EMC® VNX® Series

Version VNX1, VNX2

Security Configuration Guide for VNX

P/N 300-015-128 REV. 09

March 2020

DELL EMC

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Preface

As part of an effort to improve and enhance the performance and capabilities of its product lines, revisions of product hardware and software are periodically released. 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 Customer Support representative.

Special notice conventions used in this document

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

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

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

NOTICE Addresses practices not related to personal injury.

Note: Presents information that is important, but not hazard-related.

Where to get help

Support, product, and licensing information can be obtained as follows:

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

Troubleshooting—Go to Online Support. After logging in, locate the applicable Support by Product page.

Technical support—For technical support and service requests, go to Customer Service on Online Support. 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 Online Support, you must have a valid support agreement. Contact your product's 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
```

CHAPTER 1

Introduction

This chapter briefly describes a variety of security features implemented on the VNX.

Topics include:

Overview

EMC® VNX® implements a variety of security features to control user and network access, monitor system access and use, and support the transmission of encrypted data. The security features related to VNX for file are implemented on the Control Station and Data Movers. The security features related to VNX for block are implemented on the storage processors. This document provides information about features and configuration options that are available for configuring secure system operation and storage processing. It explains why, when, and how to use these security features. A basic understanding of these features is important to understanding VNX security.

This document is part of the VNX documentation set and is intended for administrators responsible for the overall configuration and operation of VNX. Related features and functionality information lists publications that are related to the features and functionality described in this document.

This document is pertinent to systems running the following software:

- VNX operating environment (OE) for file versions 7.1 and 8.x
- VNX OE for block versions 5.32 and 5.33

Exceptions are noted where applicable.

User interface choices

VNX offers flexibility in managing networked storage that is based on your support environment and interface preferences. This document describes how to set and manage security features using the EMC Unisphere® software. The Unisphere online help contains more information about configuring and managing your VNX. You can also perform these tasks using the EMC Unisphere Management interface. The command line interface (CLI) is different for file-based and block-based services. The *EMC VNX Command Line Interface Reference for Block* describes the CLI commands used to configure and manage a VNX for block system. The *EMC VNX Command Line Interface Reference for File* describes the CLI commands used to configure and manage a VNX for file system. Also, Using VNX for File CLI for security configuration related operations contains detailed information about using the CLI scripts to configure security on the VNX for file.

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

Terminology

The *VNX Glossary* provides a complete list of VNX terminology.

access control entry (ACE): In a Microsoft Windows environment, an element of an access control list (ACL). This element defines access rights to an object for a user or group.

access control list (ACL): A list of access control entries (ACEs) that provide information about the users and groups allowed access to an object.

access policy: The policy that defines what access control methods (NFS permissions and/or Windows ACLs) are enforced when a user accesses a file on a VNX for file system in an environment configured to provide multiprotocol access to some file systems. The access policy is set with the server_mount command and also determines what actions a user can perform against a file or directory.

authentication: The process for verifying the identity of a user trying to access a resource or object, such as a file or a directory.

Certificate Authority (CA): A trusted third party that digitally signs public key certificates.

Certificate Authority Certificate: A digitally signed association between an identity (a Certificate Authority) and a public key to be used by the host to verify digital signatures on Public Key Certificates.

command line interface (CLI): An interface for entering 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 the VNX for file cabinet components.

Common Internet File System (CIFS): A file-sharing protocol based on the Microsoft Server Message Block (SMB). It allows users to share file systems over the Internet and intranets.

Control Station: A hardware and software component of the VNX for file system that manages the system and provides an administrative user interface to VNX for file components.

Data Mover: A VNX for file cabinet component running its own operating system that retrieves files from a storage device and makes them available to a network client.

directory server: A server that stores and organizes information about a computer network's users and network resources, and that allows network administrators to manage users' access to the resources. X.500 is the best-known open directory service. Proprietary directory services include Microsoft's Active Directory.

Hypertext Transfer Protocol (HTTP): The communications protocol used to connect to servers on the World Wide Web.

Hypertext Transfer Protocol Secure (HTTPS): HTTP over SSL. All network traffic between the client and server system is encrypted. In addition, there is the option to verify server and client identities. Typically server identities are verified and client identities are not.

Kerberos: An authentication, data integrity, and data privacy encryption mechanism used to encode authentication information. Kerberos coexists with NTLM (Netlogon services) and, using secret-key cryptography, provides authentication for client/server applications.

LDAP-based directory: A directory server that provides access by LDAP. Examples of LDAP-based directory servers include OpenLDAP or Oracle Directory Server Enterprise Edition.

Lightweight Directory Access Protocol (LDAP): An industry-standard information access protocol that runs directly over TCP/IP. It is the primary access protocol for Active Directory and LDAP-based directory servers. LDAP Version 3 is defined by a set of Proposed Standard documents in Internet Engineering Task Force (IETF) RFC 2251.

Logical Unit Number (LUN): The identifying number of a SCSI or iSCSI object that processes SCSI commands. The LUN is the last part of the SCSI address for a SCSI object. The LUN is an ID for the logical unit, but the term is often used to refer to the logical unit itself.

Network File System (NFS): A distributed file system providing transparent access to remote file systems. NFS allows all network systems to share a single copy of a directory.

OpenLDAP: The open source implementation of an LDAP-based directory service.

persona: A means of providing an identity for a Data Mover as either a server or a client through a private key and associated public key certificate. Each persona can maintain up to two sets of keys (current and next), to allow for the generation of new keys and certificates prior to the expiration of the current certificate.

public key certificate: An electronic ID issued by a certificate authority. It contains the identity (a hostname) of the user or other entity such as a service, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and a digital signature from the certificate-issuing authority so that a recipient can verify that the certificate is valid. For more information, refer to the X.509 standard.

Public Key Infrastructure (PKI): A means of managing private keys and associated public key certificates for use in Public Key Cryptography.

