EMC® VNX® Series

Release 8.1

Configuring Events and Notifications on VNX® for File

P/N 300-015-125 Rev 01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright © 2012 - 2013 EMC Corporation. All rights reserved.

Published August 2013

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Corporate Headquarters: Hopkinton, MA 01748-9103

Contents

Preface

As part of an effort to improve and enhance the performance and capabilities of its product lines, EMC periodically releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Special notice conventions

EMC uses the following conventions for special notices:

Note: Emphasizes content that is of exceptional importance or interest but does not relate to personal injury or business/data loss.

NOTICE Identifies content that warns of potential business or data loss.

CAUTION Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

WARNING Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

DANGER Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information—For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to EMC Online Support (registration required) at http://Support.EMC.com.

Troubleshooting—Go to EMC Online Support at http://Support.EMC.com. After logging in, locate the applicable Support by Product page.

Technical support—For technical support and service requests, go to EMC Customer Service on EMC Online Support at http://Support.EMC.com. After logging in, locate the applicable Support by Product page, and choose either **Live Chat** or **Create a service request**. To open a service request through EMC Online Support, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Note: Do not request a specific support representative unless one has already been assigned to your particular system problem.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications.

Please send your opinion of this document to:

techpubcomments@EMC.com

1 Introduction

EMC VNX for file generates events to record errors, commands, and other information that you might need to know. You can configure the system to perform an action when specified events occur. Actions based on events are called notifications. Notifications that the system can perform include logging the event in an event log file, sending an email, or generating a Simple Network Management Protocol (SNMP) trap.

This document is part of the VNX series information set and is intended for use by system administrators responsible for configuring and maintaining file storage and network retrieval infrastructure. Topics include:

System requirements

Table 1 on page 10 describes the EMC® VNX® series software, hardware, network, and storage configurations.

Table 1. System requirements

Software	VNX series version 8.1 or later.
Hardware	No specific hardware requirements.
Network	Depends on the type of action used for notifications. For example, mail service is required for email notification, SNMP applications for traps, DNS for hostname resolution, and modems for call homes.
Storage	No specific storage requirements.

Restrictions

Email notifications are dependent on external email servers. Some email servers might require you to register the Control Station hostname in DNS.

Cautions

If any of this information is unclear, contact your EMC Customer Support Representative for assistance:

- SNMP security is based on community strings. SNMP version 1 (SNMPv1) transmits all information in clear text. Anyone monitoring the network can obtain the SNMP community name from passing traffic. RFC 1157 provides details about SNMPv1 security.
- Link-local IPv6 addresses are not supported in SNMP trap destinations.

User interface choices

VNX for file offers flexibility in managing networked storage based on your support environment and interface preferences. This document describes how to configure notifications by using the command line interface (CLI). You can also perform many of these tasks by using one of these management applications:

- EMC Unisphere® software
- Active Directory Users and Computers (ADUC) extensions

The following documents provide additional information about managing your system:

- Unisphere online help
- Application's online help

The *Installing Management Applications on VNX for File* document includes instructions on launching the Unisphere software.

You cannot use the Unisphere software to configure the following notification actions:

Limitations:

- CallHome
- Execution of a procedure
- Generation of an RPC message
- Termination of processing of event

VNX 1.0 Release Notes contain additional, late-breaking information about management applications.

Related information

Specific information related to the features and functionality described in this document is included in the following documents:

- Unisphere online help
- *EMC VNX Command Line Interface Reference for File*
- *Parameters Guide for VNX for File*
- *VNX System Operations*
- *Managing Volumes and File Systems with VNX Automatic Volume Management*
- *Managing Volumes and File Systems for VNX Manually*
- VNX for File man pages

SNMP manager documentation has more information on SNMP.

EMC VNX documentation on EMC Online Support

The complete set of EMC VNX series customer publications is available on EMC Online Support. To search for technical documentation, go to http://Support.EMC.com. After logging in to the website, click **Support by Product** and type **VNX series** in the Find a Product text box. Then search for the specific feature required.

VNX wizards

Unisphere software provides wizards for performing setup and configuration tasks. The Unisphere online help provides more details on the wizards.

2 Concepts

You can monitor and manage the system, including Data Movers and file systems, with events and notifications. The system generates events as a result of system changes, some of which might be severe enough to cause an error or disrupt user access. By using notifications, you can specify a variety of actions, such as sending an email, triggering an SNMP trap, or running a script in response to these events.

The following sections provide background about using events and notifications on the system:

Events

The VNX series generates events in response to specific changes in the state of the system caused by a command, an error, or some other condition that might require action by an administrator. For example, an event is generated when any of the following occur:

- A Data Mover restarts
- A network interface card (NIC) fails
- A file system reaches its soft or hard quota limit
- An EMC SnapSure™ save volume exceeds its limit and becomes inactive
- A virus checker server becomes unavailable

The file /nas/sys/nas_eventlog.cfg specifies default notifications (actions) that occur as a result of events. Customize notifications on page 52 provides information about setting up customized events and notifications.

Note: Do not edit the files /nas/sys/nas_eventlog.cfg and /nas/site/nas_eventlog.cfg. Edits to /nas/sys/nas_eventlog.cfg will be lost during software upgrades. The file /nas/site/nas_eventlog.cfg contains the list of configuration files currently loaded into the event handler. The directory /nas/site contains local event configuration files which are preserved during software upgrades. Create any new customized notification configuration files in this directory.

Facilities

The source of an event is called the event facility. The facility is the part of the system that generated the event. Each event facility is associated with a particular component and has a unique facility identifier (facility ID) within that component. For example, the UFS facility (facility ID 64) monitors file system quotas. If a quota is reached, an event is generated with a facility value of UFS.

The component ID specifies the area of the system from which the event was generated. The facility ID specifies a more specific subsystem within that component. Table 2 on page 14 lists IDs, components, and component definitions.

Table 2. IDs and components

ID	Component	Component definition
1	DART (data access in real time)	The operating environment that runs on the Data Mover. It is a realtime, multithreaded operating system optimized for file access, while providing service for standard protocols.

Table 2. IDs and components *(continued)*

ID	Component	Component definition
2	CS_CORE	The core software running on the Control Station.
6	CS_PLATFORM	Scripts and other network-attached storage (NAS) service software running on the Control Station.

The facilities that generate events can change from release to release. Table 3 on page 15 lists the facilities that generate events in the current release.

Table 3. Event facilities

Facility name	Facility ID	Component	Description
ACLUPD	101	DART	Access control list (ACL) database events.
ADMIN	24	DART CS_PLATFORM	Miscellaneous administrative and configuration events.
BoxMonitor	131	CS_PLATFORM	Hardware events. Monitors status of operating system on each Data Mover or blade. Also, monitors the enclosure hardware for NSX systems. The CHAMII facility also provides information.
CAM	26	DART	The Common Access Method (CAM) layer of the software provides the raw I/O communications to the data storage device. CAM events typically mean that there is a failure to communicate correctly with the storage processing components.
CEPP	146	DART	Common Event Publishing and Processing (CEPP) events. CEPP is a mechanism by which applications can register to receive event notification and context from a Data Mover. The events in this facility include only issues with CEPP itself; they do not include the events sent to registered applications.

Table 3. Event facilities *(continued)*

Facility name	Facility ID	Component	Description
CFS	27	DART CS_PLATFORM	Events associated with file system usage such as built-in usage thresholds and file system auto-extension.
CHAMII	86	DART	Monitors the hardware events of VNX series Data Movers and their enclosures. Formerly known as CHAMIIENCMON.
Checkup	142	CS_PLATFORM	NAS checkup events. The nas_checkup utility periodically runs a series of system health checks on the system and reports the problems found and the actions needed to fix them.
CIC	109	CS_CORE	Celerra interconnect events. Events associated with the internal communication between Data Movers or Control Stations or both.
CommandService	9	CS_CORE	Control Station command service daemon events. The Command Service daemon manages a number of administrative commands.
common	4	CS_CORE	Warm reboot events.
ConnectHome	133	CS_PLATFORM	ConnectHome events. The ConnectHome mechanism calls or emails EMC Customer Service automatically if a problem occurs.
DBMS	122	DART CS_CORE	Database Management System events for configuration data.
DEDUPE	148	DART	Deduplication events.
DHSM	96	DART	FileMover events.
DLM	153	CS_PLATFORM	Disk Library for mainframe events.
DNS	118	DART	Domain Name System events.

Table 3. Event facilities *(continued)*

Facility name	Facility ID	Component	Description
DPSVC	111	DART	Data Protection service events for file systems and VDM. Used for Replicator V2.
DRIVERS	36	DART	Device driver (for example: network ports, fibre ports) events.
EmailUser	144	CS_PLATFORM	Email user notification events.
EventLog	130	CS_PLATFORM	Control Station event log events.
FCP	102	DART	Low-level Fibre Channel SCSI driver events.
FSTOOLS	40	DART CS_PLATFORM	File system consistency events.
IP	43	DART	Internet Protocol events.
JServer	135	CS_PLATFORM	Celerra Monitoring Agent (JServer) events. The monitoring agent monitors all storage usage, storage projection, and Data Mover Load notifications, so events triggered by any of these notifications come from this facility.
KERNEL	45	DART	Events associated with the operating system of a Data Mover.
LIB	46	DART	Library events.
LocalHardwareMonitor	139	CS_PLATFORM	Control Station hardware events.
LOCK	68	DART	File lock manager events. The file lock manager handles file locking for all file access protocols (NFS, CIFS, and so on).
LogCollect	141	CS_PLATFORM	Automatic log collection and transfer events.
MasterControl	129	CS_PLATFORM	Control Station software events. The Master Control service manages several services on the Control Station.

Table 3. Event facilities *(continued)*

Facility name	Facility ID	Component	Description
MGFS	75	DART CS_PLATFORM	Celerra Data Migration Service (CDMS) migration file system events or FileMover events.
NASDB	137	CS_PLATFORM CS_CORE	NAS database events.
NaviEventMonitor	138	CS_PLATFORM	VNX for block
NDMP	51	DART CS_PLATFORM CS_CORE	Network Data Management Protocol (backup) events.
NETLIB	73	DART	Network Information Service events.
NFS	52	DART	Network file system events.
PERFSTATS	144	DART	Statistics Network Service (statmonService) events. The Statistics Network Service collects and reports on various system statistics.
RCPD	83	DART	Remote Copy Protocol Daemon events are generated for file system (ongoing and one-time copy) and VDM replication sessions.
RDFChannel	11	CS_CORE	Remote Data Facility (RDF) Service events. The RDF Channel service processes requests coming in from the RDF channel of the Data Mover.
REP	108	DART CS_CORE	Replication events for file systems and VDM. Used for Replicator V2.
SECMAP	115	DART	Events associated with the UNIX uid/gid to Windows SID mapping.
SECURITY	54	DART CS_PLATFORM	Security events.

Table 3. Event facilities *(continued)*

Facility name	Facility ID	Component	Description
SMB	56	DART	Common Internet File System (CIFS) events. Formerly known as Server Message Block events.
SNAPSURE_SCHED	91	CS_PLATFORM	SnapSure scheduling events.
STORAGE	58	DART	High-level SCSI driver events.
SVFS	70	DART CS_PLATFORM CS_CORE	SnapSure events.
SYR	143	CS_PLATFORM	Events associated with the System Reporting (SYR) process used to gather system configuration information.
TIMESYNC	62	DART	Time Services events.
UFS	64	DART	File system consistency events concerning the physical file system, which is dependent on the disk structure. Additionally, quota events are in this facility.
UPSMonitor	140	CS_PLATFORM	Uninterruptible Power Supply monitor for NSX systems.
USRMAP	93	DART	Usermapper events.
VC	81	DART	Virus-checking events.
VCS	107	DART	Version Control System events for snaps.
VMCAST	84	DART	Volume multicast Replicator (V1) events associated with a file system copy. This facility deprecated in version 6.0 and later.
VRPL	77	DART	Volume Replicator (V1) events. This facility deprecated in version 6.0 and later.
WINS	117	DART	Windows Internet Name Services events.

Table 3. Event facilities *(continued)*

Facility name	Facility ID	Component	Description
XLT	72	DART CS_PLATFORM	Translation (XLT) file events. Detects XLT file corruptions, and recovers those files automatically from the Control Station.

Event numbers

Each event associated with a facility is assigned a unique number within that facility. As an example, Table 4 on page 20 lists some of the events generated by the UFS facility.

Table 4. UFS event numbers

Base ID	Severity	Brief description
1	ERROR(3)	Event ${evt,5,%u} occurred while doing a dircvt
2	ERROR(3)	Event ${evt,5,%u} occurred while doing a dircvt
4	WARNING(4)	Block soft quota crossed (fs ${mountPoint,8,%s}, ${idStr,8,%s} %${userId,2,%d})
5	ERROR(3)	Block hard quota reached/exceeded (fs ${mountPoint,8,%s}, ${idStr,8,%s} ${userId,5,%u})
42	ERROR(3)	fsid ${fsid,5,%u}: transaction replay skipped. Missing volume information, fs may be corrupted

For example, if the usage of a file system grows beyond predefined quotas, the system generates UFS events (facility ID 64) with event numbers of 4 or 5.

Event severity levels

Each event has a severity level, which gives an administrator an indication of the nature of the event and whether it is necessary to take immediate action. Default notifications are defined in the configuration file /nas/sys/nas_eventlog.cfg. Table 5 on page 21 provides a list of event severity levels and shows the relationship between these severity levels and those defined by the Unisphere software.

