



EMC® VNX™ Series
Release 7.1

Using SNMPv3 on VNX™
P/N 300-013-824 Rev 01

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

Copyright © 2010 -2012 EMC Corporation. All rights reserved.

Published July 2012

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

Preface	5
Chapter 1: Introduction	7
System requirements.....	8
Cautions.....	8
User interface choices.....	8
Related information.....	8
Chapter 2: Concepts	11
SNMP.....	12
SNMPv3 benefits.....	12
Managed device.....	12
Agent.....	12
NMS.....	13
MIB.....	13
Messages.....	13
Trap.....	13
Chapter 3: Configuring	15
Enable SNMPD.....	16
Configure SNMPv1 and SNMPv2c support.....	16
Add a new SNMPv3 user.....	17
Chapter 4: Managing	19
View SNMPv3 properties.....	20
Modify SNMPv3 properties.....	20
Modify the passwords of an SNMPv3 user.....	21

Display SNMPv3 users on a Data Mover.....	22
Delete an SNMPv3 user.....	22
Verify SNMP status.....	23
Disable SNMPv1 and SNMPv2c.....	23
Disable SNMPD.....	24
Chapter 5: Troubleshooting.....	25
EMC E-Lab Interoperability Navigator.....	26
VNX user customized documentation.....	26
Error messages.....	26
EMC Training and Professional Services.....	27
Appendix A: Displaying Network Statistics.....	29
Display legacy IPv4 network statistics.....	30
Display IPv6 network statistics.....	31
Glossary.....	33
Index.....	35

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.

 Identifies content that warns of potential business or data loss.

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

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

 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 the EMC Online Support website (registration required) at <http://Support.EMC.com>.

Troubleshooting — Go to the [EMC Online Support](#) website. After logging in, locate the applicable Support by Product page.

Technical support — For technical support and service requests, go to EMC Customer Service on the [EMC Online Support](#) website. 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

This document provides information about how to configure and manage Simple Network Management Protocol version 3 (SNMPv3) on an EMC VNX.

This document is part of the VNX documentation set and is intended for network administrators responsible for configuring and maintaining a file storage and network retrieval infrastructure.

Topics included are:

- ◆ [System requirements on page 8](#)
- ◆ [Cautions on page 8](#)
- ◆ [User interface choices on page 8](#)
- ◆ [Related information on page 8](#)

System requirements

Table 1 on page 8 describes the EMC® VNX™ software, hardware, network, and storage configurations.

Table 1. System requirements

Software	VNX version 7.0.
Hardware	No specific hardware requirements.
Network	No specific network requirements.
Storage	No specific storage requirements.

Cautions

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

User interface choices

This document describes how to configure SNMPv3 by using the command line interface (CLI). You cannot use other VNX management applications to configure SNMPv3.

Related information

Specific information related to the features and functionality described in this document are included in:

- ◆ *Configuring and Managing Networking on VNX*
- ◆ *EMC VNX Command Line Interface Reference for File*
- ◆ VNX for File man pages
- ◆ *Parameters Guide for VNX for File*

For general information on the supported Management Information Bases (MIB), refer to:

- ◆ RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
- ◆ RFC 3412, *Message Processing and Dispatching for SNMP*
- ◆ RFC 3413, *SNMP Applications*

- ◆ RFC 3414, *User-based Security Model (USM) for SNMPv3*
- ◆ RFC 3415, *View-based Access Control Model (VACM) for SNMP*
- ◆ RFC 3416, *Version 2 of the Protocol Operations for SNMP*
- ◆ RFC 3417, *Transport Mappings for SNMP*
- ◆ RFC 3418, *MIB for SNMP*
- ◆ RFC 3430, *SNMP Over Transmission Control Protocol (TCP) Transport Mapping*
- ◆ RFC 1213, *MIB for Network Management of TCP/IP-based internets:MIB-II*
- ◆ RFC 2465, *MIB for IP Version 6 (IPv6): Textual Conventions and General Group*
- ◆ RFC 2466, *MIB for IPv6: ICMPv6 Group*
- ◆ RFC 4113, *MIB for User Datagram Protocol (UDP)*
- ◆ RFC 4022, *MIB for TCP*

EMC VNX documentation on the EMC Online Support website

The complete set of EMC VNX series customer publications is available on the EMC Online Support website. To search for technical documentation, go to <http://Support.EMC.com>. After logging in to the website, click the VNX Support by Product page to locate information for the specific feature required.