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

Secure Socket Layer (SSL): A security protocol that provides encryption and authentication. It encrypts data and provides message and server authentication. It also supports client authentication if required by the server.

Storage Processor (SP): A hardware and software component of the VNX for block system that runs its own operating system and manages the system and provides an administrative user interface to VNX for block components.

Transport Layer Security (TLS): The successor protocol to SSL for general communication authentication and encryption over TCP/IP networks. TLS version 1 is nearly identical with SSL version 3.

X.509: A widely used standard for defining digital certificates.

XML API : An interface for remotely managing and monitoring a VNX for file. The interface uses XML formatted messages, and is programming language neutral.

Related features and functionality information

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

- *EMC VNX Command Line Interface Reference for File*
- *EMC VNX Command Line Interface Reference for Block*
- *Man pages for File*
- *Parameters Guide for VNX*
- *VNX Glossary*
- *Installing Management Applications on VNX for File*
- *Configuring and Managing CIFS on VNX*
- *Configuring NFS on VNX*
- *Managing a Multiprotocol Environment on VNX*
- *Configuring VNX Naming Services*
- *Using VNX FileMover*
- *Configuring Events and Notifications on VNX for File*
- *Configuring and Managing Networking on VNX*
- *Configuring and Using the Audit Tool on Celerra and VNX for File Technical Note*
- *EMC Secure Remote Support for VNX*
- *Managing the SSL Certificate for the ESRS HTTPS Listener Service Technical Note*
- *Using nas_stig Utility on VNX*

The complete set of EMC VNX customer publications is available on the EMC Online Support website at http://Support.EMC.com. After logging in to the website, click the **Support by Product** page, to locate information for the specific feature required.

For general information on LDAP, refer to:

- RFC 2307, An Approach for Using LDAP as a Network Information Service

For specific information on Active Directory's LDAP and SSL configuration, refer to:

- Microsoft Knowledge Base article How to enable LDAP over SSL with a third-party certification authority (ID 321051)

For specific information on OpenLDAP and SSL configuration, refer to the OpenLDAP website (www.openldap.org). If you are using a different non-Active Directory LDAP-based directory server, refer to that vendor's documentation for information on LDAP and SSL configuration.

Unisphere management suite related white papers

White papers address major aspects of the Unisphere Management Suite, including domain management. These white papers supplement the standard Unisphere administrator and user documentation. Related white papers lists these white papers with a brief overview. The white papers can be found on the EMC Online Support website at http://Support.EMC.com, EMC's password-protected customer- and partner-only extranet.

Table 1 Related white papers

White paper	Description
EMC Unisphere: Unified Storage Management Solution	This white paper provides an overview of EMC® Unisphere®, the single management interface for VNX systems, and legacy CLARiiON® and Celerra® systems. It discusses all the features in Unisphere and lists the features supported by Unisphere v1.0, v1.1, and v1.1.25.
Domain Management with VNX storage systems	This paper discusses the configuration and management of EMC storage systems within a single storage Domain and across multiple domains using Unisphere 1.1.25 software.

CHAPTER 2

Access Control

This chapter describes a variety of access control features implemented on the VNX for file/ unified and VNX for block systems.

Topics include:

Access control settings

Unisphere programs use different strategies to authenticate users; this prevents unauthorized users from accessing VNX systems. These strategies are described in the following sections.

Both Unisphere and CLI provide the same level of security with encrypted, authenticated communications.

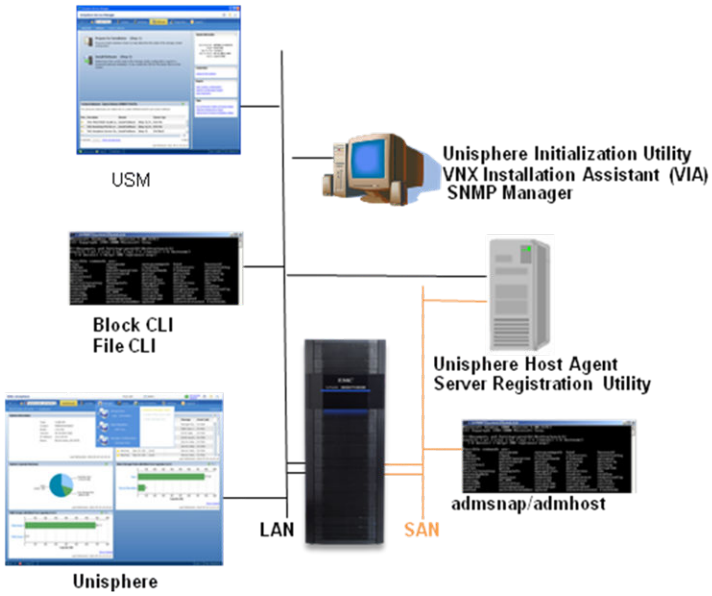
Security for management access

On any VNX storage system, the following management applications can be used to access the system:

- Unisphere - One of the two main applications you use to configure, monitor, and manage VNX systems. Unisphere is a web-based GUI that can be launched by pointing the browser to the IP address of either the Control Station or the Storage Processors (SPs).
- Command Line Interface (CLI) - The other main program you use to manage VNX systems. The CLI is separate for block and file services. Block CLI can be installed and run from any host that has network connectivity to the VNX. File CLI can be accessed by opening a remote session to the Control station using SSH.
- Unisphere Service Manager (USM) - This software allows you to update, install and maintain VNX system hardware and software as well as provide contact and system information to your service provider.
- Unisphere Host Agent or server utility - These optional software programs run on SAN-attached hosts. Their main function is to help communicate host attributes and LUN/volume mappings to the storage system.
- Unisphere Initialization Utility - This optional software allows you to initialize VNX for block systems and network settings from a workstation.
- VNX Installation Assistant (VIA) - This software allows you to initialize VNX unified (block and file) and VNX for file systems and network settings from a workstation.
- SNMP management software - This optional software allows you to monitor the state of VNX systems.
- Admsnap and admhost - These optional management utilities help you manage SnapView™ and SAN Copy™ replication objects.
- Remote support services - Remote EMC support is available for VNX systems. Many customers use this customer service software to allow EMC to help them configure and monitor their systems.
- Unisphere Server software - This software executes the storage management functions described in this guide. In this guide, this software is also called the storage management server. This software is pre-installed on VNX SPs and Control Station. This software can optionally be installed on Windows XP or Windows Server.

As shown in VNX Management components, the various components communicate with the VNX system by both in-band and out-of-band. In-band communication travels over the data connection to the VNX system, while out-of-band communication travels over the management connection to the VNX system.

Figure 1 VNX Management components



It is imperative that management access to the VNX is controlled and limited to authorized users and applications. To secure management access, VNX implements the following main functions:

- Authentication - Identify who is making a request.
- Authorization - Determine if the requestor has the right to exercise the request.
- Privacy - Protect against snooping of data.
- Trust - Verify the identity of communicating parties.
- Audit - Keep a record of who did what, and when.

Authentication

Management applications on a VNX system use authentication to prevent unauthorized users from accessing the system.

Unisphere authentication

Unisphere authenticates users by using usernames and passwords. In Unisphere, the administrator can create user accounts with easy-to-use dialog boxes. When you connect to Unisphere through the browser on your computer, a Java applet is delivered to your browser. The applet establishes a secure connection over SSL/TLS with the storage management server (software that executes the storage management functions) on the VNX through port 443.

Note: Even though `https://` is not displayed in the browser, the connection is secure.

EMC recommends that you connect to Unisphere through https://<vnx_ip> (port 443), although for VNX for block it is possible to connect through http://<vnx_ip> (port 80).

Note: On a Control Station, all HTTP management traffic directed to port 80 will be redirected automatically to the HTTPS port (443).

When you start a session, Unisphere prompts you for a username, password, and scope (local, global, or LDAP). These credentials are encrypted and sent to the storage management server. The storage management server then attempts to find a match within the user account information. If a match is found, you are identified as an authenticated user.