The lower the severity level number, the greater the severity of the event. A severity of 0 is an emergency, while a severity of 7 is a debug condition.

Table 5. Event severity levels

Severity level	Name	Description	Unisphere designation
0	Emergency	An extremely urgent condition exists; immediate action is needed.	Critical
1	Alert	Administrator attention is required.	Critical
2	Critical	A critical error condition is detected.	Critical
3	Error	A noncritical error condition is detected.	Error
4	Warning	A nonerror condition occurred that, if ignored, could become an error.	Warning
5	Notice	An abnormal condition occurred that does not require an action.	Info
6	Info	A normal condition occurred; informational only.	Info
7	Debug	A debug-related condition occurred; this should not happen in normal operations.	Debug

Notifications

A notification is an action that the Control Station takes in response to a particular event. For example, the Control Station can send an email message to an administrator when a critical event occurs. Actions that the system can take include the following:

- Logging the event in an event log file
- Sending an email message for single or multiple system events to a specific email address
- Generating an SNMP trap
- Calling home to your service provider
- Generating a webalert

- Running a script
- Sending an RPC message to a host
- Terminating processing of an event

Event log files

The most common action taken when an event occurs is to log the event in an event log file. *VNX System Operations* provides information about displaying log files by using the CLI. The default system event log can be viewed and managed by using the Unisphere software. You can find detailed information about the Unisphere interface in its online help.

Notification configuration files

The system is configured with a set of default notifications that include logging all events to the appropriate log file. The default notifications are defined in the default configuration file /nas/sys/nas_eventlog.cfg.

Note: The checkup facility has its own sample configuration file, /nas/site/checkup_eventlog.cfg, which you can use to set up email notifications. To set up email notifications from scheduled checkups, edit this file with the appropriate email addresses and then load it. The nas_checkup man page provides more information on scheduled checkups.

You can create notification definitions by creating new configuration files in the /nas/site directory and loading them by using the CLI.

You can also create mail, log, and trap notifications by using the Unisphere software.

By using custom configuration files and the CLI, you can define notifications with one or more of the available actions for any event. For example, you might put all configuration information for email notifications in a file called /nas/site/mail_eventlog.cfg and all configuration information for SNMP notifications in a file called /nas/site/trap_eventlog.cfg. You can then use the CLI to configure notifications with the customized files. If you create separate configuration files for particular notifications or events, you can load and unload them individually, without affecting configurations specified in other files.

How to create a notification configuration file

The following information describes how to create a notification configuration file. Use the following format for each entry in the notification configuration files:

- A line starting with the keyword facilitypolicy and its component ID, followed by the unique facility ID for the facility and an event severity level with the following format:

  ```
  facilitypolicy <Component_ID>:<facility_ID>, <severity_level>
  ```

where:

<Component_ID> = component ID to which the facility belongs

<facility_ID> = facility ID

<severity_level> = maximum severity level for this disposition

For example, facilitypolicy 1:64, 3 specifies an entry for events from the DART UFS facility (component ID 1, facility ID 64) with a severity level of Error (3) or lower (more severe). The notification is triggered by events with severity-level numbers equal to or less than the <severity_level> specified in the <facilitypolicy> line. In the previous example, notifications would be triggered by events with severity levels of Error (3), Critical (2), Alert (1), or Emergency (0).

Note: If a facility is specified in multiple configuration files, the highest severity number (least severe) specified in the files is used. For example, if the UFS entry has a severity level of 7 (Debug) in /nas/sys/nas_eventlog.cfg file and a severity level of 2 (critical) in cwm_notify.cfg, the event log daemon uses the maximum severity number (least severe level) of 7.

- A line starting with the keyword disposition, followed by a range of event IDs within the facility, severity level, an optional directive to control unwanted or repetitious events, and the action to take when the facility issues an event in the specified event ID range. The format is as follows:

```
disposition
[range=<range_start-range_end>][severity=<severity_start-severity_end>]

[<directive>], <action>
```

where:

<range_start-range_end> = optional range of event IDs

<severity_start-severity_end> = optional range of severity levels

<directive> = optional directive that can be one of the following:

  - threshold=<n> = number of occurrences of the event before taking the associated action. This directive treats 0 as 1, so threshold=0 is the same as threshold=1 and both values invoke the associated action on the first occurrence of the event.
  - rearm=<n> = number of occurrences that must take place to invoke the associated action after the threshold is reached. This directive works in conjunction with threshold and overrides the threshold value for subsequent event occurrences.
  - resetafter=<n> = number of seconds after which threshold and rearm counters are reset if no associated event activity occurs.
  - <action> = action to take when this event is triggered. This is not optional. The defined actions are as follows:

    logfile, mail, trap, callhome, exec, udprpc, terminate

The following example specifies that the system should generate the specified SNMP trap (2) for events with event IDs in the range of 3 to 7:

disposition range=3-7, trap "/nas/site/trap.cfg 2"

The range is optional. If no range is specified, the disposition applies to all events issued by that facility. If no severity level is specified, the maximum level is used if the facility is specified in more than one configuration file.

The following example specifies that the system should generate the specified SNMP trap (2) for any event generated by this facility. Note that the comma is still required:

disposition, trap "/nas/site/trap.cfg 2"

- An optional line starting with the keyword disposition, followed by a range of severity levels and the action to take when the facility issues an event in the specified severity-level range. The format is as follows:

  ```
  disposition [<severity_level_range>], <action>
  ```

  The following example specifies that any event with severity 1 or 2 results in an email. Specifying a range of severity levels overrides the severity level specified in the <facilitypolicy> line, 7 in this case.

  facilitypolicy 1:64, 7

  disposition severity=1-2, mail "user@domain"

Events can have more than one action. For example, a specific event could have logfile, and trap actions. Create a configuration file on page 53 describes the procedure to create and modify a configuration file.

You can use comment lines, which start with the number sign (#), to document notification configuration files.

Simple Network Management Protocol

One type of notification you can configure for certain events is an SNMP notification, or SNMP trap. SNMP is a network protocol based upon a manager or agent model and is used to communicate management information between a network management station (NMS) and agents in the network elements. 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 in the network.

SNMP messages

There are three types of SNMP messages:

- Get requests from the SNMP manager — Request information from the remote device.
- Set requests from the SNMP manager — Modify the configuration of the remote device.

- Trap messages from the SNMP agent on the remote device — Provide notification and monitoring of events.

The trap message is the way an agent communicates with the SNMP manager, notifying the manager of an event, such as a crash, a restart, or a network interface card failure. The manager might respond to a trap message by polling agents to get more information.

The system responds to SNMP get requests and can generate SNMP trap messages for specified events. The values you can set or modify are community, syscontact, and location.

SNMP security and the community string

The SNMP community string is the basis for security in SNMP. The default community name is, the well-known name, public. This name should be changed to prevent unwanted access to the system. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. You can set up an SNMP trap for any system event.

Using more than one community name can provide multiple levels of security.

Note: SNMP version 1 (SNMPv1) transmits all information in clear text. Anyone monitoring the network can obtain the SNMP community name from passing traffic. RFC 1157 provides details about SNMPv1 security.

Third-party commercial SNMP products

There are many commercial third-party SNMP management products, including:

- Computer Associates Unicenter TNG
- Hewlett-Packard OpenView Network Node Manager
- Hewlett-Packard OpenView Operations
- IBM Tivoli NetView
- IBM Tivoli TME10 NetView
- IBM Tivoli TME10 Enterprise Console
- Micromuse Netcool/OMNIbus

3 Configuring

The tasks to configure events and notifications are:

Configure DNS on the Control Station

By using DNS services, it is easier to administer hostname resolution. Most of the time, DNS configuration is done at the time of system implementation.

Action
To configure the Domain Name Server (DNS), search domains, and DNS servers for the Control Station, use this command syntax: `$ nas_cs -set -dns_domain <dns_domain_name> -search_domains <domain_name>[,...] -dns_servers <ip_address>[,...]` where: *<dns_domain_name>* = domain name of the primary Control Station *<domain_name>* = DNS domains searched *<ip_address>* = IPv4 or IPv6 addresses of the DNS servers Examples: To set the DNS domain, search domains, and DNS servers for the Control Station that uses IPv4 addresses, type: `$ nas_cs -set -dns_domain nasdocs.emc.com -search_domains localdomain -dns_servers 172.24.175.172, 172.24.175.173` To set the DNS domain, search domains, and DNS servers for the Control Station that uses IPv6 addresses, type: `$ nas_cs -set -dns_domain nasdocs.emc.com -search_domains localdomain -dns_servers 3ffe:0000:3c4d:0015:0000:0000:0300:00aa, 3ffe:0000:3c4d:0015:0000:0000:0300:00bb` To set the DNS domain, search domains, and DNS servers for the Control Station that uses a mix of addresses, type: `$ nas_cs -set -dns_domain nasdocs.emc.com -search_domains localdomain -dns_servers 172.24.175.172, 3ffe:0000:3c4d:0015:0000:0000:0300:00bb, 172.24.175.173` Note: For VNX unified/file and block systems version 7.1 or later, you can use Unisphere to configure IPv4 and IPv6 DNS servers. In Unisphere select All Systems and go to Domains ➤ Configure DNS (Local Domain task list). As an alternative, select a system and go to Settings ➤ Configure DNS (Network Settings task list). For VNX gateway systems version 7.1 or later, in Unisphere go to System ➤ Control Station Properties (Network Settings task list).

Check if email is working properly before configuring notifications

This procedure combines the commands echo, mail, and hostname. The results of the echo command are passed to the mail command and the hostname (Control Station name) is sent to the recipient.

Action
To test if email is working properly before configuring notifications, use this command syntax: `$ echo test from `hostname` | mail -v -s "`hostname` subject" <recipient email address>` Ensure to enclose hostname in single, backward quotes; otherwise, the command fails. The man pages for echo, mail, and hostname commands provide more information. where: **-v** = verbose output option of mail command **-s** = subject option of the message **`hostname`** = result of hostname command that is passed to the requested commands (echo, and mail) *<subject>* = email subject *<recipient email address>* = recipient's email address Example: To send a test email to user1, type: **$ echo test from `hostname` | mail -v -s "`hostname` test message" user1@nasdocs.emc.com**
Output
The following output provides information about the state of email service on the Control Station: `user1@nasdocs.emc.com... Connecting to eagle.lss.nasdocs.emc.com. via esmtp...` `220 igw ESMTP Sendmail 8.10.1/8.10.1; Tue, 22 Jun 2004 11:14:19 -0400 (EDT)` `>>> EHLO manatee6.pag.nasdocs.emc.com` `250-igw.nasdocs.emc.com Hello [192.168.80.140], pleased to meet you` `.` `.` `.` `>>> MAIL From:<nasadmin@manatee6.pag.nasdocs.emc.com> SIZE=104` `250 2.1.0 <nasadmin@manatee6.pag.nasdocs.emc.com>... Sender ok` `>>> RCPT To:<user1@nasdocs.emc.com>` `250 2.1.5 <user1@nasdocs.emc.com>... Recipient ok` `>>> DATA` `354 Enter mail, end with "." on a line by itself` `>>> .` `250 2.0.0 i5MFEJr00252 Message accepted for delivery` `user1@nasdocs.emc.com... Sent (i5MFEJr00252 Message accepted for delivery)` `Closing connection to eagle.lss.nasdocs.emc.com.` `>>> QUIT` `221 2.0.0 igw.nasdocs.emc.com closing connection`

Note
In the resulting output from the command, the following line indicates that email on the Control Station is working properly: `250 2.1.5 <user1@nasdocs.emc.com>... Recipient ok,` If the recipient did not receive the email, there might be network problems external to the Control Station. Check if sendmail is running on page 83 provides more information on what to do if email notifications are not working as expected.

You can also test email notifications by using the Test button. For this, create an event notification for email using the Unisphere software. Then, go to **System ➤ Monitoring and Alerts ➤ Notifications ➤ Event**. Click **Test** on the notification list. Configure notifications by means of email on page 31 provides another means of setting up and testing email notifications.

Configure notifications by means of email

Email notifications allow you to configure email for multiple, serious system events in one place, eliminating the need to configure notifications with the same email recipients.

The tasks to configure email notifications are:

Note: Events will continue to be sent as callhomes to EMC support if Connect Home is enabled.

You can continue to configure email notifications for specific events. You can also configure and test email notifications by using the Unisphere software. Go to **System** and from the task list, under **Service Tasks**, select **Manage Email User**.

Enable email notifications

Action
To enable email notification, use this command syntax: `$ nas_emailuser -modify -enabled {yes | no}` where: yes = enabled. Example: To enable email notification, type: `$ nas_emailuser -modify -enabled yes`
Output
`OK`

Configure email notifications

Before you begin

If DNS is not configured on the Control Station, email notifications will not be delivered. *Configuring VNX Naming Services* provides information about configuring DNS.

The mailbox portion of the fully qualified domain name uses the following ASCII characters: a–z, A–Z, 0–9, !, #, $, %, &, *, +, -, /, =, ?, ^, _, `, {, |, }, ., ‘, and ~. Periods cannot be the first or last character in the mailbox. Alphanumeric strings are accepted. Enclose email addresses in single quotes. For example: ’storage_admin1@nasdocs.emc.com’. You can use single quotes within an email address, but you must escape them correctly. The first example shows how to use a single quote on its own in an address, while the second shows how to use a single quote within a single-quoted address:

- admin\'email@nasdocs.emc.com
- 'first'\''admin@nasdocs.emc.com,second'\''admin@nasdocs.emc.com'

You can customize the subject prefix to meet your specific requirements, such as email filtering.