A network managed by Simple Network Management Protocol (SNMP) consists of three main components:

- ◆ Managed devices
- ◆ Agents
- ◆ Network management systems (NMS)

You can run management applications such as EMC Ionix ControlCenter or HP OpenView to monitor the health of the VNX.

Topics included are:

- ◆ [SNMP on page 12](#)
- ◆ [Managed device on page 12](#)
- ◆ [Agent on page 12](#)
- ◆ [NMS on page 13](#)
- ◆ [MIB on page 13](#)
- ◆ [Messages on page 13](#)
- ◆ [Trap on page 13](#)

SNMP

The SNMP collects and processes valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals. When the network is operating ideally, SNMP establishes a state that is called a baseline, which lists all of the operational parameters.

The SNMP protocol acts as a network safeguard against irregularities that might hamper the functioning of the network. It notifies the system managers of any sudden change in the conditions or the network configuration. It uses network watchdogs, called agents, to monitor network parameters. If an error occurs, or is likely to occur in the near future, SNMP notifies the management station by sending an alert called Trap.

As of this release, a new SNMP agent, the SNMP daemon (SNMPD), which runs on the Data Mover, supports SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 supports IPv4, IPv6, and enhanced security over SNMPv1 and SNMPv2c.

SNMPv3 benefits

SNMPv3 primarily adds security and remote configuration enhancements to SNMPv1 and SNMPv2c.

SNMPv3 provides important security features such as:

- ◆ Authentication to verify that the message is from a valid source
- ◆ Encryption of packets to prevent snooping by an unauthorized source
- ◆ Message integrity to ensure that a packet is not tampered with in transit

Managed device

A managed device contains an SNMP agent, which is a network element that resides on a managed network. Managed devices collect and store the network management information. This information is sent to a NMS using SNMP. A managed device is generally any type of device including but not limited to, routers, access servers, switches, bridges, hubs, and computers.

Agent

An agent is a network management software module that resides in a managed device. The agent has local knowledge of the network management information and it translates that information into a form that is compatible with SNMP.

NMS

A NMS runs applications that monitor and control managed devices. An NMS provides the processing and memory resources required for performing network management. A managed network can have one or more network management systems.

SNMP enables the NMS to act as an SNMP manager and remotely monitor and manage devices such as routers running an SNMP agent. The agent is the interface to the physical device. It receives requests from the NMS and responds with information about the state of the device. The SNMP agent also accepts directives from the NMS to alter the state of the device. It can also send unsolicited messages, or traps, to the SNMP manager to warn of significant events related to the device.

MIB

A Management Information Base (MIB) is a database used to manage the devices in a network. To manage and monitor a device, the characteristics of the device use a format known to the SNMP agent and the manager. The physical and virtual characteristics of the device are represented by network objects. A collection of these objects make up the MIB.

SNMP uses a specified set of commands and queries. A MIB should contain information on these commands and on the target objects, such as controllable devices or potential areas of status information. A MIB tunes the network to achieve the desired results and to avoid errors.

Object Identifier

An Object Identifier is the identification value of an object that is defined in a MIB. Object identifiers are arranged in a hierarchical tree structure.

Messages

In an SNMP operation, network information is exchanged through messages. Each SNMP operation has its own type of message. Management systems use messages to request that an operation be performed on the managed variable maintained by an SNMP agent.

Trap

Traps are network packets that contain data relating to a component of the system sending the trap. The data could be statistical in nature or status related. An SNMP Trap is a message, alert, or notification, which is initiated by a network element and sent to the network management system. SNMP provides the ability to send traps to advise an administrator when one or more conditions have been met. These conditions are defined in the MIB.

Note: Data Mover agent does not send any traps.