Note: If authentication fails, you can attempt to retry authenticating from the same IP address a maximum of six times. If the sixth attempt fails, the system will block any authentication attempt from the same IP address for four minutes; that is, the system will not respond to another attempt for four minutes. The failure count clears when an initial authentication succeeds or a new authentication attempt succeeds four minutes after the previous failures.

With the exception of VNX gateways, the storage management server also uses authentication and encryption when communicating with other storage management servers. Communication between storage management servers occurs when information is replicated throughout the domain. For example, when user account information changes, the information is replicated to each instance of the storage management server in the domain.

VNX for block CLI authentication

VNX for block CLI requires that user credentials be passed with each command. You can provide user credentials in either of the following ways:

- You can provide credentials with each command.
- You can use the `addusersecurity` command to create a file on the host that stores user credentials. If you enter a VNX for block CLI command without credentials, the CLI gets your credentials from this file and sends your credentials with the command.

  If you do not explicitly include your credentials with CLI commands, this security file must contain valid Unisphere credentials. This file is stored in your home directory and its contents are encrypted. This file and its encryption key are protected by access control lists (ACLs) and a machine-specific pass phrase.

VNX for file CLI authentication

For VNX for file CLI, you need to connect by remote terminal using SSH into the Control Station and log in to the Control station using either a local or global account, or an account with LDAP authentication using SSH. There are two default local accounts on the Control Station (discussed in Default accounts) or you can create a new local account for this purpose.

Logging in to the system using the Control Station CLI

When a domain-mapped user logs in to the Control Station CLI, the domain name provided must match the domain name or fully qualified domain name known to VNX OE for File.

The supported domain-mapped user login formats for LDAP domain-mapped users are:

- <domain name>\<user> (for example, mycompany\anne)
- <user>@<domain name> (for example, anne@mycompany)

The domain name can be specified as the fully qualified domain name. For example:

- <fully qualified domain name>\<user> (for example, mycompany.com\anne)
- <user>@<fully qualified domain name> (for example, anne@mycompany.com)

Note: Users can only log in under a single domain. Consequently, mycompany and mycompany.com are treated as the same domain.

The supported domain-mapped user login formats for storage domain-mapped users are:

- storageDomain\<user> (for example, storageDomain\anne)
- <user>@storageDomain (for example, anne@storageDomain)

Note: storageDomain is a case-sensitive keyword, not a variable, and you must type it exactly as shown.

User scope

User accounts on a storage management server can have one of three scopes:

- Local - This user can access only a single VNX.
- Global - This user can access the entire Unisphere domain.
- LDAP - This user has an account in the LDAP directory, and can access any storage system that uses the LDAP server to authenticate users.

The local scope is ideal when access to a single VNX is required. Users with global scope are easier to manage because you can use one account to access all VNX storage systems within a Unisphere domain. Users with LDAP scope are the most flexible because the accounts are not specific to the storage systems.

There may be duplicate usernames with different scopes. For example, a user "Sarah" with a global scope is different from a user "Sarah" with an LDAP scope.

Authentication with LDAP or Active Directory

The storage management server can authenticate users against directory servers, such as Active Directory (Active Directory is Microsoft's directory server), using LDAP or LDAPS. Authentication against an LDAP server simplifies management because you do not need a separate set of credentials for VNX storage system management. It is also more secure because enterprise password policies can be enforced identically for the storage environment and the server environment.

Managing an LDAP Domain (file/unified and block)

In a VNX domain, the same LDAP server is used for both file/unified and block setup. To manage an LDAP domain, log in to Unisphere and use **All Sysems > Domains > Users** (task list) **> Manage LDAP Domain** to define server connections, accept or validate the related certificates, and map user group roles. As an alternative method, you can select a system, and then use **Settings > Security Settings** (task list) **> Manage LDAP Domain**. After this one-time setup, logins to Unisphere or CLI can be authenticated with an LDAP account. For more information about how to set up connection to an LDAP server, refer to the Unisphere online help.

Managing an LDAP Domain (gateway)

To manage an LDAP configuration for a VNX gateway system, log in to Unisphere and select your system, and then use **Settings > Security Settings** (task list) **> Manage LDAP Domain** to configure the Control Station so it can access the LDAP-based directory server. For more information about how to set up connection to an LDAP server, refer to the Unisphere online help.

After this one-time setup, where Unisphere is configured with connection information for the LDAP server and Unisphere roles are mapped to LDAP groups, logins to Unisphere or CLI can be authenticated with an LDAP account. For a VNX gateway system, LDAP configuration information is specific to the VNX gateway system and is not replicated to any other system.

LDAP service configuration options

Before Unisphere or CLI can authenticate LDAP users, it must be configured to communicate with the LDAP service. Unisphere allows you to add the IP addresses and LDAP connection parameters of the LDAP servers. You will need to obtain the LDAP connection parameters from the LDAP service administrator. When configuring the LDAP service in Unisphere, note the following best practices:

- For highly available communications with the LDAP service, create service connections with two LDAP servers. If one of the servers is unavailable, the storage management server will send the authentication request to the secondary LDAP server.

- For the highest levels of security, configure the service connections to use the LDAPS protocol if your LDAP server supports it. This will ensure that all communication between the storage management server and the LDAP server is encrypted with SSL/TLS so that no user credentials are sent in plain text.

The LDAP configuration needs to be performed only once for each Unisphere domain; the configuration will be replicated to all other nodes within the domain.

Role mapping

Once communications are established with the LDAP service, specific LDAP groups must be given access to Unisphere by mapping them to Unisphere roles. The LDAP service only performs the authentication. Once authenticated, the user's authorization is determined by the assigned Unisphere role. The most flexible configuration is to create LDAP groups that correspond to Unisphere roles. This allows you to control access to Unisphere by managing the members of the LDAP groups.

Note: LDAP user level role mapping that is related to storage processors (SPs) and Unisphere roles can be configured by using the VNX for block CLI. See the *VNX Command Line Interface (CLI) Reference for Block* for more information.

For example, assume that there is an LDAP group called "Storage Admins" of which Bob and Sarah are members. Another LDAP group exists called "Storage Monitors" of which Mike and Cathy are members. The "Storage Admins" group can be mapped to the Unisphere Administrator role, giving Bob and Sarah full control of the storage systems. The "Storage Monitors" group can be mapped to the Unisphere Operator role, giving Mike and Cathy read-only access to the storage systems. If six months later Mike becomes a more trusted administrator, he can be given full access to the storage systems (Administrator role) simply by adding him to the "Storage Admins" LDAP group.