Procedure

Action
To configure email notifications, use this command syntax: `$ nas_emailuser -modify -to {<email_addr>,...} -cc {<email_addr>,...} -email_server <email_server> -subject_prefix <email_subject> -from <email_addr>`

Action
where: *<email_addr>* = for -to, one or more comma-separated, email addresses, from 3 to 255 characters, in the format 'mailbox@fully-qualified-domain-name'. Each individual email address can be a maximum of 63 characters. *<email_addr>* = for -cc, one or more optional, comma-separated, email addresses, from 3 to 255 characters, in the format 'mailbox@fully-qualified-domain-name'. Each individual email address can be a maximum of 63 characters. *<email_addr>* = for -from, sender's optional email address, from 3 to 63 characters, in the format 'mailbox@fully-qualified-domain-name'. If you do not specify a sender, an address in the format root@<hostname> is used by the system. For example: 'root@doc.emc.com'. *<email_server>* = the optional email server that accepts and routes the email notifications. Specifies an optional IPv4 or IPv6 address or the fully qualified domain name, from 1 to 63 characters, of the email server. The IPv4 addresses 0.0.0.0 and 255.255.255.255 are not allowed. *<email_subject>* = the optional subject prefix of the email notification, from 1 to 63 printable ASCII characters. The default subject prefix is VNX Notification. Example: To configure email notifications using email server 10.6.50.122 from administrator to support, while copying engineering and documentation, type: **$ nas_emailuser -modify -to support1@nasdocs.emc.com, support2@nasdocs.emc.com -cc engineering@nasdocs.emc.com, documentation@nasdocs.emc.com -email_server 10.6.50.122 -subject_prefix "VNX Notification -- Jan 10, 2011" -from administrator@nasdocs.emc.com**
Output
OK

Display an email notifications configuration

Action
To display the email notifications configuration, type: **$ nas_emailuser -info**
Output
Service Enabled = Yes Recipient Address(es) = xu2018support1@nasdocs.emc.comxu2019,xu2019support2@nasdocs.emc.comxu2019 Carbon copy Address(es) = xu2018engineering@nasdocs.emc.comxu2019,xu2019documentation@nasdocs.emc.comxu2019 Email Server = 10.6.50.122 Subject Prefix = VNX Notification -- Jan 10, 2011 Sender Address = xu2018administrator@nasdocs.emc.comxu2019

The following output shows an example of an email notification based on the configuration information that you supplied and generated when a BoxMonitor error occurs. Inventory information for your system is provided toward the bottom of the message. This information is abbreviated for this example.

Output

```
From: administrator@nasdocs.emc.com
To: support1@nasdocs.emc.com,support2@nasdocs.emc.com
CC: engineering@nasdocs.emc.com,documentation@nasdocs.emc.com
Subject: VNX Notification -- Jan 10, 2011

Event Time: Jan 10 03:14:07 2038

Brief Description: Slot 2: Enclosure 0 blade 1 I2C PSA bus error.

Full Description:

This is a management switch internal error. The error is logged when the
management switch is not able to control or query the status of enclosure

components because of a hardware problem that may be caused by a component

or connection outside the management switch.

Recommended Action:

Examine the /nas/log/sys_log to locate the cause of the management switch

event. This may be caused by bad I2C connections on the motherboard or the

enclosure. This can also happen when the two management switches in the
enclosure have conflicting views of the system. Replacing the enclosure
hardware or one of the management switches may be necessary.



Name: vnxdev-36
Model: VNX5500
Serial Number: FNM00102000265
Software Version: 05.31.000.3.091

Severity: CRITICAL
Component: CS_PLATFORM
Facility: BoxMonitor
Message ID: 78928609795
```

Output

```
------------------------------------------------------------------------
System Configuration Snapshot: Sun Jan 10 03:15:01 EST 2011
Control Station Slot No: 0
/nas/sbin/model:

VNX5500
/nas/bin/nas_inventory -list:
Component                          Type              Status  System ID
Shelf 0/0 Battery A                Battery           OK      VNX VNX5500
FNM00102000265
Shelf 0/0 Battery B                Battery           OK      VNX VNX5500
FNM00102000265
VNX VNX5500 FNM00102000265         VNX               OK      VNX VNX5500
FNM00102000265
VNX VNX5500 FNM001020002652007     VNX               OK      VNX VNX5500
FNM001020002652007

                                        .
                                        .
                                        .
------------------------------------------------------------------------
Depending on your service level agreement, you can contact your service
provider to resolve the problem or follow the instructions in the recom-
mended
actions.
```

Test an email notification configuration

Test an email notification posts a test event, which delivers an email notification to the configured recipients.

Action
To test email notifications, type: **$ nas_emailuser -test**
Output
OK

After you finish

Confirm with the configured recipients that they received the test email with the correct system identification information.

Disable email notifications

Action
To disable email notification, use this command syntax: $ **nas_emailuser -modify -enabled** {**yes** | **no**} where: **no** = disabled. Example: To disable email notification, type: **$ nas_emailuser -modify -enabled no**
Output
OK

Re-initialize email notifications

If the configuration file becomes corrupt or is deleted, you can use the -init option to re-initialize the email notification feature. However, you should only use this option if you are directed to run it by a system message.

Action
To re-create the configuration file, type: **$ nas_emailuser -init**
Output
OK

Gather required information

To specify notifications for specific events, you need to gather information about event facilities and the events they generate.

The tasks to gather required information are:

1. Determine facilities in a component that generate events on page 38
2. Determine events associated with a facility on page 40
3. Locate more information about an event on page 42
4. Determine a list of all possible actions on page 43
5. Determine which events trigger an action on page 44

Determine facilities in a component that generate events

1. To view the list of components, type:

   $ nas_event -list -component -info

   Output:

   ```
   ID      Component
   1       DART
   2       CS_CORE
   6       CS_PLATFORM
   ```

2. To view a list of all facilities of the component DART that generate events, type:

   $ nas_event -list -component DART -facility -info

```
Output:
DART(1)
|->Id     Facility
   24     ADMIN
   26     CAM
   27     CFS
   36     DRIVERS
   40     FSTOOLS
   43     IP
   45     KERNEL
   46     LIB
   51     NDMP
   52     NFS
   54     SECURITY
   56     SMB
   58     STORAGE
   62     TIMESYNC
   64     UFS
   68     LOCK
   70     SVFS
   72     XLT
   73     NETLIB
   75     MGFS
   77     VRPL
   78     LDAP
   81     VC
   83     RCPD
   84     VMCAST
   86     CHAMII
   93     USRMAP
   96     DHSM
  101     ACLUPD
  102     FCP
  107     VCS
  108     REP
  111     DPSVC
  115     SECMAP
  117     WINS
  118     DNS
  122     DBMS
  144     PERFSTATS
  146     CEPP
  148     DEDUPE
```

Determine events associated with a facility

Action
To view a list of events and event ID numbers associated with a facility, use this command syntax: `$ nas_event -list -component <component> -facility <facility>` where: *<component>* = component name *<facility>* = case-sensitive facility name A component must be listed with a facility to view the list of events generated by that facility. Example: To list the events associated with the DART facility, type: **`$ nas_event -list -component DART -facility SVFS`**

Output

```
DART(1)
|--> SVFS(70)
BaseID     Severity       Brief_Description
1         WARNING(4)     FSID:${id,5,%u} SavVol:${vol,8,%s} MaxSize:${max-
size,5,%u}
                           MB %Full(hwm=${hwm,2,%d}) reached
(t:${ticks,3,%q})
2          ERROR(3)        FSID:${id,22,%u} SavVol:${vol,76,%s} Inactive
3          INFO(6)        Restore completed successfully.(PFS_VOLID:${vol-
name,76,%s})
4          INFO(6)         Restore in progress ${percent,5,%1u} percent
done. (PFS_VOLID:${volid,
                           76,%s})
5          EMERGENCY(0)    FSID:${id,22,%u} SavVol:${vol,76,%s} conversion
 paused
                           (t:${ticks,6,%llu})
6          ERROR(3)        FsVol:${FsVolName,76,%s} SavVol:${SaveVol-
Name,76,%s} Inactivate ALL ckpt
```

List all events on the Control Station

Action
To view a list of all events on the Control Station, type: **`$ export NAS_DB=/nas ; /nas/bin/nas_event -l -c -i \	awk '/^[ ]*[0-9]+/{print $1}'	xargs -n1 -i bash -c \ "export COMP={} ; /nas/bin/nas_event -l -c {} -i	awk '/^[ ]*[0-9]+/{print \$1}'\	xargs -n1 -i /nas/bin/nas_event -l -c \$COMP -f \{\} -id"	fgrep -v 'DEBUG(7)'`**

Output

```
DART(1)
|--> ADMIN(24)
MessageID       BaseID     Severity       Brief_Description
68989485057     1          EMERGENCY(0)   ${command,8,%s}
DART(1)
|--> CAM(26)
MessageID       BaseID     Severity       Brief_Description
86169485313     1          WARNING(4)     The SCSI HBA ${hbano,2,%d} is
operating
normally.
86169485314     2          WARNING(4)     Warning: The SCSI HBA
${hbano,2,%d} has
failed.
86169485315     3          WARNING(4)     Warning: The SCSI HBA
${hbano,2,%d} is
inaccessible.
81874518020     4          ERROR(3)       I/O Error:
c${path_id,5,%u}t${target_i
d,5,%u}l${target_lun,5,%u} Irp 0x${irp,2,%08x}  CamStatus 0x${cam_sta-
tus,2,%02x}
ScsiStatus 0x${scsi_status,2,%02x} Sense
0x${sns_key,2,%02x}/0x${asc,2,%02x}/0x
${asq,2,%02x}
DART(1)
|--> CFS(27)
MessageID       BaseID     Severity       Brief_Description
86169550849     1          WARNING(4)     filesystem size threshold
(${usageHWM,
2,%d}%) crossed (fs ${mountPath,55,%s})
86169550851     3          WARNING(4)     The file system size (fs
${mountPath,8
,%s}) dropped below the threshold of (${usageHWM,2,%d}%)
86169550852     4          WARNING(4)     File system size threshold
(${size,5,%
u}%) was crossed for (fs ${fsname,68,%s})
86169550853     5          WARNING(4)     The file system size (fs
${mountPath,8
,%s}) dropped below the threshold of (${usageHWM,2,%d}%)
94759485446     6          INFO(6)        FsId: ${id,5,%lu} MaxSize:
${maxSize,2
,%d} MB HWM: ${usage,2,%d}%. ${extSizeStr,8,%s}
94759485447     7          INFO(6)        The file system size (fs
${mountPath,8
,%s}) dropped below the threshold of (${usageHWM,2,%d}%)
94759485448     8          INFO(6)        The file system size (fs
${mountPath,8
,%s}) dropped below the threshold of (${usageHWM,2,%d}%)
                                          .
                                          .
                                          .
```

After you finish

If you want to create a searchable file containing all events, redirect the output to a file.

Locate more information about an event

To locate more information about an event, determine the message ID for the event and then use the message ID to display the additional information:

1. To view a list of events, and associated message IDs, for a facility, use this command syntax:

   $ **nas_event -list -component** *<component>* **-facility** *<facility>* **-id**

   where:

   <component> = component name

   <facility> = case-sensitive facility name

   Example:

   To list the message IDs for all events of a facility, type:

   $ nas_event -list -component DART -facility SVFS -id

   Output:

```
DART(1)
|--> SVFS(70)
MessageID       BaseID     Severity       Brief_Description
86172368897     1          WARNING(4)     FSID:${id,5,%u}
SavVol:${vol,8,%s} MaxSize:${maxsize,5,%u} MB %Full(hwm=${hwm,2,%d})
reached (t:${ticks,3,%q})
81877401602     2          ERROR(3)       FSID:${id,22,%u}
SavVol:${vol,76,%s} Inactive
94762303491     3          INFO(6)        Restore completed successfully.
 (PFS_VOLID:${volname,76,%s})
94762303492     4          INFO(6)        Restore in progress
${percent,5,%1u} percent done. (PFS_VOLID:${volid,76,%s})
68992499717     5          EMERGENCY(0)   FSID:${id,22,%u}
SavVol:${vol,76,%s} conversion paused (t:${ticks,6,%llu})
81877401606     6          ERROR(3)       FsVol:${FsVolName,76,%s}
SavVol:${Save VolName,76,%s} Inactivate ALL ckpt
```

   Note: The number 81877401606 is a message ID.

2. To locate more information about an event, use this command syntax:

   $ **nas_message -info** *<message_id>*

   where:

   <message_id> = multidigit ID number

   Example:

   To obtain additional information about an event by using the message ID, type:

   $ nas_message -info 81877401606

   Output:

```
MessageID = 81877401606
BaseID    = 6
Severity  = ERROR
Component = DART
Facility  = SVFS
Type      = EVENT

Brief_Description  = FsVol:${FsVolName,76,%s} SavVol:${SaveVolName,76,%s}
 Inactivate ALL ckpt

Full_Description   = All checkpoints are inactive due to limited space
on the save volume.

Recommended_Action = Check the system configuration to see if more space
 can be allocated for the save volume.
```

Determine a list of all possible actions

Action
To view a list of all possible actions that you can take, type: **$ nas_event -list -action -info**
Output
action terminate trap exec mail callhome logfile

Note
Mail notification is not a default; therefore, it does not appear in the list of possible actions until an event is configured for mail notification.