The tasks to configure SNMPv3 are:

- ◆ [Enable SNMPD on page 16](#)
- ◆ [Configure SNMPv1 and SNMPv2c support on page 16](#)
- ◆ [Add a new SNMPv3 user on page 17](#)

Enable SNMPD

Action
<p>To enable SNMPD, use this command syntax:</p> <pre>\$ server_snmpd <movername> -service -start</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <hr/> <p>Note: Only a single SNMPD runs on each Data Mover. In the event of a failover, the standby Data Mover runs the SNMPD.</p> <hr/> <p>Example:</p> <p>To enable SNMPD on server_2, type:</p> <pre>\$ server_snmpd server_2 -service -start</pre>
Output
<pre>server_2: OK</pre>

Configure SNMPv1 and SNMPv2c support

Action
<p>To configure SNMPv1 and SNMPv2c, use this command syntax:</p> <pre>\$ server_snmpd <movername> -modify -community <community></pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p><community> = optional community string for SNMPv1 and SNMPv2c. It enables SNMPv1 or SNMPv2c access. The field can have a maximum of 31 characters and accepts any character.</p> <p>Example:</p> <p>To configure SNMPv1 and SNMPv2c on server_2, type:</p> <pre>\$ server_snmpd server_2 -modify -community private</pre>
Output
<pre>server_2: OK</pre>

Add a new SNMPv3 user

Action
<p>To add a new SNMPv3 user with authentication and privacy passwords, use this command syntax:</p> <pre>\$ server_snmpd <movername> -user -create <name> -authpw -privpw</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p><name> = required name of the SNMPD user from 1 to 31 characters. You can use the following characters: 0-9, a-z, A-Z, underscore, hyphen, and dot can be present other than as the first character.</p> <p>Example:</p> <p>To add a new SNMPv3 user on server_2, type:</p> <pre>\$ server_snmpd server_2 -user -create rsmith -authpw -privpw</pre> <hr/> <p>Note: The system prompts you for the authentication and privacy passwords. Both passwords can be from 8 to 250 characters and can accept any ASCII character.</p> <hr/> <pre>Enter the authentication password:***** Confirm the authentication password:***** Enter the privacy password:***** Confirm the privacy password:*****</pre>
Output
<pre>server_2: OK</pre>

The tasks to manage SNMPv3 are:

- ◆ [View SNMPv3 properties on page 20](#)
- ◆ [Modify SNMPv3 properties on page 20](#)
- ◆ [Modify the passwords of an SNMPv3 user on page 21](#)
- ◆ [Display SNMPv3 users on a Data Mover on page 22](#)
- ◆ [Delete an SNMPv3 user on page 22](#)
- ◆ [Verify SNMP status on page 23](#)
- ◆ [Disable SNMPv1 and SNMPv2c on page 23](#)
- ◆ [Disable SNMPPD on page 24](#)

View SNMPv3 properties

Action
<p>To view the properties of the SNMPv3 services for a Data Mover, use this command syntax:</p> <pre>\$ server_snmpd <movername> -info</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p>Example:</p> <p>To view the properties of the SNMPv3 services for server_2, type:</p> <pre>\$ server_snmpd server_2 -info</pre>
Output
<pre>server_2: enabled = yes location = RTP, NC contact = Robert Smith community = public</pre>

Modify SNMPv3 properties

Action
<p>To modify the SNMPv3 properties, use this command syntax:</p> <pre>\$ server_snmpd <movername> -modify -location <location> -contact <contact> -community <community></pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p><location> = optional location of the Data Mover up to a maximum of 254 characters. The field accepts all characters.</p> <p><contact> = optional name of the contact person up to a maximum of 254 characters. The field accepts all characters.</p> <p><community> = optional community string for the SNMPv1 and SNMPv2c. It enables SNMPv1 or SNMPv2c access. The field can have a maximum of 31 characters and can accept any character.</p> <p>Example:</p> <p>To modify the SNMPv3 properties on server_2, type:</p> <pre>\$ server_snmpd server_2 -modify -location "RTP, NC" -contact "Robert Smith" -community public</pre>

Output

```
server_2:
OK
```

Modify the passwords of an SNMPv3 user

Action

To modify the passwords of an SNMPv3 user, use this command syntax:

```
$ server_snmpd <movertime> -user -modify <name> -authpw -privpw
```

where:

<movertime> = name of the Data Mover.

<name> = required name of the SNMPD user from 1 to 31 characters. You can use the following characters: 0-9, a-z, A-Z, underscore, hyphen, and dot can be present other than first character.