Credential caching and account synchronization (block)

The storage management server locally caches credentials for an LDAP user once the user has been authenticated. This caching minimizes traffic to the LDAP service and enhances the user experience by eliminating latency due to authentication requests. Keep in mind that the storage management server authenticates all commands that modify the storage system configuration and not just at login. Caching eliminates redundant authorization requests to the LDAP server.

By default, Unisphere will clear the local cache every 24 hours to force synchronization with the accounts on the LDAP server. In an environment where user accounts are changing often and credentials need to be flushed, this synchronization interval may be tuned down to 30 minutes without noticeable performance impact. Alternatively, manual synchronization forces an immediate clearing of the local cache. This is useful if an employee is terminated and their access to the storage system needs to be removed in a timely fashion.

Default accounts

Default accounts exist for management access and service access.

Default Management Accounts - See Authentication configuration for information on default management accounts and how to change the related passwords.

Default Service Accounts - Default combinations exist for the management port and service port for access by EMC service personnel. EMC strongly encourages you to change the management port username/password combination (see Secure serviceability settings (block) for more details). Service personnel will need the username and password, so be prepared to disclose this information.

Authentication configuration

Security is initialized differently for VNX unified/file and VNX for block systems.

VNX unified/file systems will have the following management accounts factory installed:

- root - This is a VNX for file local account and provides root-level privileges on the control station.
- nasadmin - This is a VNX for file local account and provides administrator level privileges on the control station.
- sysadmin - This is a global system account and provides administrator level privileges for both VNX for file and VNX for block.

A system account is a special global account that is needed for internal communication between block and file services. VNX unified/file systems require at least one system account. You cannot delete this system account unless another global administrator account or global security administrator account is available.

VNX Installation Assistant (VIA) is the utility for initializing VNX unified/file systems. EMC recommends to change the default password for the three accounts when first initializing a VNX unified/file system using VIA.

VNX for block systems do not have any default management accounts. The Unisphere Initialization wizard is the utility used for initializing VNX for block systems. Security can be initialized on VNX for block systems in the following ways:

- User can choose to create a global account when initializing the system using Unisphere Initialization wizard.
- User can create a global account when first logging into Unisphere.

A system account is not created by default on VNX for block systems because it is not needed; however, adding another VNX unified/file system to the VNX for block system's local domain would require a system account and the user will be prompted accordingly to create a system account.

For all VNX systems (VNX unified/file and VNX for block), at least one global account is required. This account must have the "administrator" or "security administrator" role. An LDAP server(s) can be configured if LDAP authentication is desired, and other global or local accounts can also be created.

Security functions having to do with configuring authentication can be performed either from Unisphere or secure CLI.

User actions performed without authentication

VNX systems will not permit any actions without authentication.

Component authentication (block)

SCSI's primary authentication mechanism for iSCSI initiators is the Challenge Handshake Authentication Protocol (CHAP). CHAP is an authentication protocol that is used to authenticate iSCSI initiators at target login and at various random times during a connection. CHAP security consists of a username and password. You can configure and enable CHAP security for initiators and for targets. Log in to Unisphere and use **All Systems > System List** and right-click the entry for the storage system for which you want to configure CHAP, then use **> iSCSI > CHAP Management**. To enable CHAP, select your system and then use **Settings > Network > Settings for Block**. For more information on configuring and enabling CHAP, refer to the Unisphere online help.

The CHAP protocol requires initiator authentication. Target authentication (mutual CHAP) is optional.

Authorization

The Storage Management Server authorizes user activity based on the role of the user. A role is a collection of access privileges that provides the account administrator with a simple tool for assigning access rights. Unisphere and VNX for file CLI authorize user activity based on the role of the user. VXN for block CLI is based on user credential authentication. Unisphere roles include eight main roles (Operator, Network Administrator, NAS Administrator, SAN Administrator, Storage Administrator, Administrator, Security Administrator, and VM Administrator) and three Data Protection roles (Local Data Protection, Data Protection and Data Recovery).

Note: The main Unisphere roles and data protection roles can have global or local scopes.

Main Unisphere roles

The main roles include:

- Operator - Read-only privilege for storage and domain operations; no privilege for security operations.
- Network Administrator - All operator privileges and privileges to configure DNS, IP settings, and SNMP.
- NAS Administrator - Full privileges for file operations. Operator privileges for block and security operations.
- SAN Administrator - Full privileges for block operations. Operator privileges for file and security operations.
- Storage Administrator - Full privileges for file and block operations. Operator privileges for security operations.
- Security Administrator - Full privileges for security operations including domains. Operator privileges for file and block operations.
- Administrator - Full privileges for file, block, and security operations. This role is the most privileged role.
- VM Administrator - Enables you to view and monitor basic storage components of your VNX system through vCenter by using VMware's vSphere Storage APIs for Storage Awareness (VASA).

Note: The combination of Security Administrator and Storage Administrator privileges is equivalent to those of an Administrator.

As a security and system integrity best practice, superusers (administrators in Unisphere) should not run with full administrative privileges for day-to-day operations. The security administrator role should be used to segment authorized actions between separate accounts. By dividing administrative privileges into security administrator and storage administrator roles, storage administrator accounts will be authorized only to perform storage related actions, and security administrator accounts will only be authorized to perform domain and security related functions. With the security administrator role, accounts with full administrative privileges can be reduced to one and duties can be separated for day-to-day operations.

Unisphere requires the creation of user accounts, where a user account is identified as the unique combination of username, role, and scope. This ability provides flexibility in setting up user accounts. It is expected that most IT personnel will be assigned a global operator account so they can monitor every storage system in the domain. Also, they can be assigned local storage administrator accounts for each specific storage system they are authorized to configure.

You can create global user accounts, each with privileges appropriate to their responsibilities. To create new global user accounts in your local domain, log in to Unisphere and use **All Systems > Domains > Users** (task list) **> Manage Global Users**. Alternatively, select your system, and then