Determine which events trigger an action

Action
To view a list of events that trigger a particular action, use this command syntax: `$ nas_event -list -action <action>` where: *<action>* = name of the action: mail, trap, logfile, callhome, exec, terminate, updrpc Example: To list the events that trigger a trap action to EMC, type: **`$ nas_event -list -action trap | more`**
Output
`CS_PLATFORM(6)` `|--> BoxMonitor(131)` `BaseID Severity Brief_Description` `1 CRITICAL(2) EPP failed to initialize.` `3 CRITICAL(2) Failed to create ${threadname,8,%s} thread.` `4 CRITICAL(2) SIB Read failure: ${string,8,%s}` `.` `.` `CS_PLATFORM(6)` `|--> SYR(143)` `BaseID Severity Brief_Description` `5 INFO(6) The SYR file ${src_file_path,8,%s} with ${dest_extension,8,%s} extension is attached.`

Configure SNMP trap notifications

The tasks to configure SNMP traps for notifications are:

1. Modify the MIB file for SNMP traps on page 45
2. Configure SNMP traps on page 46
3. Send a test SNMP trap on page 47
4. Receive a test SNMP trap on page 49
5. Configure SNMP on Data Movers on page 52

Modify the MIB file for SNMP traps

If the default SNMP traps do not properly describe the condition that you want to trap, you can define additional SNMP traps by modifying the system MIB file:

1. Modify the MIB, /nas/sys/emccelerra.mib, to include the following lines:

```
celCFS TRAP-TYPE
ENTERPRISE emcCelerra
VARIABLES {celEvent}
DESCRIPTION
     "<description>"
::=<unique-id-number>
```

where:

<description> = description of the trap.

<unique-id-number> = arbitrary, yet unique, trap number for the event that you specified in the notification configuration file. Some trap numbers are reserved. Ensure to check the trap definition section of the MIB, /nas/sys/emccelerra.mib, before assigning a trap number.

Note: Ensure that the trap number in the MIB and in the configuration file you are modifying are the same. The trap number correlates a particular trap in the MIB with events that you specify in the configuration file. Save a copy of the modified MIB in another location because it is overwritten when the system is upgraded. On HP OpenView, load the MIB by using Options ➤ Load/Unload MIBs:SNMP.

---

2. Configure the MIB on the SNMP Manager.

Configure SNMP traps

An SNMP trap configuration file informs the Control Station which SNMP managers should receive a message when a trap occurs. Specify which trap configuration file (located in the /nas/site directory) to use when you configure a trap notification. A trap configuration file can contain multiple entries, one per line. Modifications to the file are maintained when the system is upgraded.

Before you begin

The Control Station can use /etc/hosts, NIS, or DNS to resolve hostnames and IP addresses. These services must be configured and running. In addition, set up the /etc/nsswitch.conf file to determine the search order the Control Station uses when resolving names. The /etc/hosts file is a text file listing hostnames and their corresponding IP addresses. If you use hostnames in a trap configuration file, be sure to add the hostnames and IP addresses to the /etc/hosts file if you are not using DNS for name resolution. The changes take effect as soon as the file is saved. There is no need to restart the system.

Procedure

Action
By using a text editor, add the following lines to the file /nas/site/trap.cfg to configure the SNMP Managers: **#snmp trap configuration file** **snmpmanager** *<hostname>* **; communityname** *<community>* where: snmp trap configuration file = comment line snmpmanager = keyword *<hostname>* = hostname or IPv4 or IPv6 address ; = separator character, preceded and followed by a space communityname = keyword *<community>* = community name for the SNMP manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Example: `#snmp trap configuration file` `snmpmanager 128.154.11.20 ; communityname xyz_community` `snmpmanager host1 ; communityname xyz_community`

Send a test SNMP trap

You can use nas_snmptrap and snmptrapd -f -Le -Lf on the Control Station to send a test SNMP trap.

Before you begin

For VNX series Control Stations, snmptrapd is already running. To prevent the generation of two sets of logs when testing an SNMP trap on these systems, as root kill the existing snmptrapd service run by typing:

```
# killall snmptrapd
```

To restart snmptrapd services after testing, type:

```
# /usr/sbin/snmptrapd -c /nas/sys/snmptrapd.conf -p 162 -u /var/run/snmptrapd.pid
>/dev/null 2>&1 &
```

Procedure

1. Log in to the Control Station as root.
2. Ensure that the Control Station is listed in the trap.cfg file.

   Example:

   ```
   snmpmanager localhost ; communityname public
   ```

3. Start the SNMP trap daemon on the Control Station by typing:

   ```
   # /usr/sbin/snmptrapd -f -Le -Lf /nbsnas/var/log/my_eventlog_messages &
   ```

   Note: Because snmptrapd is already running on VNX series Control Stations, this command returns an informational error message. Some systems do not have the /nbsnas directory. If this is true for your system, use the /nas/var/log directory.

   The **&** starts the daemon in the background and allows you to continue typing commands. Messages are logged to the my_eventlog_messages file.

   You can enable SNMP on the Control Station through the Unisphere software. Go to the **Settings ➤ Network ➤ Settings for File ➤ Network Services** tab. You can also enable and disable SNMP on Data Movers.

4. From root, send a trap by using this syntax:

   ```
   # /nas/sbin/nas_snmptrap <config_file_path> -m /nas/sys/emccelerra.mib -r
   <trap_number> -f <facility_id> -i <event_id> -s
   <severity_level> -d "<description>"
   ```

   where:

   <config_file_path> = path of the trap configuration file

   /nas/sys/emccelerra.mib = MIB file

<trap_number> = unique trap number for the event

<facility_id> = ID number of the facility generating the event

<event_id> = event ID number

<severity_level> = severity level of the event

<description> = description of the trap (up to 255 characters)

Example:

```
# /nas/sbin/nas_snmptrap /nas/site/trap.cfg -m /nas/sys/emccelerra.mib  -r 1 -f
64 -i 5 -s 7 -d "test SNMP traps"
```

Output:

```
2003-01-20 17:05:17 eng192152 [192.168.192.152] (via localhost.localdomain

[127.0.0.1]) TRAP, SNMP v1, community public.
           enterprises.1139.2 Enterprise Specific Trap (1) Uptime: 14
days, 1:39:04.68
           enterprises.1139.2.1.1.1 = 64
           enterprises.1139.2.1.1.2 = 5
           enterprises.1139.2.1.1.3 = 7
           enterprises.1139.2.1.1.4 = "test SNMP traps "
```

You can create an event notification for a trap in the Unisphere software. To create, go to **System ➤ Monitoring and Alerts ➤ Notifications ➤ Event**. Then, click **Test** on the notification list.

Receive a test SNMP trap

You can receive a test SNMP trap by configuring the Control Station as the target.

1. Set up the SNMP Manager to receive Virus Checker SNMP traps by adding the following line to the file /nas/site/trap.cfg:

   snmpmanager *<target>* **; communityname** *<public>*

   where:

   <target> = IPv4 or IPv6 address, hostname, or fully qualified domain name of the SNMP Manager that gets the traps.

   <public> = community name to use for authentication with the SNMP Manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public.

2. Modify the MIB, found at /nas/sys/emccelerra.mib, to include the following lines:

   ```
   celVC TRAP-TYPE
   ENTERPRISE emcCelerra
   VARIABLES {celEvent}
   DESCRIPTION

       "Trap message will be sent in the event of a VC service associated
   notification request."
   ::=11
   ```

   where:

   11 = arbitrary, yet unique, trap number for the event you specified in the my_eventlog.cfg file

   Save a copy of the modified MIB in another location because it is overwritten when the system is upgraded. On HP OpenView, load the MIB by using **Options ➤ Load/Unload MIBs:SNMP**.

3. Configure MIB on the SNMP Manager.

4. Ensure that the Control Station name is in the /etc/hosts file:

   ```
   # Do not remove the following line, or various programs
   # requiring network functionality will fail.
   127.0.0.1           localhost.localdomain localhost
   <address>           <example_cs0> <example_cs0.nasdocs.emc.com>
   ```

   where:

   <address> = IPv4 or IPv6 address of the Control Station. The IPv4 address is always present. The IPv6 address is present only if IPv6 is configured.

   <example_cs0> = Control Station name and *<nasdocs.emc.com>* is the name of the domain that includes the mail server. Substitute Control Station and domain information for the ones in the example.

Note: Underscores are used in the example text here for readability only. The underscore is an invalid character in the Control Station name and should not be used.

5. Create a new notification configuration file named /nas/site/my_eventlog.cfg by copying /nas/sys/nas_eventlog.cfg to my_eventlog.cfg.

6. Use a text editor to add the following statements to my_eventlog.cfg:

```
# Virus Checker Events
# email and trap notification for any Virus Checker event
#
facilitypolicy 1:81,7
     disposition range=1-28, mail "storadmin01@nasdocs.emc.com"
     disposition range=1-28, trap "/nas/site/trap.cfg 11"
```

where:

`facilitypolicy 1:81` = dispositions that need to be applied to events in the VC facility (facility ID 81) of the DART component (component ID 1).

`7` = severity-level threshold (captures events of severity 7 or lower).

`disposition range=1-28` = events 1 through 28, which equate to all VC events.

`storadmin01@nasdocs.emc.com` = email address that receives email notification. Replace these with one or more email addresses at company.

`11` = arbitrary, yet unique, trap number you associate with the event in the MIB (code shown in step 2).

Determine events associated with a facility on page 40 provides information about determining which events are associated with which facilities.

7. Using the full pathname, load the new notification configuration file by using the following command:

```
$ nas_event -Load /nas/site/my_eventlog.cfg
```

Output:

```
EventLog : will load /nas/site/my_eventlog.cfg...done
```

Note: You must unload the configuration file before making additional changes. You must specify the absolute path of the configuration file to unload.

8. Verify that the new notifications (email and traps) have been accepted by using the following commands:

```
$ nas_event -list -action mail
```

or

```
$ nas_event -list -action trap
```

Note: Mail is not a default action. Until an event is configured for mail notification, the command nas_event -list -action mail returns an error.

The output should at least display:

```
DART(1)
|--> VC(81)
BaseID     Severity      Brief_Description
1          NOTICE(5)     The virus checker is running normally.
2          ERROR(3)      ${type,8,%s} high water mark reached.
3          WARNING(4)    ${type,8,%s} low water mark reached.
4          ERROR(3)      No virus checker server is available.
5          ERROR(3)      No virus checker server is available. CIFS is
stopped.
6          ERROR(3)      No virus checker server is available. Virus
checking
           is stopped.
7          ERROR(3)      '${filename,8,%s}' was not checked.
8          NOTICE(5)     Server ${ipaddr,8,%s} is online. RPC program
version
${rpc,2,%d}, ${cava,8,%s}.
9          ERROR(3)      Error on server ${ipaddr,8,%s}:
${status,8,%s}${winerror,8,%s}, RPC program version ${rpc,2,%d},
${cava,8,%s}.
10         NOTICE(5)     The virus checker is started.
11         NOTICE(5)     Scanning was completed for file system
${fsid,2,%d} mounted
           on ${mountPath,8,%s}. ${dirs,2,%d} directories were scanned
and
           ${files,2,%d} files were submitted to the scan engine.
12         ERROR(3) Scanning was aborted for file system ${fsid,2,%d}
mounted on
         ${mountPath,8,%s} for this reason: ${error,8,%s}. ${dirs,2,%d}

         directories were scanned and ${files,2,%d} files were submitted
 to the
           scanengine.
13         ERROR(3)      The antivirus (AV) engine deleted ${file,8,%s},
 ${user,8,%s}.
14         ERROR(3)      The antivirus (AV) engine renamed ${file,8,%s},
 ${user,8,%s}.
15        WARNING(4)    The antivirus (AV) engine modified ${file,8,%s},
 ${user,8,%s}.
16         NOTICE(5)     The virus checker is stopped.
```

9. Generate a test Virus Checker event by using the following command:

```
$ /nas/sbin/postevent -c 1 -f 81 -I 16 -s 5
```

The following shows SNMP traps from the Virus Checker facility.

Note: For traps with a destination that resolves to an IPv6 address, the trap will be sent to the IPv6 address, but the IPv4 address of the Control Station that sent the trap will be embedded in the trap message.

Output
2008-02-06 13:32:42 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1) TRAP, SNMP v1, community public SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (11) Uptime: 19:44:34.83 SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 81 SNMPv2- SMI::enterprises.1139.2.1.1.2 = INTEGER: 4 SNMPv2- SMI::enterprises.1139.2.1.1.3 = INTEGER: 3 SNMPv2- SMI::enterprises.1139.2.1.1.4 = STRING: "Feb 6 13:32:42 2008 VC:3:4 No virus checker server is available. " 2008-02-06 13:32:50 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1) TRAP, SNMP v1, community public SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (11) Uptime: 19:44:42.91 SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 81 SNMPv2- SMI::enterprises.1139.2.1.1.2 = INTEGER: 16 SNMPv2- SMI::enterprises.1139.2.1.1.3 = INTEGER: 5 SNMPv2- SMI::enterprises.1139.2.1.1.4 = STRING: "Feb 6 13:32:50 2008 VC:5:16 The virus checker is stopped. "

Configure SNMP on Data Movers

The server_snmpd command manipulates SNMP configuration values of the server agent for the specified Data Mover.

The values you can set or modify are community, syscontact, and location. *Using SNMPv3 on VNX* and *EMC VNX Command Line Interface Reference for File* provides more information about this command.

Action
To assign a new value of private to a server SNMP agent's community for a Data Mover, type: **$ server_snmpd server_2 -modify -community private**
Output
server_2 : OK

Customize notifications

To customize notifications, create the configuration file and load it on the system. You can also create log, mail, or trap notifications through the Unisphere software.

