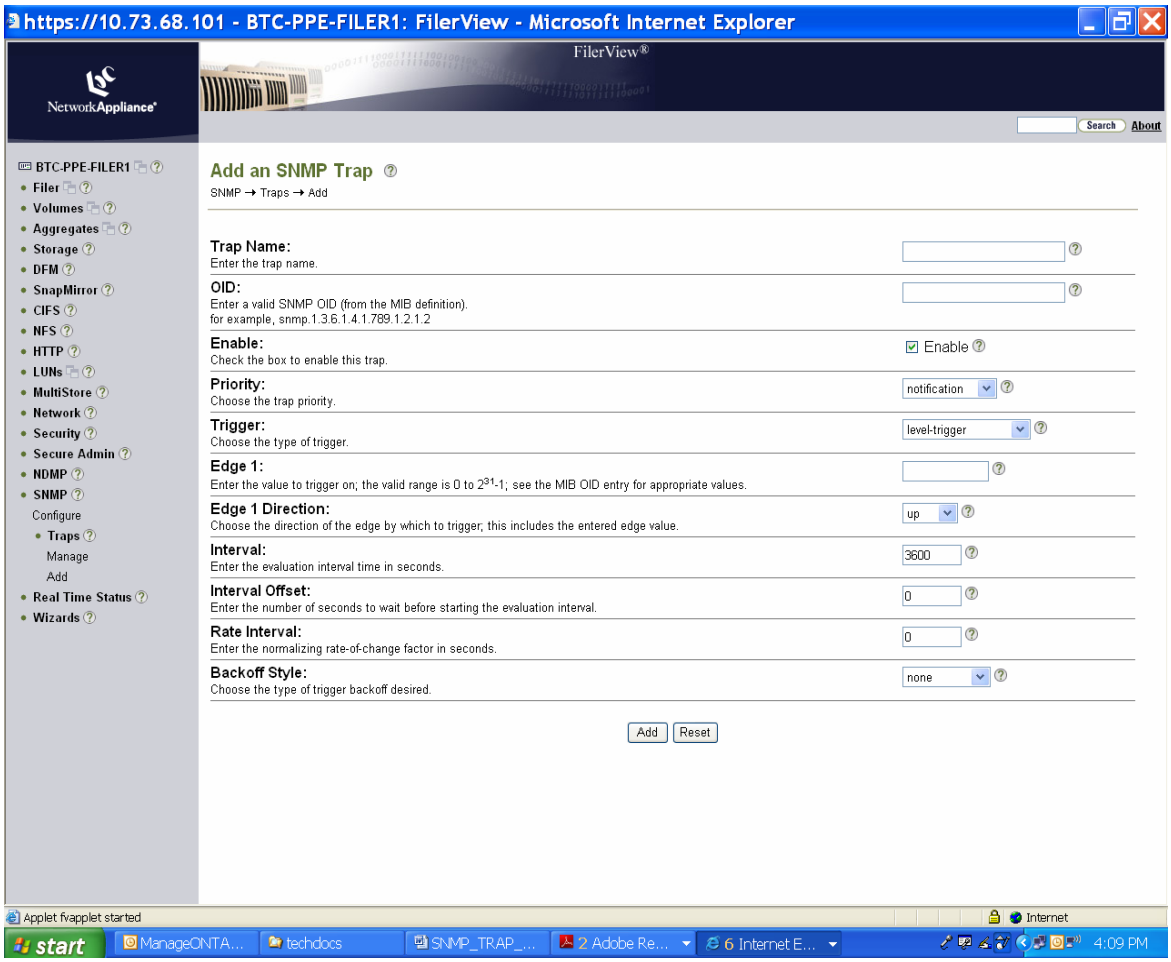


Figure 1) Adding a User-defined Trap using FilerView GUI

> ***Best practice**: Do not create traps against OIDs in sub-tables. (OIDs that are not in sub-tables end in 0.) The storage does not preserve the ordering of elements in sub-tables over reboots, and occasionally a trap that was supposed to work against one element will work against another after rebooting.*

3.5 Receiving Traps

Data ONTAP SNMP traps are disabled by default. To receive SNMP traps, traps need to be enabled first. This can be done as mentioned in section "**3.3 Configuring Traps.**"

Once the Traps are enabled, a management host can receive Data ONTAP SNMP traps in one of the following ways:

1. Add management hosts to the Data ONTAP Trap-hosts list

No traps are sent unless at least one trap host is specified. Up to a maximum of eight trap hosts are supported.