use **Settings > Security > User Management** (task list) **Global Users**. You can only access the global users feature from **Settings** if your selected system is a system in your local domain.

You can create local user accounts for file and block systems, each with privileges appropriate to their responsibilities. A local user for block can only manage block features on the local system. Similarly, a local user for file can only manage file server features on the local system. To create new local user accounts for block, log in to Unisphere and select your VNX for block system, and then use **Settings > User Management** (task list) **Local Users for Block**. To create new local user accounts for file, log in to Unisphere and select your VNX for file system, and then use **Settings > User Management** (task list) **Local Users for File**.

For more information on creating user accounts, refer to the Unisphere online help.

Data Protection roles

Data Protection (Replication) tasks are often performed by third-party personnel. In the earlier releases, a user needed storage administrator-level privileges to perform data protection tasks; however, allowing third-party personnel this level of access could pose a security threat. To solve this problem, VNX systems have three Data Protection roles:

Note: None of these roles allows the user to create new data protection objects such as snapshots, clones, SAN Copy sessions, or mirrors. The user can control only existing data protection objects. Users can view the domain for objects that they cannot control; this allows them to have a fuller understanding of their environment.

- Local Data Protection - Has privileges only to do SnapView (snapshots and clones) and Snapsure (Checkpoints) tasks; however, data recovery operations like rollback a snapshot or reverse synchronize a clone are not allowed. Also, this role does not have privilege to create new storage objects.
- Data Protection - Includes all local data protection privileges, MirrorView, and SAN Copy tasks; however, data recovery tasks such as promoting a secondary and fracturing a mirror are not allowed. Also, this role does not have privilege to create new storage objects.
- Data Recovery - Includes all local data protection and data-protection role privileges and the ability to do data recovery tasks; however, this role does not have privilege to create new storage objects.

Capabilities of data protection roles lists the data protection tasks and which roles have privilege to perform those tasks. VNX for File CLI role-based access provides detailed information about how role-based access is used to determine which of the VNX for file CLI commands (task) a particular user can execute.

Table 2 Capabilities of data protection roles

Task	Local data protection	Data protection	Data recovery
Snapview			
Start a (consistent) snap session	Yes	Yes	Yes
Stop a (consistent) snap session	Yes	Yes	Yes
Activate a session to a snapshot LUN	Yes	Yes	Yes
Deactivate a session from a snapshot LUN	Yes	Yes	Yes
Synchronize a clone	Yes	Yes	Yes

Table 2 Capabilities of data protection roles (continued)

Task	Local data protection	Data protection	Data recovery
Fracture a clone	Yes	Yes	Yes
Roll back a snap session	No	No	Yes
Reverse synchronize a clone	No	No	Yes
Mirrorview			
Synchronize a mirror / consistency group	No	Yes	Yes
Fracture a mirror / consistency group	No	No	Yes
Control the update parameters of an asynchronous mirror	No	Yes	Yes
Modify the update frequency of an asynchronous mirror	No	Yes	Yes
Throttle a mirror / consistency group	No	Yes	Yes
Promote a synchronous or asynchronous secondary mirror / consistency group	No	No	Yes
SAN Copy			
Start a session	No	Yes	Yes
Stop a session	No	Yes	Yes
Pause a session	No	Yes	Yes
Resume a session	No	Yes	Yes
Mark a session	No	Yes	Yes
Unmark a session	No	Yes	Yes
Verify a session	No	Yes	Yes
Throttle a session	No	Yes	Yes

Component access controls

Component access control settings define access to the product by external and internal systems or components.

Component authorization

A storage group is an access control mechanism for LUNs. It segregates groups of LUNs from access by specific hosts. When you configure a storage group, you identify a set of LUNs that will be used by only one or more hosts. The storage system then enforces access to the LUNs from the host. The LUNs are presented only to the hosts in the storage group, and the hosts can see only the LUNs in the group (LUN masking). To configure a storage group, select your system and

then use **Host > Storage Groups**. For more information on configuring a storage group, refer to the Unisphere online help.

IP filtering adds another layer of security by allowing administrators and security administrators to configure the storage system to restrict administration access to specified IP addresses. These settings can be applied to the local storage system or to the entire domain of storage systems. See Secure serviceability settings (block) for more details about IP filtering.

VNX for file CLI role-based access

The administrative user account you use to access the command line interface is associated with specific privileges, also referred to as roles. A role defines the privileges (operations) a user can perform on a particular VNX object. The ability to select a predefined role or define a custom role that gives a user certain privileges is supported for users who access VNX through the CLI, EMC Unisphere™, and the XML API.

VNX for File CLI role-based access provides detailed information about how role-based access is used to determine which of the VNX for file CLI commands a particular user can execute.

Windows-styled credentials for UNIX users

VNX for file allows you to create a common Windows-style (NT) credential. Users therefore have the same credentials regardless of their file access protocol, providing more consistent access control. *Managing a Multiprotocol Environment on VNX* describes how to configure this feature.

Protecting session tokens

The connection between a user and Unisphere and between two VNX for file systems uses SHA1 to generate checksums to protect the session tokens (cookies) that identify users after they log in. The SHA1 secret value used to generate the checksums is set at random during installation; however, to enhance security, you can change the default SHA1 secret value. When you change this value, existing session tokens (cookies) are no longer valid and current users of Unisphere will have to log in again. You must be root to modify Control Station properties. Refer to Protect session tokens for detailed information.

CIFS Kerberos authentication

By default, VNX for file allows both Kerberos and NTLM authentication. Since Kerberos is now the recommended authentication method in Windows environments, you may want to disable NTLM authentication. The *server_cifs* man page describes how to configure this setting and *Configuring and Managing CIFS on VNX* describes authentication.

NFS security settings

Although generally regarded as a vulnerable file-sharing protocol, you can make NFS more secure by using the following configuration settings:

- Defining read-only access for some (or all) hosts
- Limiting root access to specific systems or subnets
- Hiding export and mount information if a client does not have mount permissions for the file system corresponding to that entry

In addition, if strong authentication is required, you can configure Secure NFS, which uses Kerberos. *Configuring NFS on VNX* describes how to configure these settings.

All NFS exports are displayed by default. To hide NFS exports, you must change the value of the **forceFullShowmount** for mount facility parameter using the server_param command.

Access policies for NFS and CIFS

The VNX for file set of customizable access modes allow you to choose the best possible interaction between NFS and CIFS access for your environment. *Managing a Multiprotocol Environment on VNX* describes how to configure this feature.

You can select how security attributes are maintained and the type of interaction between NFS and CIFS users including:

- NATIVE
- UNIX
- NT
- SECURE
- MIXED
- MIXED_COMPAT

The MIXED access policy is required when using NFSv4.

Data security settings

Data security settings enable definition of controls to prevent data permanently stored by the product to be disclosed in an unauthorized manner.