The tasks to customize notifications are:

1. Create a configuration file on page 53
2. Load a configuration file on page 55

3. Verify the configuration file loaded on page 55

Create, load, and verify tasks can be done through the Unisphere software. To accomplish these tasks, go to **System ➤ Monitoring and Alerts ➤ Notifications ➤ Event**. The actions are limited to email, trap, and logfile. The online help has more details.

Note:

1. In case of CLI, if the nas_emailuser command is used to specify the sender address, custom notifications created in the format "mailuser @domain.com" will use the root user instead of the sender address specified in the command.
2. In the Unisphere software you can specify the email address by selecting System and from the task list, under Service Tasks, selecting Manage Email User. However, if you create custom notification by using System ➤ Monitoring and Alerts ➤ Notifications, it will use the root user instead of the address specified in the "Sender Email Address."

Create a configuration file

You can create and modify configuration files to fit your specific system environment:

1. Log in to the Control Station.
2. Change to the /nas/site directory by typing:

   ```
   $ cd /nas/site
   ```

3. Copy the /nas/sys/nas_eventlog.cfg file to the current directory so that you can use it as a template. Rename it by using this command syntax:

   ```
   $ cp /nas/sys/nas_eventlog.cfg new_filename
   ```

   where:

   new_filename = name of the customized configuration file

   Example:

   ```
   $ cp /nas/sys/nas_eventlog.cfg custom_event_config.cfg
   ```

   Note: Do not use the name nas_eventlog.cfg as the name for the customized configuration file. Do not modify any of the default notification configuration files.

   ---

4. Use a text editor to modify *new_filename*.

   where:

   new_filename = name of the customized configuration file

5. If you copied /nas/sys/nas_eventlog.cfg as the basis for the customized file, delete everything in the file except those lines related to the facility policies and dispositions

you want to change. This will help you avoid unintentionally changing default notifications.

6. Add the following statements to the notification file to associate events with the actions you want:

```
# UFS
#
facilitypolicy  1:64, 3
    disposition range=0-7, logfile "/nas/log/sys_log"
    disposition range=4-7, mail
"nasadmin@nasdocs.emc.com,helpdesk@nasdocs.emc.com"
    disposition range=3-7, trap "/nas/site/trap.cfg 2"
```

where:

`facilitypolicy 1:64` = dispositions that need to be applied to events in the UFS facility (facility ID 64) of the DART component (component ID 1)

`3` = severity level of Error (3) or worse. If a facility is specified in more than one configuration file, the maximum severity level specified is used

`logfile` = entry added to the /nas/log/sys_log file for events 0 through 7

`mail` = comma-separated email addresses sent for events 4 through 7

`trap` = SNMP trap (2) report sent for events 3 through 7. The Control Station consults /nas/site/trap.cfg for information about where to send the trap

Event notification actions on page 90 provides a complete list of actions. Configure SNMP traps on page 46 provides more information on trap configuration files.

7. Save the file and then exit.

Notifications on page 21 provides more information about how to create a notification configuration file. When you set up a new notification, ensure that you test it and that the email is reaching the intended recipient.

Load a configuration file

After creating the customized configuration file, you must load the file for new notifications to take effect:

1. Log in to the Control Station.

   If you create separate configuration files, the order in which the configuration files are loaded determines the order in which the actions occur. The actions specified in the first file you load occur before the actions specified in subsequent files.

2. Load the customized configuration file by using this command syntax:

   `$ nas_event -Load <customized_file>`

   where:

   <customized_file> = full pathname of the customized configuration file

   Example:

   ```
   $ nas_event -Load /nas/site/custom_event_config.cfg
   ```

   Output:

   ```
   EventLog : will load /nas/site/custom_event_config.cfg...done
   ```

   Note: Do not put customized configuration files in the /nas/sys directory or the files will be overwritten when the system is upgraded.

Verify the configuration file loaded

Action
To verify that the customized configuration file is loaded, type: **$ nas_event -Load -info**
Output
The list of loaded configuration files appears: `Loaded config. files:` `1: /nas/sys/nas_eventlog.cfg` `2: /nas/sys/storage_eventlog.cfg` `3: /nas/http/webui/etc/web_client_eventlog.cfg` `4: /nas/site/custom_event_config.cfg` You might need to modify the configuration of the SNMP management application before it can use these changes. Configure SNMP trap notifications on page 45 provides more information.

SNMP traps and email notifications: Example configurations

The following sections provide examples of configuring SNMP traps and email notifications to notify you:

- When file system usage exceeds certain limits on page 56
- When a SnapSure SavVol usage reaches its high water mark on page 60
- When there are Virus Checker events on page 64
- When a hard or soft quota is exceeded on page 69
- ddm/esa/3700018275a1a2DM5_OBJECT_SPEC=RELATION_ID&DM5_ANCHOR=#topic_DE7E7EF14BED4EA1A61F60A51FDB5219

When file system usage exceeds certain limits

You can configure the system to generate an SNMP trap and an email notification to several file system administrators when the size of a file system exceeds a certain percentage full, based on system tracking of the file system size threshold. The default file system size threshold is 90 percent full. This applies to the global built-in CFS event to check each file system against the fsSizeThreshold parameter.

Using the Unisphere software, you can create individualized threshold notifications for file systems. For example, you can notify when a particular file system hits 80 percent usage and also notify when a different file system hits 85 percent usage. The Unisphere software defines these notifications as resource notifications and they are independent of any notifications set on the CFS event.

Monitoring the percentage full is useful because file system performance can degrade as its used space approaches 100.

Managing Volumes and File Systems with VNX Automatic Volume Management and *Managing Volumes and File Systems for VNX Manually* provide information about how to change this threshold to another percentage value. See the description about changing the fsSizeThreshold parameter.

You need root access to the system.

By default, an event is generated on the system when the used space in a file system exceeds 90 percent of the total capacity of the file system.

Configure the system to generate a notification when file system usage exceeds certain limits

In the Unisphere software, you can create individualized threshold notifications for file systems. For example, you can notify when a particular file system hits 80 percent usage and also notify when a different file system hits 85 percent usage. The Unisphere software defines these notifications as resource notifications.

1. Configure DNS to enable email notification:

   $ **nas_cs -set -dns_domain** *<dns_domain_name>* **-search_domains** *<domain_name>[,...]* **-dns_servers** *<ip_address>[,...]*

   where:

   <dns_domain_name> = domain name of the primary Control Station

   <domain_name> = DNS domains searched

   <ip_address> = IPv4 or IPv6 addresses of the DNS servers

   Most of the time, DNS configuration is done at the time of system implementation.

   Note: Steps 1–3, 8, and 9 can be done by using the Unisphere software by selecting System ➤ Monitoring and Alerts ➤ Notifications ➤ Storage Usage. The actions are limited to email and trap.

2. Create a new notification configuration file named /nas/site/my_eventlog.cfg by copying /nas/sys/nas_eventlog.cfg to my_eventlog.cfg.

3. Use a text editor to add the following statements to my_eventlog.cfg:

```
# CFS High Water Mark Event Control
# notification for the file system size threshold exceeded
#
facilitypolicy 1:27,7
     disposition range=1-1, logfile "/nas/log/sys_log"
     disposition range=1-1, mail "storadmin01@nasdocs.emc.com"
     disposition range=1-1, mail "storadmin02@nasdocs.emc.com"
     disposition range=1-1, mail "storadmin03@nasdocs.emc.com"
     disposition range=1-1, trap "/nas/site/trap.cfg 12"
```

   where:

   `facilitypolicy 1:27` = dispositions that need to be applied to events in the CFS facility (facility ID 27) of the DART component (component ID 1).

   `7` = severity-level threshold (captures events of severity 7 or lower).

   disposition range=1-1 = events 1 through 1, which equates to the CFS event "Crossed the fs (file system) size threshold." Event ID 1 is the event ID of the fs threshold event.

   `logfile` = entry added to the /nas/log/sys_log file for events 1 through 1.

`storadmin01@nasdocs.emc.com, storadmin02@nasdocs.emc.com`, and `storadmin03@nasdocs.emc.com` = email addresses that receive email notification. Replace these with one or more email addresses at the company.

`12` = arbitrary, yet unique, trap number you associate with the event in the MIB (code shown in step 5).

Determine events associated with a facility on page 40 provides information about determining which events are associated with which facilities.

4. Set up the SNMP Manager by adding the following line to the file /nas/site/trap.cfg:

   snmpmanager *<target>* **;** **communityname** *<public>*

   where:

   <target> = IPv4 or IPv6 address, hostname, or fully qualified domain name of the SNMP Manager that gets the traps.

   <public> = community name to use for authentication with the SNMP Manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public.

5. Modify the MIB, found at /nas/sys/emccelerra.mib, to include the following lines:

```
celCFS TRAP-TYPE
ENTERPRISE emcCelerra
VARIABLES {celEvent}
DESCRIPTION
     "Trap message will be sent when a file system exceeds the threshold."
::=12
```

   where:

   `12` = arbitrary, yet unique, trap number for the event you specified in the my_eventlog.cfg file.

   Note: Save a copy of the modified MIB in another location because it is overwritten when the system is upgraded. On HP OpenView, load the MIB by using Options ➤ Load/Unload MIBs:SNMP.

6. Configure MIB on the SNMP Manager.

7. Ensure that the Control Station name is in the /etc/hosts file:

```
# Do not remove the following line, or various programs
# requiring network functionality will fail.
127.0.0.1           localhost.localdomain localhost
<address>           <example_cs0> <example_cs0.nasdocs.emc.com>
```

   where:

   <address> = IPv4 or IPv6 address of the Control Station. The IPv4 address is always present. The IPv6 address is present only if IPv6 is configured.

<example_cs0> = Control Station name and <nasdocs.emc.com> is the name of domain that includes the mail server. Substitute Control Station and domain information for the ones in the example.

Note: Underscores are used in the example text here for readability only. The underscore is an invalid character in the Control Station name and should not be used.

---

8. Using the full pathname, load the new notification configuration file by using the following command:

   $ nas_event -Load /nas/site/my_eventlog.cfg

   Output:

   ```
   EventLog : will load /nas/site/my_eventlog.cfg...done
   ```

Note: You must unload the configuration file before making additional changes. You must specify the absolute path of the configuration file to unload.

---

9. Verify that the new notifications (email and traps) have been accepted by using the following commands:

   $ nas_event -list -action mail

   or

   $ nas_event -list -action trap

Note: Mail is not a default action. Until an event is configured for mail notification, the command nas_event -list -action mail returns an error.

The output should at least display:

```
DART(1)
|--> CFS(27)
BaseID     Severity       Brief_Description
1          WARNING(4)     filesystem size threshold   (${usageHWM,2,%d}%)
 crossed
(fs ${mountPath,55,%s})
```

When the used space in a file system exceeds the threshold, an SNMP trap message and an email notification are sent to the file system administrator. The /usr/sbin/snmptrapd daemon must be started on the Control Station to display SNMP trap messages. Send a test SNMP trap on page 47 provides more information.

The trap message on the SNMP Manager looks like this:

Output
Feb 6 13:17:43 2008 CFS:4:1 Slot 3: 1191865801: filesystem size threshold (90%) crossed (fs /ufs1)

Note
The 1 in CFS:4:1 indicates the CFS event "Crossed the fs (file system) size threshold" and the Data Mover (Slot 3) and the mount point of the file system (/ufs1) involved are shown.

An example of an email notification follows:

Output

```
To: root@matisse-cs0.rtp.dg.com
Subject: EMCServer matisse-cs0, Component - DART, Facility - CFS, Severity
 - WARNING

Feb  6 13:17:43 2008 DART:CFS:WARNING:1 Slot 3: 1191865801: filesystem
size threshold (90%) crossed (fs /ufs1)
```

Note: There might be a delay in email sending due to activity on the Data Mover, network traffic, activity on the Control Station, or other factors onsite.

When a SnapSure SavVol usage reaches its high water mark

You can configure the system to generate an SNMP trap and an email notification to several file system administrators when a SnapSure SavVol usage reaches its high water mark (HWM).

By default, SnapSure audits SavVols automatically and writes a message to the system log when a user-set (0 percent to 100 percent) or default HWM of 90 percent full is reached. In addition to the log file, you can set up trap and email notification.

Configure the system to generate a notification when SnapSure SavVol usage reaches its high water mark

1. Configure the Domain Name Server (DNS) to enable email notification:

   $ **nas_cs -set -dns_domain** *<dns_domain_name>* **-search_domains** *<domain_name>[,...]* **-dns_servers** *<ip_address>[,...]*

   where:

   <dns_domain_name> = domain name of the primary Control Station

   <domain_name> = DNS domains searched

   <ip_address> = IPv4 or IPv6 addresses of the DNS servers

   Most of the time, DNS configuration is done at the time of system implementation.

2. Create a new notification configuration file named /nas/site/my_eventlog.cfg by copying /nas/sys/nas_eventlog.cfg to my_eventlog.cfg.

3. Use a text editor to add the following statements to my_eventlog.cfg:

```
# SVFS High Water Mark Event Control
# notification for the SavVol high water mark usage reached
#
facilitypolicy 1:70,7
     disposition range=1-1, logfile "/nas/log/sys_log"
     disposition range=1-1, mail "storadmin01@nasdocs.emc.com"
     disposition range=1-1, mail "storadmin02@nasdocs.emc.com"
     disposition range=1-1, mail "storadmin03@nasdocs.emc.com"
     disposition range=1-1, trap "/nas/site/trap.cfg 14"
```

where:

`facilitypolicy 1:70` = dispositions that need to be applied to events in the SVFS facility (facility ID 70) of the DART component (component ID 1).