Example:

To modify the SNMPv3 passwords for rsmith, type:

```
$ server_snmpd server_2 -user -modify rsmith -authpw -privpw
```

Note: The system prompts you for the authentication and privacy passwords. Both passwords can be from 8 to 250 characters and can be any ASCII character.

```
Enter the authentication password:*****
```

```
Confirm the authentication password:*****
```

```
Enter the privacy password:*****
```

```
Confirm the privacy password:*****
```

Output

```
server_2 :
OK
```

Display SNMPv3 users on a Data Mover

Action
<p>To display the SNMPv3 users on a Data Mover, use this command syntax:</p> <pre>\$ server_snmpd <movername> -user -list</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p>Example:</p> <p>To display the SNMPv3 users on server_2, type:</p> <pre>\$ server_snmpd server_2 -user -list</pre>
Output
<pre>server_2: rsmith</pre>

Delete an SNMPv3 user

Action
<p>To delete a user access from SNMPv3, use this command syntax:</p> <pre>\$ server_snmpd <movername> -user -delete <name></pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p><name> = required name of the SNMPD user from 1 to 31 characters. You can use the following characters: 0-9, a-z, A-Z, underscore, hyphen, and dot (not allowed as the first character).</p> <p>Example:</p> <p>To delete an SNMPv3 user rsmith's access on server_2, type:</p> <pre>\$ server_snmpd server_2 -user -delete rsmith</pre>
Output
<pre>server_2: OK</pre>

Verify SNMP status

Action
<p>To verify if the SNMPD service is running, use this command syntax:</p> <pre>\$ server_snmpd <movername> -service -status</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p>Example:</p> <p>To verify that the SNMPD service is running on server_2, type:</p> <pre>\$ server_snmpd server_2 -service -status</pre>
Output
<pre>server_2: SNMP Running</pre>

Disable SNMPv1 and SNMPv2c

To improve security, you can disable SNMPv1 and SNMPv2c community-based security and switch to SNMPv3. However, all the Network Management Stations may not be SNMPv3 compliant.

Action
<p>To disable SNMPv1 by deleting the community string, use this command syntax:</p> <pre>\$ server_snmpd <movername> -modify -community -clear</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p>Example:</p> <p>To disable SNMPv1 on server_2, type:</p> <pre>\$ server_snmpd server_2 -modify -community -clear</pre>
Output
<pre>server_2: OK</pre>

Disable SNMPD

You must disable the SNMP agent to have no open ports to the network.

Note: The `server_netstat` command is dependent on SNMP. It will stop working when the SNMP agent is disabled.

Action
<p>To disable the SNMPD service, use this command syntax:</p> <pre>\$ server_snmpd <movername> -service -stop</pre> <p>where:</p> <p><movername> = name of the Data Mover.</p> <p>Example:</p> <p>To disable the SNMPD services, type:</p> <pre>\$ server_snmpd server_2 -service -stop</pre>
Output
<pre>server_2: OK</pre>

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 the [EMC Online Support](#) website and resolving problems.

Topics included are:

- ◆ [EMC E-Lab Interoperability Navigator on page 26](#)
- ◆ [VNX user customized documentation on page 26](#)
- ◆ [Error messages on page 26](#)
- ◆ [EMC Training and Professional Services on page 27](#)

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 the EMC Online Support website at <http://Support.EMC.com>. After logging in, locate the applicable Support by Product page, find **Tools**, and click **E-Lab Interoperability Navigator**.

VNX user customized documentation

EMC provides the ability to create step-by-step planning, installation, and maintenance instructions tailored to your environment. To create VNX user customized documentation, go to: <https://mydocs.emc.com/VNX>.

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 website:
 - 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.

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 the EMC Online Support website 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.

You can display the network statistics by using the `server_netstat` command.

Note: The `server_netstat` command does not work when the SNMPD service is disabled, because the SNMP user is not available.

Topics included are:

- ◆ [Display legacy IPv4 network statistics on page 30](#)
- ◆ [Display IPv6 network statistics on page 31](#)

Display legacy IPv4 network statistics

Action		
To display the legacy IPv4 network statistics on a Data Mover, use this syntax:		
<code>\$ server_netstat <movername> -A inet -a</code>		
where:		
<movername> = name of the Data Mover.		
Example:		
To display the legacy IPv4 network statistics of server_2, type:		
<code>\$ server_netstat server_2 -A inet -a</code>		
Output		
Proto	Local Address	Foreign Address (state)