Data integrity

VNX systems use several proprietary data integrity features to protect customer data on the system.

Encryption of data at rest

For information concerning the Data at Rest Encryption (D@RE) feature which is pertinent only to VNX systems running VNX operating environment (OE) for Block versions 5.33 and later, see Data Security Settings.

For more information about encryption of data at rest, please see the document *Approaches for Encryption of Data-At-Rest in the Enterprise* on the EMC Online Support website at http://Support.EMC.com.

Password policy

Strong passwords are an important element of a security strategy. To ensure that sufficiently strong passwords are chosen by all VNX for file local users, you can define a password quality policy that enforces a certain complexity for user-defined passwords. This feature does not apply to domain-mapped users, whose passwords are governed by policies within the domain.

The default password policy includes the following requirements:

- A minimum password length of 8 characters
- A maximum of 3 attempts to define a new password of acceptable value before the command fails
- A minimum of 3 characters that were not in the previous password
- A minimum of one numeral in the new password

Note: There is currently no requirement to use special characters (such as !, @, #, $, %, &, ^, and *) or lower and uppercase characters in the password.

VNX for file also supports a default password expiration period of 120 days.

Note: Changes made to the password quality policy apply only to a password defined after the policy is revised.

Physical security controls

The area where the storage systems reside should be chosen or configured to provide physical security for the VNX systems. These include basic measures such as providing sufficient doors and locks, permitting only authorized and monitored physical access to the system, providing a reliable power source, and following standard cabling best practices.

In addition, the serial port connection requires particular care. EMC and our service partners are capable of enabling emergency access with a serial connection to the storage processor. The customer is responsible for managing the authorized access to the management port as described in Secure serviceability settings (block) as well as for locating the storage system in a physically secure environment. This includes appropriate protection of physical access to the storage processor including the serial port for emergency service.

Restricting anonymous root login on the serial console and SSH enhances system security on VNX for file/unified systems. See Restrict anonymous root login for more information.

Protecting the GRUB boot loader with a password increases the security of the system. Setting a password for GRUB requires root access and can be accomplished by logging in to the CLI as the root user. Set the password in the GRUB configuration file. This file is often located in one of several locations; for example, `/etc/grub.conf`, or `/boot/grub/grub`, or `/boot/grub/menu.lst`. To set a plain-text password, edit your GRUB configuration file by adding the following line before the first uncommented line:

`password`*`<password>`*

Login banner and message of the day

A login banner and message of the day (MOTD) provide a way for an administrator to communicate with VNX for file users. The same login banner is seen from the command line interface and Unisphere. The MOTD is seen only from the command line interface. You must be root to modify Control Station properties.

To configure the banner through Unisphere, select **System > System Management**(task list) **> Control Station Properties**. You can find a description of this feature in Unisphere online help.

To configure the banner and MOTD using the VNX for file CLI, refer to Using VNX for file CLI for security configuration operations for detailed information.

CHAPTER 3

Logging

This chapter describes a variety of logging features implemented on the VNX (includes Block and File only).

Topics include:

Log settings

A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

VNX event logs contain messages related to user management actions, activities by service personnel, and internal events on the storage system that may be helpful for the diagnosis and resolution of storage-system software and hardware issues.

Audit logging on a VNX for block system

Audit logging is intended to provide a record of all activities, so that:

- Checks for suspicious activity can be performed periodically.
- The scope of suspicious activity can be determined

Audit logs are especially important for financial institutions that are monitored by regulators.

Audit information on VNX for block systems is contained within the event log on each SP. The log contains hardware and software diagnostic information as well as audit information. It contains a time-stamped record for each event, and each record contains the following information:

- Event code
- Description of event
- Name of the storage system
- Name of the corresponding SP
- Hostname associated with the SP

The storage management server adds audit records to the event log. An audit record is created each time a user logs in, enters a request through Unisphere, or executes a Secure CLI command. Each audit record is time-stamped, and identifies the following additional information for each request:

- Requestor (Unisphere username)
- Type of request
- Target of request
- Success or failure of request

The storage management server also restricts the ability to clear the audit log to administrators and security administrators only. Whenever the log is cleared by an authorized user, an event is logged to the beginning of the new log. This prevents users from removing evidence of their actions.

All service actions that the RemotelyAnywhere tool performs are also logged. These include logins/logouts, failed logins, file transfers, file modifications, and SP reboots.

SP event logs on VNX for block systems can store only a fixed number of events and will wrap if that limit is exceeded. This may take days, weeks, months, or years depending on the logging activity. Therefore, if the security requirement is to keep all logs for a set period of time, you will need to archive the logs from the VNX for block system on a regular basis. You can do this with the CLI **getlog** command, but a much more integrated method is to use the **log to system log** option of the Event Monitor template to log events to the Windows system log. You can then archive these logs as required.

VNX and RSA Envision

To make VNX storage systems even more secure, they also leverage the continuous collecting, monitoring, and analyzing capabilities of RSA enVision. RSA enVision performs the following functions:

- **Collects logs** - Collects event log data from over 130 event sources - from firewalls to databases. RSA enVision can also collect data from custom, proprietary sources using standard transports such as Syslog, OBDC, SNMP, SFTP, OPSEC, or WMI.
- **Securely stores logs** - Compresses and encrypts log data so that it can be stored for later analysis, while maintaining log confidentiality and integrity.
- **Analyzes logs** - Analyzes data in real time to check for anomalous behavior that requires an immediate alert and response. The RSA enVision proprietary logs are also optimized for later reporting and forensic analysis. Built-in reports and alerts allow administrators and auditors quick and easy access to log data that is easy to understand.

RSA enVision collects and analyzes administrative events logged by VNX storage systems, and creates logs of this information that it stores on the VNX storage system. This gives auditors easy access to scheduled and unscheduled reports about administrative events that occurred on VNX storage systems; the auditor does not have to access the actual device itself or have knowledge of VNX administrative applications. Specific use cases include:

- Providing an audit trail for making copies of data
- Alerting and reporting when replication services malfunction
- Creating reports on daily device configuration changes
- Creating alerts and reports about user actions
- Creating alerts about disks that are removed

Auditing on a VNX for file system