This can be done using CLI, FilerView or Manage ONTAP SDK as shown below:

CONFIGURATION SETTING	CLI	Manage ONTAP SDK API	FilerView NAVIGATION PATH
Add SNMP Trap Hosts	$*snmp traphost add <hostname>*	*snmp-traphost-add*	|--SNMP |--Configure |--Traphosts

Table 4) Setting trap hosts

Whenever a trap is triggered it is sent to all the hosts that are specified in the Trap-hosts list.

2. 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 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 email address, a pager number, an SNMP trap host, or a user-defined script. By setting the Alarm recipient as 'SNMP trap host,' SNMP Trap events can be received by the trap host.

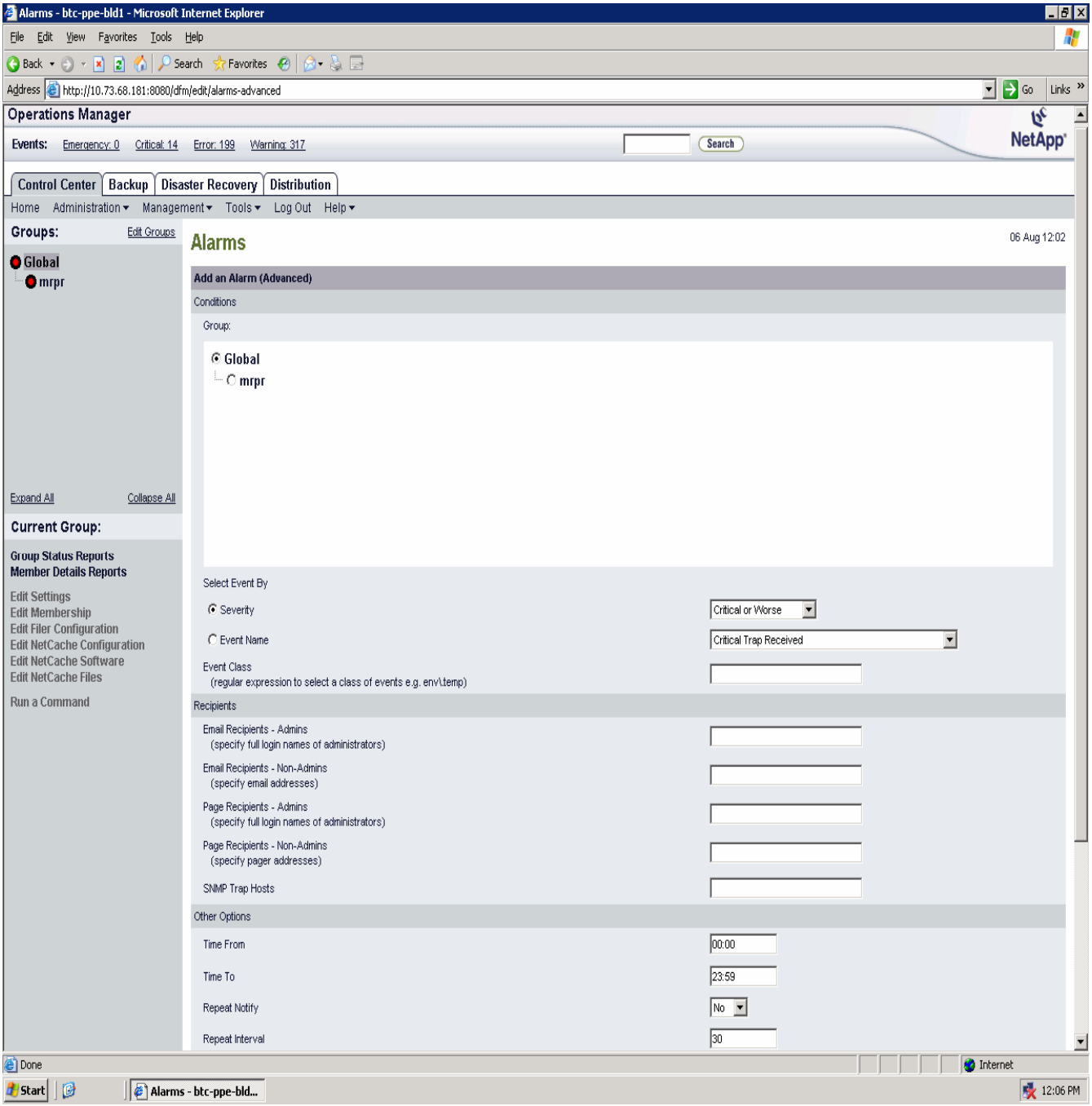


Figure 2) Setting Alarms in Operations Manager

4. 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.

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 the system 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, or 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 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 is 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 have 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.

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

ONTAP Command for defining or changing a user-specified trap:

$snmp traps *trapname.parm value*

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

PARAM	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 any more. 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.