tcp	128.221.252.2.51013	128.221.252.100.818 ESTABLISHED
tcp	*.ftp	*.* LISTEN
tcp	*.sunrpc	*.* LISTEN
tcp	*.1234	*.* LISTEN
tcp	*.nfs	*.* LISTEN
tcp	*.5033	*.* LISTEN
tcp	*.5081	*.* LISTEN
tcp	*.5083	*.* LISTEN
tcp	*.5084	*.* LISTEN
tcp	*.5085	*.* LISTEN
tcp	*.7777	*.* LISTEN
tcp	*.8888	*.* LISTEN
tcp	*.10000	*.* LISTEN
tcp	*.12345	*.* LISTEN
tcp	*.51798	*.* LISTEN
tcp	*.51874	*.* LISTEN
tcp	*.59512	*.* LISTEN
tcp	*.62662	*.* LISTEN
tcp	*.snmp	*.* LISTEN
tcp	*.4658	*.* LISTEN
tcp	*.51013	*.* LISTEN
tcp	128.221.252.2.3081	*.* LISTEN
tcp	128.221.252.2.5082	*.* LISTEN
tcp	128.221.253.2.3081	*.* LISTEN
tcp	128.221.253.2.5082	*.* LISTEN
Proto Local Address		

udp	*.snmp	
udp	*.router	
udp	*.4646	
udp	*.4647	
udp	*.4658	
udp	*.9999	
udp	*.31491	
udp	*.60149	
udp	*.61456	

Display IPv6 network statistics

Action			
To display the IPv6 network statistics on a Data Mover, use this syntax:			
<code>\$ server_netstat <movername> -A inet6 -a</code>			
where:			
<movername> = name of the Data Mover.			
Example:			
To display the IPv6 network statistics of server_2, type:			
<code>\$ server_netstat server_2 -A inet6 -a</code>			
Output			
Proto	Local Address	Foreign Address	(state)

tcp	::.ftp	::.0	LISTEN
tcp	::.sunrpc	::.0	LISTEN
tcp	::.1234	::.0	LISTEN
tcp	::.nfs	::.0	LISTEN
tcp	::.5033	::.0	LISTEN
tcp	::.5081	::.0	LISTEN
tcp	::.5083	::.0	LISTEN
tcp	::.5084	::.0	LISTEN
tcp	::.5085	::.0	LISTEN
tcp	::.7777	::.0	LISTEN
tcp	::.8888	::.0	LISTEN
tcp	::.10000	::.0	LISTEN
tcp	::.12345	::.0	LISTEN
tcp	::.51798	::.0	LISTEN
tcp	::.51874	::.0	LISTEN
tcp	::.59512	::.0	LISTEN
tcp	::.62662	::.0	LISTEN
tcp	::.snmp	::.0	LISTEN
Proto	Local Address	Remote Address	

udp	::.snmp	::.0	

C

command line interface (CLI)

Interface for typing commands through the Control Station to perform tasks that include the management and configuration of the database and Data Movers and the monitoring of statistics for VNX for file cabinet components.

D

daemon

UNIX process that runs continuously in the background, but does nothing until it is activated by another process or triggered by a particular event.

E

event notification

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

See also *notifications*.

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*.

D

- delete
 - user 22
- disable
 - SNMPD 24
 - SNMPv1 23
 - SNMPv2c 23

E

- EMC E-Lab Navigator 26
- error messages 26

I

- IPv4
 - network statistics 30
- IPv6
 - network statistics 31

M

- messages, error 26
- MIB
 - list of RFCs 8
 - object identifier 13

N

- network statistics 29, 30, 31
 - IPv4 30
 - IPv6 31

S

- SNMP

- SNMP (*continued*)
 - agent 12
 - components 11
 - daemon 16
 - description 12
 - Enable SNMPD 16
 - managed device 12
 - message 13
 - MIB 13
 - network statistics 29
 - notifications 13
 - object identifier 13
 - system requirements 8
 - trap 13
- SNMPD
 - disable 24
 - enable 16
- SNMPv3
 - add
 - new user 17
 - benefits 12
 - configure
 - SNMPv1 16
 - SNMPv2c 16
 - delete
 - user 22
 - disable
 - SNMPv1 23
 - SNMPv2c 23
 - display
 - users 22
 - modify
 - password 21
 - new user
 - addition 17
 - properties 20
 - security 12
 - user

SNMPv3 (*continued*)
 user (*continued*)
 password 21
 verify
 status 23

T

troubleshooting 25

U

user interface choices 8

V

verify (*continued*)
 SNMPv3
 status 23
View
 SNMPv3 properties 20