The VNX for file system provides configuration files and commands to capture management activities initiated from the Control Station, specifically access to key system files and end-user data. You must be root to modify Control Station properties.

The Technical Note *Configuring and Using the Audit Tool on Celerra and VNX for File*, available on the EMC Online Support website at http://Support.EMC.com, provides specific information about how to implement auditing on a VNX for file system. To access the Technical Note:

1. Log in to the EMC Online Support website with your user account credentials.
2. Click **Support by Product**.
3. For **Find a Product**, type VNX Series and click **>>**.
4. Click **Documentation >>**.
5. Click **Title** and scroll to the document.

Data at Rest Encryption audit logging

The Data at Rest Encryption (D@RE) feature provides a separate auditing function that supports logging of the following keystore operations:

- Feature activation
- Key creation

- Key destroy
- Keystore backup
- Disk encryption completed
- SLIC addition

The audit log for keystore operations is stored in the private space on the system. Use the VNX for block `securedata -auditlog` CLI command to retrieve audit log and checksum information. For detailed information about the command, see the *Command Line Interface Reference for Block*.

CHAPTER 4

Communication Security

This chapter describes a variety of communication security features implemented on the VNX, VNX for file, and VNX for block systems.

Topics include:

Communication security settings

Communication security settings enable the establishment of secure communication channels between the product components as well as between product components and external systems or components.

Port usage

The ports used by the various components to pass data back and forth are an important aspect of Unisphere communication. Customers that require highly secure network configurations must understand which network ports are required by the various Unisphere components. Firewalls between components must be configured to allow connections from the source component to the port listed on the destination component. Firewalls must also allow traffic back to the source for an established connection (most do by default).

For information related to ports for VNX for block, refer to Ports used by Unisphere components on VNX for block. For information related to ports for VNX for file (Control Station and Data Mover), refer to VNX for file primary network services and VNX for file outgoing network connections.

Ports used by Unisphere components on VNX for block

VNX for block - Ports used by Unisphere components lists the Unisphere components and the ports that are used for communication.

Table 3 VNX for block - Ports used by Unisphere components

Source component	Destination component	Network port	Protocol	Functionality	Type
Unisphere	Storage management server	80/443 or 2162/2163[a]	HTTP/SSL	Basic management	out-of-band
Storage management server	Storage management server	443 or 2163	HTTP/SSL	Storage system to Storage system domain communication	out-of-band
Storage management server	Host Agent	6389	TCP	LUN/volume mapping information displayed in Unisphere	out-of-band
SP Agent (or Host Agent)	SMTP server	25	TCP	Email alerts	out-of-band
Host Agent	SP Agent	6389	TCP	Central monitoring	out-of-band
Unisphere Service Manager	Storage management server	443 or 2163	TCP/SSL	Service Tasks	out-of-band
Block CLI	Storage management server	443 or 2163	TCP/SSL	Basic management	out-of-band
RemotelyAnywhere	RemotelyAnywhere Host	9519, 22	TCP	Remote Support, login, SSH access	out-of-band

Table 3 VNX for block - Ports used by Unisphere components (continued)

Source component	Destination component	Network port	Protocol	Functionality	Type
Storage management server	LDAP Server	389	TCP	Unsecure LDAP queries	out-of-band
Storage management server	LDAP Server	636	TCP	Secure LDAP queries	out-of-band
Storage management server or iSCSI port[b]	iSNS Server	3205	TCP	Internet storage naming service (iSNS)	out-of-band
iSCSI initiator	VNX OE for block	3260	TCP	iSCSI data connection	in-band
Unisphere Storage System Initialization Utility	Storage management server	2162	UDP	Array Discovery	out-of-band
Storage management server	Unisphere Storage System Initialization Utility	2163	UDP	Response to discovery request	out-of-band
Storage management server	NTP Server	123	UDP	NTP time synchronization	out-of-band
SP Agent (or Host Agent)	SNMP Manager	161	TCP/UDP	SNMP Traps	out-of-band
Storage management server	ESX or Virtual Center Server	443	HTTP/SSL	VM-aware Unisphere	out-of-band

a. 2162/2163 are alternate port pairs that may be used (not supported on VNX unified systems) to hide the VNX for block from attacks that target the default HTTP and SSL/TLS ports. Only the Java applet download is allowed over the unsecured HTTP port. All other communication to the storage system is with the secure SSL/TLS port.
b. iSNS registrations will be sent through whichever port can successfully route the packet to the iSNS server.

How VNX for file works on the network

At its core, VNX for file is designed to function as a Common Internet File System (CIFS) and/or as a Network File System (NFS) file server. FTP and TFTP services are also available. The methods used to access VNX for file for these purposes (for example, the ports and protocols to use) are defined by standards. Thus, the VNX for file network presence is largely dictated by these standards. In addition, like any network device, there are ancillary services (for example, VNX Replicator, User Mapper, and such) that are expected by client systems and compatibility concerns dictate that VNX for file provide these services.

There are several ways of examining or describing the VNX for file network presence. One method is to enumerate the open network ports and describe their characteristics (for example, whether they are standard network services or VNX for file-specific services). Most of these ports are standard network ports whose external properties (for example, port number, authentication method, and service provided) are determined by existing standards. These standards are usually Request for Comments (RFCs), but they may be de facto standards as well. (Most often, this occurs in conjunction with CIFS services, where compatibility with Microsoft's file services is important.)

Another method to describe the VNX for file network presence takes a higher, more contextual approach such as what services are provided to end users (who access files on VNX for file), what

services are provided to manage and monitor VNX for file, and what is available to work in a network environment (for example, the portmap or rpcbind service on port 111).

Another and more contextual approach of examining or describing the VNX for file network presence would be to list the applicable services being provided, such as the following:

- which services are provided to end users (who access files on VNX for file)
- which services are provided to manage and monitor VNX for file
- which services are available to work in a network environment (for example, the portmap or rpcbind service on port 111)

Defense in depth

Because the behavior of the vast majority of the open network ports on VNX for file is governed by network standards, there are no additional steps available for VNX for file to protect these ports other than disabling their associated services and closing the ports. Disabling services such as portmap will hinder the general operations of VNX for file, and in some cases, the impact will be severe.

However, the notion of defense in depth dictates that any potential vulnerability is addressed with additional protections to control who may access the ports. This may be done with firewalls in the network environment (external to VNX for file) or by enabling the iptables functionality on the Control Station.

In addition, the VNX for file Data Mover provides two powerful mechanisms for controlling network connectivity:

- Packet Reflect
- Virtual local area networks (VLANs)

Packet Reflect ensures that outbound (reply) packets always exit through the same interfaces through which the inbound (request) packets entered. Because majority of the network traffic on a Data Mover, including all file system I/O, is initiated by the client, the Data Mover uses Packet Reflect to reply to client requests. With Packet Reflect, there is no need to determine the route to send the reply packets. Packet Reflect is enabled by default.