`7` = severity-level threshold (captures events of severity 7 or lower).

`disposition range=1-1` = events 1 through 1, which equates to the SVFS event "high water mark of SavVol reached." Event ID 1 is the event ID of the High Water Mark event.

`logfile` = entry added to the /nas/log/sys_log file for events 1 through 1.

`storadmin01@nasdocs.emc.com, storadmin02@nasdocs.emc.com`, and `storadmin03@nasdocs.emc.com` = email addresses that receive email notification Replace these with one or more email addresses at company.

`14` = arbitrary, yet unique, trap number you associate with the event in the MIB (code shown in step 5).

Determine events associated with a facility on page 40 provides information about determining which events are associated with which facilities.

4. Set up the SNMP Manager by adding the following line to the file /nas/site/trap.cfg:

snmpmanager *<target>* **; communityname** *<public>*

where:

<target> = IPv4 or IPv6 address, host name, or fully qualified domain name of the SNMP Manager that gets the traps.

<public> = community name to use for authentication with the SNMP Manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public.

5. Modify the MIB, found at /nas/sys/emccelerra.mib, to include the following lines:

```
celSVFS TRAP-TYPE
ENTERPRISE emcCelerra
VARIABLES {celEvent}
DESCRIPTION
     "Trap message will be sent when a SavVol high water mark reached."
::=14
```

where:

14 = arbitrary, yet unique, trap number for the event you specified in the my_eventlog.cfg file

Note: Save a copy of the modified MIB in another location because it is overwritten when the system is upgraded. On HP OpenView, load the MIB by using Options ➤ Load/Unload MIBs:SNMP.

6. Configure MIB on the SNMP Manager.

7. Ensure that the Control Station name is in the /etc/hosts file:

```
# Do not remove the following line, or various programs
# requiring network functionality will fail.
127.0.0.1           localhost.localdomain localhost
<address>           <example_cs0> <example_cs0.nasdocs.emc.com>
```

where:

<address> = IPv4 or IPv6 address of the Control Station. The IPv4 address is always present. The IPv6 address is present only if IPv6 is configured.

<example_cs0> = Control Station name and *<nasdocs.emc.com>* is the name of domain that includes the mail server. Substitute Control Station and domain information for the ones in the example.

Note: Underscores are used in the example text here for readability only. The underscore is an invalid character in the Control Station name and should not be used.

8. Using the full pathname, load the new notification configuration file by using the following command:

```
$ nas_event -Load /nas/site/my_eventlog.cfg
```

Output:

```
EventLog : will load /nas/site/my_eventlog.cfg...done
```

Note: You must unload the configuration file before making additional changes. You must specify the absolute path of the configuration file to unload.

9. Verify that the new notifications (email and traps) have been accepted by using the following commands:

```
$ nas_event -list -action mail
```

or

```
$ nas_event -list -action trap
```

Note: Mail is not a default action. Until an event is configured for mail notification, the command nas_event -list -action mail returns an error.

Output:

For nas_event -list -action mail, the output should at least display:

```
DART(1)
|--> SVFS(70)
BaseID      Severity        Brief_Description
1           WARNING(4)      FSID:${id,5,%u} SavVol:${vol,8,%s}
MaxSize:${maxsize,5,%u}
MB %Full(hwm=${hwm,2,%d}) reached (t:${ticks,3,%q})
```

For nas_event -list -action trap, the output should at least display:

```
DART(1)
|--> SVFS(70)
BaseID      Severity        Brief_Description
1           WARNING(4)      FSID:${id,5,%u} SavVol:${vol,8,%s}
MaxSize:${maxsize,5,%u}
MB %Full(hwm=${hwm,2,%d}) reached (t:${ticks,3,%q})
```

When the HWM is reached for a SavVol, an SNMP trap message and email notification are sent to the file system administrator. The /usr/sbin/snmptrapd daemon must be started on the Control Station to display SNMP trap messages. Send a test SNMP trap on page 47 provides more information.

The trap message on the SNMP Manager looks like this:

Output

```
2008-02-06 13:26:28 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1)
TRAP,
SNMP v1, community public
     SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (14) Uptime:
 19:38:21.11
     SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 70
     SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 1
     SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 4
     SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING:
"Feb  6 13:26:28 2008 SVFS:4:1 Slot 2: 1191866214:
FSID:25 SavVol:121 MaxSize:1000 MB %Full(hwm=80) reached
(t:1191866214232323) "
```

Note

The 1 in SVFS:4:1 indicates the SVFS event “High water mark of SavVol reached," on Data Mover (Slot 2).

The following is an example of email notification:

Output

```
To: root@matisse-cs0.rtp.dg.com
Subject: EMCServer matisse-cs0, Component - DART, Facility - SVFS, Severity
 - WARNING

Feb  6 13:26:28 2008 DART:SVFS:WARNING:1 Slot 2: 1191866214: FSID:25
SavVol:121 MaxSize:1000 MB %Full(hwm=80) reached (t:1191866214232323)
```

Note: There might be a delay in email sending due to activity on the Data Mover, network traffic, activity on the Control Station, or other factors onsite.

When there are Virus Checker events

You can configure the system to generate SNMP traps and an email notification to Windows administrators when there are Virus Checker events. You need root access to the system.

Configure the system to generate a notification for Virus Checker events

1. Configure DNS to enable email notification:

   $ **nas_cs -set -dns_domain** *<dns_domain_name>* **-search_domains** *<domain_name>[,...]* **-dns_servers** *<ip_address>[,...]*

   where:

   <dns_domain_name> = domain name of the primary Control Station

   <domain_name> = DNS domains searched

   <ip_address> = IPv4 or IPv6 addresses of the DNS servers

   Most of the time, DNS configuration is done at the time of system implementation.

2. Create a new notification configuration file named /nas/site/my_eventlog.cfg by copying /nas/sys/nas_eventlog.cfg to my_eventlog.cfg.

3. Use a text editor to add the following statements to my_eventlog.cfg:

```
# Virus Checker Events
# email and trap notification for any Virus Checker event
#
facilitypolicy 1:81,7
     disposition range=1-28, mail "storadmin01@nasdocs.emc.com"
     disposition range=1-28, trap "/nas/site/trap.cfg 11"
```

   where:

   `facilitypolicy 1:81` = dispositions that need to be applied to events in the VC facility (facility ID 81) of the DART component (component ID 1).

   `7` = severity-level threshold (captures events of severity 7 or lower).

   `disposition range=1-28` = events 1 through 28, which equates to all VC events.

   `storadmin01@nasdocs.emc.com` = email address that receives email notification. Replace these with one or more email addresses at company.

   `11` = arbitrary, yet unique, trap number you associate with the event in the MIB (code shown in step 5).

Determine events associated with a facility on page 40 provides information about determining which events are associated with which facilities.

4. Set up the SNMP Manager by adding the following line to the file /nas/site/trap.cfg:

   snmpmanager *<target>* **; communityname** *<public>*

   where:

   <target> = IPv4 or IPv6 address, hostname, or fully qualified domain name of the SNMP Manager that gets the traps.

   <public> = community name to use for authentication with the SNMP Manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public.

5. Modify the MIB, found at /nas/sys/emccelerra.mib, to include the following lines:

```
celVC TRAP-TYPE
ENTERPRISE emcCelerra
VARIABLES {celEvent}
DESCRIPTION
      "Trap message will be sent in the event of a VC service associated
 notification
       request."
::= 11
```

   where:

   11 = arbitrary, yet unique, trap number for the event you specified in the my_eventlog.cfg file

   Note: Save a copy of the modified MIB in another location because it is overwritten when the system is upgraded. On HP OpenView, load the MIB by using Options ➤ Load/Unload MIBs:SNMP.

6. Configure MIB on the SNMP Manager.

7. Ensure that the Control Station name is in the /etc/hosts file:

```
# Do not remove the following line, or various programs
# requiring network functionality will fail.
127.0.0.1           localhost.localdomain localhost
<address>           <example_cs0> <example_cs0.nasdocs.emc.com>
```

   where:

   <address> = IPv4 or IPv6 address of the Control Station. The IPv4 address is always present. The IPv6 address is present only if IPv6 is configured.

   <example_cs0> = Control Station name and <nasdocs.emc.com> is the name of domain that includes the mail server. Substitute Control Station and domain information for the ones in the example.

Note: Underscores are used in the example text here for readability only. The underscore is an invalid character in the Control Station name and should not be used.

8. Using the full pathname, load the new notification configuration file by using the following command:

```
$ nas_event -Load /nas/site/my_eventlog.cfg
```

Output:

```
EventLog : will load /nas/site/my_eventlog.cfg...done
```

Note: You must unload the configuration file before making additional changes. You must specify the absolute path of the configuration file to unload.

9. Verify that the new notifications (email and traps) have been accepted by using the following commands:

```
$ nas_event -list -action mail
```

or

```
$ nas_event -list -action trap
```

Note: Mail is not a default action. Until an event is configured for mail notification, the command nas_event -list -action mail returns an error.

The output should at least display:

```
DART(1)
|--> VC(81)
BaseID     Severity       Brief_Description
1          NOTICE(5)      The virus checker is running normally.
2          ERROR(3)       ${type,8,%s} high water mark reached.
3          WARNING(4)     ${type,8,%s} low water mark reached.
4          ERROR(3)       No virus checker server is available.
5          ERROR(3)       No virus checker server is available. CIFS is
 stopped.
6          ERROR(3)       No virus checker server is available. Virus
checking is
                          stopped.
7          ERROR(3)       '${filename,8,%s}' was not checked.
8          NOTICE(5)      Server ${ipaddr,8,%s} is online. RPC program
version
                          ${rpc,2,%d}, ${cava,8,%s}.
9         ERROR(3)       Error on server ${ipaddr,8,%s}: ${status,8,%s}$

                          {winerror,8,%s}, RPC program version
${rpc,2,%d},
                          ${cava,8,%s}.
10         NOTICE(5)      The virus checker is started.
11         NOTICE(5)      Scanning was completed for file system
${fsid,2,%d}
                          mounted on ${mountPath,8,%s}. ${dirs,2,%d}
directories
                          were scanned and ${files,2,%d} files were
submitted to
                          the scan engine.
12         ERROR(3)       Scanning was aborted for file system
${fsid,2,%d} mounted
                          on ${mountPath,8,%s} for this reason:
${error,8,%s}.
                          ${dirs,2,%d} directories were scanned and
${files,2,%d}
                          files were submitted to the scan engine.
13        ERROR(3)       The antivirus (AV) engine deleted ${file,8,%s},
 ${user,8,%s}.
14        ERROR(3)       The antivirus (AV) engine renamed ${file,8,%s},
 ${user,8,%s}.
15       WARNING(4)     The antivirus (AV) engine modified ${file,8,%s},
 ${user,8,%s}.
16         NOTICE(5)      The virus checker is stopped.
```

When the Virus Checker is stopped and started, the Control Station generates SNMP trap messages and email. The /usr/sbin/snmptrapd daemon must be started on the Control Station to display SNMP trap messages. Send a test SNMP trap on page 47 provides more information.

Here are some examples of Virus Checker trap messages:

Output

```
2008-02-06 13:32:42 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1)
TRAP,
SNMP v1, community public
    SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (11) Uptime:
19:44:34.83
    SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 81
    SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 4
    SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 3
    SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING: "Feb  6 13:32:42 2008
VC:3:4
No virus checker server is available.  "
2008-02-06 13:32:50 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1)
TRAP, SNMP v1,
community public
    SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (11) Uptime:
19:44:42.91
    SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 81
    SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 16
    SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 5
    SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING: "Feb  6 13:32:50 2008
VC:5:16
The virus checker is stopped. "
```

When Virus Checker is started, some of the following trap messages are generated:

Output

```
SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (11) Uptime:
19:52:45.25
    SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 81
    SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 10
    SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 5
    SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING: "Feb  6 13:40:52
2008 VC:5:10 Slot 2: 1089402969: The virus checker is started. "
2008-02-06 13:41:20 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1)
TRAP, SNMP v1,
community public
    SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (11) Uptime:
19:53:12.58
    SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 81
    SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 10
    SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 5
    SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING: "Feb  6 13:41:20 2008
VC:5:10 Slot 3:
1089454545: The virus checker is started. "
```

Here is an example of a mail notification when Virus Checker is started:

Output

```
To: root@matisse-cs0.rtp.dg.com
Subject: EMCServer matisse-cs0, Component - DART, Facility - VC, Severity
 - NOTICE

Feb  6 13:41:20 2008 DART:VC:NOTICE:10 Slot 3: 1089454545: The virus
checker is started.
```

Here is an example of a mail notification when Virus Checker is stopped:

Output

```
To: root@matisse-cs0.rtp.dg.com
Subject: EMCServer matisse-cs0, Component - DART, Facility - VC, Severity
 - NOTICE

Feb  6 13:32:50 2008 DART:VC:NOTICE:16 The virus checker is stopped.
```

When a hard or soft quota is exceeded

You can configure the system to generate SNMP traps and an email notification to several storage administrators whenever a hard or soft quota for users, groups, or trees is exceeded.

Configure the system to generate a notification when a quota is exceeded

1. Configure DNS to enable email notification:

   $ **nas_cs -set -dns_domain** *<dns_domain_name>* **-search_domains** *<domain_name>[,...]* **-dns_servers** *<ip_address>[,...]*

   where:

   <dns_domain_name> = domain name of the primary Control Station

   <domain_name> = DNS domains searched

   <ip_address> = IPv4 or IPv6 addresses of the DNS servers

   Most of the time, DNS configuration is done at the time of system implementation.

2. Create a new notification configuration file named /nas/site/my_eventlog.cfg by copying /nas/sys/nas_eventlog.cfg to my_eventlog.cfg.

3. Use a text editor to add the following statements to my_eventlog.cfg:

   ```
   # email and trap notification for soft and hard quota exceeded
   #
   facilitypolicy  1:64, 7
        disposition range=4-5, mail "storadmin01@nasdocs.emc.com"
        disposition range=4-5, trap "/nas/site/trap.cfg 20"
   ```

where:

`facilitypolicy 1:64` = dispositions that need to be applied to events in the UFS facility (facility ID 64) of the DART component (component ID 1).

`7` = severity-level threshold (captures events of severity 7 or lower).

`storadmin01@nasdocs.emc.com` = email addresses that receive email notification. Replace these with one or more email addresses at company.

`disposition range=4-5` = events 4 through 5, which equates to the UFS events "Block soft quota crossed" and "Hard limit reached or exceeded."

Determine events associated with a facility on page 40 provides information about determining which events are associated with which facilities.

4. Set up the SNMP Manager by adding the following line to the file: /nas/site/trap.cfg:

   snmpmanager *<target>* **; communityname** *<public>*

   where:

   <target> = IPv4 or IPv6 address, hostname, or fully qualified domain name of the SNMP Manager that gets the traps.

   <public> = community name to use for authentication with the SNMP Manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public.

5. Modify the MIB, found at /nas/sys/emccelerra.mib, to include the following lines:

```
celUFS TRAP-TYPE
ENTERPRISE emcCelerra
VARIABLES {celEvent}
DESCRIPTION
     "Trap message will be sent in the event of a UFS quota exceeded."
::=20
```

   where:

   `20` = arbitrary, yet unique, trap number for the event you specified in the my_eventlog.cfg file.

   Note: Save a copy of the modified MIB in another location because it is overwritten when the system is upgraded. On HP OpenView, load the MIB by using Options ➤ Load/Unload MIBs:SNMP.

   ---

6. Configure MIB on the SNMP Manager.

7. Ensure that the Control Station name is in the /etc/hosts file:

```
# Do not remove the following line, or various programs
# requiring network functionality will fail.
127.0.0.1           localhost.localdomain localhost
<address>           <example_cs0> <example_cs0.nasdocs.emc.com>
```

   where:

<address> = IPv4 or IPv6 address of the Control Station. The IPv4 address is always present. The IPv6 address is present only if IPv6 is configured.

<example_cs0> = Control Station name and <nasdocs.emc.com> is the name of domain that includes the mail server. Substitute Control Station and domain information for the ones in the example.

Note: Underscores are used in the example text here for readability only. The underscore is an invalid character in the Control Station name and should not be used.

---

8. Using the full pathname, load the new notification configuration file by using the following command:

   $ nas_event -Load /nas/site/my_eventlog.cfg

   Output:

   ```
   EventLog : will load /nas/site/my_eventlog.cfg...done
   ```

   Note: You must unload the configuration file before making additional changes. You must specify the absolute path of the configuration file to unload.

   ---

9. Verify that the new notifications (email and traps) have been accepted by using the following command:

   $ nas_event -list -action mail

   or

   $ nas_event -list -action trap

   Note: Mail is not a default action. Until an event is configured for mail notification, the command nas_event -list -action mail returns an error.

   The output should at least display:

   ```
   DART(1)
   |--> UFS(64)
   BaseID     Severity       Brief_Description
   4          WARNING(4)     Block soft quota crossed (fs
   ${mountPoint,55,%s},
                             ${idStr,8,%s} ${quotaId,25,%u})
   5          ERROR(3)       Block hard quota reached/exceeded (fs
   ${mountPoint,55,%s},
                             ${idStr,8,%s} ${userId,25,%u})
   ```

10. Edit the quota event notification settings for the file systems on a Data Mover with the following command:

    $ nas_quotas -config -edit -mover server_2

11. You will see the following lines defining quota event notification settings for the file systems on the specified Data Mover:

    ```
    soft quota crossed: (no)
    hard quota crossed: (no)
    ```

By default, the fields are set to (no), which disables event notification when the event occurs. To enable event reporting for the desired file systems, change their settings to (yes). Repeat this change of quota event notification settings for each Data Mover.

When a hard or soft quota for users, groups, or trees is exceeded, the Control Station generates SNMP trap messages and email. The /usr/sbin/snmptrapd daemon must start on the Control Station to display SNMP trap messages. Send a test SNMP trap on page 47 provides more information.

When a hard or soft quota is exceeded, the following trap messages are generated:

Output

```
2008-02-06 13:46:59 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1)
TRAP,
SNMP v1, community public
      SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (20) Uptime:
 19:58:51.70
       SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 64
       SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 4
       SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 4
       SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING: "Feb  6 13:46:59
2008
UFS:4:4 Slot 2: 1191867432: Block soft quota crossed (fs /root_vdm_1/ufs12,
 uid 32784). "
2008-02-06 13:48:40 matisse-cs0.rtp.dg.com [10.6.4.76] (via 127.0.0.1)
TRAP, SNMP v1, community public
      SNMPv2-SMI::enterprises.1139.2 Enterprise Specific Trap (20) Uptime:
 20:00:32.66
       SNMPv2-SMI::enterprises.1139.2.1.1.1 = INTEGER: 64
       SNMPv2-SMI::enterprises.1139.2.1.1.2 = INTEGER: 5
       SNMPv2-SMI::enterprises.1139.2.1.1.3 = INTEGER: 3
       SNMPv2-SMI::enterprises.1139.2.1.1.4 = STRING: "Feb  6 13:48:40
2008
UFS:3:5 Slot 2: 1191867444: Block hard quota reached/exceeded (fs
/root_vdm_1/ufs12,
uid 32784). "
```

When the file system hard or soft quota is exceeded, notifications similar to the following messages are sent:

Output

```
To: root@matisse-cs0.rtp.dg.com
Subject: EMCServer matisse-cs0, Component - DART, Facility - UFS, Severity
 - WARNING

Feb  6 13:46:59 2008 DART:UFS:WARNING:4 Slot 2: 1191867432: Block soft
quota crossed
(fs /ufs2 , uid 32784).

To: root@matisse-cs0.rtp.dg.com
Subject: EMCServer matisse-cs0, Component - DART, Facility - UFS, Severity
 - ERROR

Feb  6 13:48:40 2008 DART:UFS:ERROR:5 Slot 2: 1191867444: Block hard quota
 reached/exceeded
 (fs /ufs2, uid 32784).
```

Note

The 5 in DART:UFS:ERROR:5 indicates the UFS event "Block hard quota reached/exceeded" and 4 in DART:UFS:WARNING:4 indicates the UFS event "Block soft quota crossed." The Data Mover (Slot 2) and the mount point of the file system (/ufs2) involved are shown. The u in uid indicates a user quota alert, treeid indicates a tree quota alert, and the g in gid indicates a group quota alert.

When Data Mover crosses a certain threshold for CPU utilization, memory utilization, or average response time for NFS operations

You can receive automated SNMP trap or email notifications when a Data Mover crosses a certain threshold for a set period of minutes and persistence for CPU utilization, memory utilization, or average response time for NFS operations. You can also be notified when the condition is no longer applicable and subsides to a normal level.

The alerter daemon (nas_ alerterd) reads a policy configuration file and connects to active Data Movers. For each active Data Mover, for which you have configured a policy for CPU utilization, the CPU utilization is sampled once every minute. Similarly, for each active Data Mover, for which you have configured policies for memory utilization and average response time for NFS operations, memory utilization and average response time for NFS operations are sampled once every minute. When all samples meet the applicable policy for the persistence period and the threshold condition, an alert is generated. As long as the subsequent samples continue to meet the policy, no further notifications are sent. When a sample fails to meet the policy threshold condition, the alert will be cleared and another trap or email notification will be generated.

The alerter daemon generates a number of events, including when:

- A CPU sample value meets the persistence and threshold condition of a policy.
- A CPU sample drops below the threshold for a policy.
- A memory sample value meets the persistence and threshold condition of a policy.
- A memory sample drops below the threshold for a policy.

- An average response time for NFS operations sample value meets the persistence and threshold condition of a policy.
- An average response time for NFS operations sample drops below the threshold for a policy.
- The connection to the Data Mover was lost.
- The connection to the Data Mover was re-established.

The alerter daemon starts as part of the NAS service on the Control Station and shuts down when the NAS service shuts down.

Configure the system to generate a notification when a policy for CPU utilization, kernel memory utilization, or average response time for NFS operations crosses a certain threshold

Note: Your VNX is delivered with some policies already configured. These policies could be sufficient for your environment and, therefore, you may not need to configure additional policies.

1. Configure the Domain Name Server (DNS) to enable email notification:

   $ **nas_cs -set -dns_domain** *<dns_domain_name>* **-search_domains** *<domain_name>[,...]* **-dns_servers** *<ip_address>[,...]*

   where:

   <dns_domain_name> = domain name of the primary Control Station

   <domain_name> = DNS domains searched

   <ip_address> = IPv4 or IPv6 addresses of the DNS servers

   Often, DNS configuration is done at the time of system implementation.

2. Edit the policy file.

   You can configure a CPU utilization notification policy, a memory utilization notification policy, or an average response time for NFS operations policy by editing the policy file, /nas/site/nas_alerterd.conf. The policy file uses comma-separated fields in the [POLICY] section in the following format:

   $ *<policy_name>*,*<data_mover_name>*, *<statpath_name>*,*<operator>*, *<threshold>*, *<persistence>*

   where:

   <policy_name> = unique name within the policy file to identify the policy by name. The policy name is case-sensitive and should be limited to alphanumeric characters (with no white space).

<data_mover_name> = Data Mover name or ALL indicates all Data Movers for which CPU utilization, memory utilization statistics, or the average response time per file system per client per NFS operation will be monitored.

<statpath_name> = the pathname for CPU utilization statistics, memory utilization statistics, or average response time per file system per client per NFS operation. The different elements in the pathname are separated by a period.

<operator> = comparison operator and must be one of the following:

- eq = equal to
- gt = greater than (default)
- ge = greater than or equal to
- lt = less than
- le = less than or equal to

<threshold> = percentage of CPU utilization or memory utilization, or for NFS operations, the average response time in microseconds per call.

<persistence> = number of minutes or quantity of times that the condition needs to be true to generate an alert.

output_format = (optional) either csv or text.

<sampling_interval> = (optional) elapsed time between samples.

<sampling_duration> = (optional) length of time over which to take samples.

<statpath_names_to_collect> = (optional) comma-separated list of sampled statpath names to collect as a result of a raised event.

You can also configure two additional items located in the [COMMON] section of the policy file:

<stats_collection_dir> = a fully qualified directory path for the location of files containing the result of server_stats sessions. If the stat_collection_dir option is not set, the server_stats session will not run for any policy requiring server_stats disposition.

allow_concurrent_collection = this option determines if multiple instances of server_stats sessions may be concurrently running for the same policy/DataMover combination.

For example, the following policy for server_2 uses a ge operator, a 90 threshold, and a 15-minute persistence. This means that to generate an alert, the CPU utilization value needs to be greater than or equal to 90 percent for at least 15 consecutive minutes. If an alert was generated and subsequently the CPU utilization sample drops to less than or equal to 90 percent, the alert is cleared:

```
CPU_Server2,server_2,kernel.cpu.utilization.cpuUtil,ge,90,15
```

Additional policy file examples are as follows.

In the following policy an alert is generated, if server_2 or server_3 or both have CPU utilizations of at least 80 percent for 5 minutes. The alert will clear when the CPU utilization drops below 80 percent:

```
CPU_Server2,server_2,kernel.cpu.utilization.cpuUtil,gt,80,5
CPU_Server3,server_3,kernel.cpu.utilization.cpuUtil,gt,80,5
```

The following policy illustrates that you can configure multiple policies for a single Data Mover. An alert is generated for any Data Mover with a CPU utilization of at least 85 percent for 15 minutes, and an alert is generated for server_2 if it reaches a CPU utilization of at least 80 percent for 5 minutes. An alert is also generated for server_2 if it reaches a memory utilization of at least 80 percent for 5 minutes. The alerts will clear when the CPU utilization drops below the threshold:

```
CPU_ALL,ALL,kernel.cpu.utilization.cpuUtil,ge,85,15
CPU_Server2,server_2,kernel.cpu.utilization.cpuUtil,gt,80,5
Memory_Server2,server_2,kernel.memory.util,gt,80,5
```

In the following policy an alert is generated for any DataMover with an average response time for NFS operations of at least 5000 microseconds per call for 1 minute. The output format will be in csv and the interval and duration of the sampling will be 15 seconds and 120 minutes, respectively. The sampled statpaths names to collect as a result of a raised event will be nfs.client, nfs.user, nfs.group, nfs.export. The alert will clear when the average response time drops below 5000 microseconds per call.

```
nfs_avgtime,ALL,nfs.filesystem.*.client.*.op.*.avgTime,ge,5000,1,csv,15,120,nfs.client,nfs.user,nfs.group,nfs.export
```

3. Restart the nas_alerterd process.

   After editing the CPU utilization policies or any of the other policies, you must restart the alerter daemon by using the following command, which requires root privilege:

   ```
   killall -s SIGINT nas_alerterd
   ```

   The daemon will restart automatically after being stopped.

4. Edit the notification configuration file.

   Configure trap and email notifications by editing the /nas/sys/nas_eventlog.cfg file with a text editor to update the email address or delete the email address if you do not want it:

   ```
   facilitypolicy  6:154, 7
            disposition, logfile "/nas/log/sys_log"
            disposition range=1-4, mail <user-email>
            disposition range=1-4, trap "/nas/site/trap.cfg 2"
   ```

   where:

   `facilitypolicy 6:154` = dispositions that need to be applied to events in the PERFSTATS facility (facility ID 144) of the DART component (component ID 6)

   `7` = severity-level threshold (captures events of severity 7 or lower)

   `logfile` = entry added to the /nas/log/sys_log file for events

   `disposition range=1-4` = events 1 through 4

   `<user-email>` = email address that receives email notifications

   `2` = the unique ID number for the trap defined in the MIB.

5. Set up the SNMP Manager by adding the following line to the file /nas/site/trap.cfg:

   snmpmanager *<target>* **; communityname** *<public>*

   where:

   <target> = IPv4 or IPv6 address, hostname, or fully qualified domain name of the SNMP Manager that gets the traps.

   <public> = community name to use for authentication with the SNMP Manager. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public.

6. Ensure that the Control Station name is in the /etc/hosts file:

   ```
   # Do not remove the following line, or various programs
   # requiring network functionality will fail.
   127.0.0.1           localhost.localdomain localhost
   <address>           <example_cs0> <example_cs0.nasdocs.emc.com>
   ```

   where:

   <address> = IPv4 or IPv6 address of the Control Station. The IPv4 address is always present. The IPv6 address is present only if IPv6 is configured.

   <example_cs0> = Control Station name and *<nasdocs.emc.com>* is the name of the domain that includes the mail server. Substitute Control Station and domain information for the ones in the example.

   Note: Underscores are used in the example text here for readability only. The underscore is an invalid character in the Control Station name and should not be used.

   ---

7. Load the notification configuration file.

   Use the full pathname to load the new notification configuration file by using the following command:

   ```
   $ nas_event -Load /nas/sys/nas_eventlog.cfg
   ```

8. Specify host to receive SNMP trap.

   To use SNMP traps, edit /nas/site/trap.cfg to specify the host that will receive the trap.

9. Verify that the new notifications (email and traps) have been accepted by using the following commands:

   ```
   $ nas_event -list -action mail
   ```

   or

   ```
   $ nas_event -list -action trap
   ```

4 Managing

The tasks to manage SNMP ports are:

- Change the SNMP port where SNMP traps are sent on page 80

Change the SNMP port where SNMP traps are sent

To integrate VNX for file's SNMP trap notifications mechanism with the EMC ControlCenter® NAS agent or another monitoring application already using the standard SNMP port 162, you can configure the SNMP port to which to send the trap.

Action
By using a text editor, add the following line to the file /nas/site/trap.cfg: **snmpmanager** *<IPv4Addr>[:<port>] | <\[IPv6Addr\]:port>* **; communityname** *<public>* where: *<IPv4Addr>[:<port>] | <\[IPv6Addr\]:port>* = IP address of the host application where IPv4Addr and IPv6Addr are IP addresses and <port> is the port number where the application listens for SNMP traps. IPv6 addresses should be enclosed in square brackets if a port is specified; the brackets do not signify optional content. *<public>* = community name to use for authentication with the SNMP Manger. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. Check with the site manager for what to use in place of public. Examples: **snmpmanager 172.24.108.20:163 ; communityname public** **snmpmanager [2620:0:f17a:5679:216:17ff:fe77:c796]:163 ; communityname public**

5 Troubleshooting

As part of an effort to continuously improve and enhance the performance and capabilities of its product lines, EMC periodically releases new versions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, contact your EMC Customer Support Representative.

Problem Resolution Roadmap for VNX contains additional information about using EMC Online Support and resolving problems.

Topics included in this chapter are:

EMC E-Lab Interoperability Navigator

The EMC E-Lab™ Interoperability Navigator is a searchable, web-based application that provides access to EMC interoperability support matrices. It is available on EMC Online Support at http://Support.EMC.com. After logging in, in the right pane under **Product and Support Tools**, click **E-Lab Navigator**.

Email notifications not received

If the Control Station is not able to send a notification that specifies an email address as its destination, the Control Station places the message in its root user mailbox. Retrieve the message and check its header to verify the destination address. You can use the mail log files in the /var/log directory to troubleshoot sendmail problems.

Note: The online Support Solutions Knowledgebase provides more information about troubleshooting problems with the sendmail feature on the Control Station. Use the text from the error message's brief description or the message's ID to search the Knowledgebase on the EMC Online Support website. After logging in to EMC Online Support, locate the applicable Support by Product page, and search for the error message.

Check for mail messages addressed to root as follows:

1. Log in to the Control Station as root. If you logged in with your administrative username and password, you can change to root by typing:

   ```
   $ su -
   ```

2. At the command prompt, type:

   ```
   # mail
   ```

   This displays a list of messages addressed to root.

3. To see the list of commands for the mail program, at the mail prompt, type:

   ```
   # help
   ```

Check if sendmail is running

Use this command to check if sendmail is running, as root (su -), type:

Action
ps -ef | grep sendmail
Output
If sendmail is running, you will see output similar to the following: `root 29698 1 0 Jan07 ? 00:00:00 sendmail: accepting connections` If sendmail is not accepting connections, you must configure it.

Configure sendmail

To configure sendmail on the Control Station:

1. Log in to the Control Station as root. If you logged in with your administrative username and password, you can change to root by typing:

   $ su -

2. To configure sendmail, type:

   # /sbin/chkconfig --add sendmail

   # /sbin/service sendmail start

Notifications missing or not working

If you believe an event has occurred and the notification you expected did not happen, first check the notification configuration files to see what other actions are defined for the event. For example, most events have a log file action defined. If so, you can check the appropriate log file to see if that action occurred, or if just a single action failed. You need to configure notifications in order to receive notifications once the events are posted.

Use a command similar to the following to view the quota event notification settings for file systems on a Data Mover:

`nas_quotas -config -edit -mover server_2`

You will see these lines defining quota event notification settings for the file systems on the specified Data Mover:

soft quota crossed: (no)

hard quota crossed: (no)

By default, the fields are set to (no), which disables event notification when the event occurs. To enable event reporting for the desired file systems, change their settings to (yes). Repeat this change of quota event notification settings for each Data Mover on which the file systems are mounted.

Probable causes for not receiving email notifications include:

- Email exchange rejecting email
- Email exchange not being located

To troubleshoot:

- Check root's email inbox on the Control Station.
- Look for returned messages and look at the returned message to identify why it was returned.

Possible solutions:

- Ensure that the Control Station's hostname is in DNS and is resolvable from your email exchange.
- Ensure that your email exchange's IP address can be resolved by DNS from the Control Station.
- Ensure that the email exchange is responding.

Other solutions might be warranted as determined by the cause of the rejected email. If you do not see rejected emails, check the email notification configuration and look for email routing or delivery problems within your email system.

SNMP security issues

If SNMP does not respond and you implemented SNMP security, follow these steps to troubleshoot the issue:

- Check the community name. Community names are case-sensitive. It is a general practice to use uppercase letters to begin community names. Use alphanumeric characters and the special characters ~ ! @ # $ % ^ * + = { } : ? _ to specify the community name. If you remove all community names, including the default name (public), SNMP does not respond to any community names presented.
- Ensure that the host is set to accept SNMP packets from specific hosts.

Verify generation of an SNMP trap as a result of an event

If you believe an SNMP trap was not issued or was issued incorrectly, first check that the trap.cfg file is correct. Configure SNMP traps on page 46 provides more information on trap.cfg.

Use SNMP manager to determine if an SNMP trap is being issued correctly.

SNMP traps not working after Control Station restart or power outage

If the snmptrapd and snmpd daemons are not running, the SNMP trap messages you set up are not sent. After a Control Station restart or a power outage, the snmpd daemon might or might not start on a restart depending on being set up by /sbin/chkconfig to start. The snmptrapd daemon is not set up under the /sbin/chkconfig function, so it does not start after a restart unless you write a run control script to start it or start it manually.

If you enable or disable SNMP through the **System ➤ Network ➤ Network Services** tab, the daemon state survives a Control Station restart. It automatically sets up chkconfig.

Note: For VNX series Control Stations, snmptrapd is already running.

To manually start the snmptrapd daemon, log in to the Control Station as root and type:

```
/usr/sbin/snmptrapd -f -Le -Lf /nas/var/log/my_eventlog_messages &
```

The command starts the snmptrapd daemon as a background process. Some systems do not have the /nbsnas directory. If this is true for your system, use the /nas/var/log directory.

The snmptrapd and snmpd daemons manage SNMP trap messages, which are logged to the my_eventlog_messages file.

Error messages

All event, alert, and status messages provide detailed information and recommended actions to help you troubleshoot the situation.

To view message details, use any of these methods:

- Unisphere software:
  - Right-click an event, alert, or status message and select to view Event Details, Alert Details, or Status Details.
- CLI:
  - Type nas_message -info <MessageID>, where <MessageID> is the message identification number.
- *Celerra Error Messages Guide*:
  - Use this guide to locate information about messages that are in the earlier-release message format.
- EMC Online Support:

- Use the text from the error message's brief description or the message's ID to search the Knowledgebase on EMC Online Support. After logging in to EMC Online Support, locate the applicable **Support by Product** page, and search for the error message.

EMC Training and Professional Services

EMC Customer Education courses help you learn how EMC storage products work together within your environment to maximize your entire infrastructure investment. EMC Customer Education features online and hands-on training in state-of-the-art labs conveniently located throughout the world. EMC customer training courses are developed and delivered by EMC experts. Go to EMC Online Support at http://Support.EMC.com for course and registration information.

EMC Professional Services can help you implement your system efficiently. Consultants evaluate your business, IT processes, and technology, and recommend ways that you can leverage your information for the most benefit. From business plan to implementation, you get the experience and expertise that you need without straining your IT staff or hiring and training new personnel. Contact your EMC Customer Support Representative for more information.

Appendix A

Event Notification Actions

Event notification actions include:

- Event notification actions on page 90

Event notification actions

Table 6 on page 90 summarizes notifications (actions) you can take when an event occurs.

Table 6. Event notification actions

Action	Arguments	Description
logfile	*<logfile_pathname>*	Puts an entry in the log file specified by <logfile_pathname>.
mail	*<address>* | *user*	<address> – Sends email to the specified email address. Use a separate mail line for each additional email address. user – Sends email using the settings specified by the /nas/bin/nas_emailuser CLI or System and from the task list, under Service Tasks, select Manage Email User.
trap	*<config_file> <trap_number>*	Sends SNMP trap number <trap_number> to the SNMP manager as defined in the <config_file> configuration file. SNMP traps are sent on UDP port 162.
callhome	*binary* | *immediate*	Generates a CallHome action to EMC. binary – Sends home a binary file (for EMC use only) immediate – Calls home immediately materials – additional information added to a call home message with the location of log files when the Control Station uses FTP to send the log files to the FTP server CallHome is configured when the system is installed. This action is for the use of EMC and its authorized service providers only.
exec	*<procedure_name> <args>*	Executes the procedure specified by <procedure_name> with the arguments specified by <args>.

Table 6. Event notification actions *(continued)*

Action	Arguments	Description
udprpc	*<proc_num>,<prog_num>, <version>@<host>*	Sends an RPC message (by using UDP) to a host, where <proc_num> is the RPC procedure number, <prog_num> is the program number, <version> is the version number, and <host> is the hostname. The <proc_num> and <prog_num> arguments are required. If <version> is not supplied, version 1 is the default. If <host> is not supplied, <localhost> is the default.
terminate		Immediately terminates processing of the event, providing a way to override already defined actions so that troubleshooting can be performed.

Glossary

A

alert
In Unisphere™ software, a system event that requires administrative attention. These events may be severe enough to cause a system error or disrupt user access.

E

event
System-generated message caused by a command, an error, or other condition that may require action by an administrator. Events are typically written to an event log, and may trigger an event notification.

event log
File of system-generated messages based on meeting a condition of a particular severity level. There are separate event logs for the Control Station and for each physical and virtual Data Mover in the system.

event notification
Process by which specified events meeting a severity threshold trigger an action or notification.

See also *notifications*.

F

facility
Component of VNX for file that monitors the system and generates an event when a certain condition is detected.

M

Management Information Base (MIB)
Hierarchical database maintained by an agent that a network management station can query by using a network management protocol such as the SNMP.

N

network management station (NMS)
Systems that execute management applications, such as SNMP commands to monitor and control network elements.

notifications
Actions the Control Station takes in response to particular events. Some possible actions include sending an email message or an SNMP trap. There are two types of notifications: event notifications, which are notifications based on predefined system events such as a temperature being too high, and resource notifications, which are notifications based on user-specified resource usage limits or thresholds.

S

Simple Network Management Protocol (SNMP)
Method used to communicate management information between the network management stations and the agents in the network elements.

SNMP agent
Software module in a managed device, such as VNX for file or Symmetrix system, that maintains local management information and delivers that information to a manager by using SNMP.

SNMP community
Name for the SNMP transaction with a remote system. This is used as a password to control access to the SNMP MIB.

SNMP trap
Asynchronous message sent from an SNMP agent to an SNMP management program. Traps are typically used to report errors. VNX for file can be configured to send SNMP traps when specified events occur.

See also *event notification*.

Index

T