VLANs are logical networks that function independently of the physical network configuration. For example, VLANs enable you to put all of a department's computers on the same logical subnet, which can increase security and reduce network broadcast traffic.

Configuring and Managing Networking on VNX provides additional information about Packet Reflect and VLANs as well as how to configure these features.

Network services on VNX for file

In Unisphere, you can list the current state of some network services (and associated communications ports and protocols) on the Control Station and Data Movers. You can enable, disable, and monitor these services. To improve VNX for file security, you should restrict access to VNX for file by disabling network services that are not used in your environment. You must be root to modify Control Station properties. Some services that are running on the Data Movers require a reboot for changes to take effect.

To manage network services through Unisphere, select **Settings > Network > Settings for File > Network Services**. You can find a description of this feature in Unisphere online help.

Session timeout on VNX for file

VNX for file enforces a session timeout for administrative sessions accessed from both Unisphere and Control Station shells. Sessions time out after a specified period of inactivity. Session timeout is enabled by default. You must be root to modify Control Station properties.

To manage Unisphere session timeout, select **Settings > Security Settings** (task list) **> Manage Idle Timeout**. You can find a description of this feature in the Unisphere online help.

You can manage shell session timeout using the VNX for file CLI. Refer to Configuring session timeout for detailed information.

Private networks

VNX for file uses 128.221.252, 128.221.253, and 128.221.254 for internal subnets. If these subnets may cause interference with your existing subnets, they can be changed during the initial installation of the system by EMC professional services. During installation, an attempt is made to communicate with the EMC VNX for block (if appropriate) by using the private IPs to determine whether the system is a gateway or a unified system. Therefore, during the installation, specific IPs from these subnets will be pinged. This check is limited to the installation and there should not be any communication on the public network for any of the private IPs under normal operation.

VNX for file primary network services

At the highest level, VNX for file provides NFS, CIFS, and FTP or TFTP file access services to end users. These are the final services provided and generally, the reason why VNX for file exists in the network environment. To some extent, all other network activity related to VNX for file is ancillary to this functionality; the additional network services exist to support these high-level services.

VNX for file Data Mover network ports and VNX for file Control Station network ports outline the collection of network services (and the corresponding ports) that may be found on VNX for file. VNX for file Data Mover network ports addresses the services on a Data Mover, and VNX for file Control Station network ports addresses the services on a Control Station.

Note: Not all VNX for file deployments have all these services available. For example, a VNX for file system may be configured to provide either CIFS or NFS file services. It is also worth noting that some of the ports are dynamically allocated, meaning that there is no set port number associated with the service. In these cases, an administrator may notice that a different port is used rather than the ones specified in these tables.

VNX for file CIFS network services

When CIFS network services are enabled on VNX for file and configured to work with an existing Windows infrastructure (for example, Microsoft's Active Directory), a broad set of network services (and their corresponding ports) must be enabled. Some of these ports (137, 138, and 139 on the Data Mover) exist to support the older Windows systems (Windows NT and earlier). Other ports are used to communicate with an Active Directory server to authenticate users or receive Group Policy Object (GPO) configuration directives.

Typically, network traffic is authenticated based on the existing standards set by Microsoft practices. Access to shares, files, and directories is authenticated by using Active Directory credentials. However, there is a great deal of control over how CIFS users are authenticated. This is described in detail in a variety of documents on VNX for file management. In particular, the following documents provide useful information:

- *Configuring and Managing CIFS on VNX*
- *Managing a Multiprotocol Environment on VNX*

These documents are particularly useful if files and directories are going to be made simultaneously available to both CIFS and NFS users.

Besides the standard, Kerberos-based, Active Directory authentication approach for CIFS in Windows 2000 and 2003 environments, VNX for file also supports NTLMv2 for Windows NT environments and UNIX and share-level passwords. The latter two methods are not recommended; they exist to support very specialized environments. The documentation about configuring CIFS outlines their use.

A recommended method to segregate several CIFS environments within the same physical Data Mover is to use Virtual Data Movers (VDMs). A VDM is a VNX for file software feature that enables administrators to group file systems and NFS and CIFS servers into virtual containers. Each VDM can support many CIFS/NFS points of presence. A single VDM contains DNS, LDAP, and/or NIS user domain. If your environment calls for multiple and isolated AD domains, a separate VDMs for each domain should be used. *Configuring Virtual Data Movers on VNX* provides details about VDM concepts and management techniques.

Management of the VNX for file CIFS services requires a two-pronged approach. The initial provisioning to create volumes, file systems, and shares is performed from the VNX for file Control Station (by using either the command line interface or the Unisphere software graphical user interface). However, you must use Windows management tools to set the security attributes of shares. This is consistent with most customers' request to integrate into the traditional Windows workflow or management infrastructure.

VNX for file CIFS network presence

When a high-level CIFS service is activated on VNX for file, a collection of network services or ports is activated on the Data Mover to support the CIFS client access. The functionality and behavior of specific ports are described in VNX for file Data Mover network ports. The activated ports are:

- Ports 137, 138, and 139 - NETBIOS services for older CIFS clients.
- Port 445 - The main access point for CIFS file services. It replaces the 137, 138, and 139 ports.
- Port 12345 - For the usermapper service-mapping Windows Security Identifiers (SIDs) to UNIX-style User ID (UIDs) and Group IDs (GIDs)

SMB encryption and signing

VNX for file/unified systems support of SMB 3.0 and Windows 2012 includes encrypting CIFS traffic on the network. This encryption of data in transit provides end-to-end encryption of all SMB data and requests sent between the CIFS server and the client system and protects these exchanges from eavesdropping or snooping attacks on the network.

SMB encryption can be configured per share or for each CIFS or Virtual Data Mover (VDM) CIFS server. Once a share is defined as encrypted, any SMB3 client must encrypt all its requests related to the share; otherwise, access to the share will be denied.

Note: Use of SMB encryption impacts performance and CPU utilization on both client and server.

To enable SMB encryption, you either set the encryption through the **server_export** command or set it through the registry of the CIFS server. There is no setting required on the SMB client.

A new type option, **Encrypted**, has been added to the server_export command. If you set this option, it indicates that the server requires encrypted messages for accessing the CIFS share. For example, to create a share "share10" that is accessible only through encrypted SMB messages, type **server_export vdm1 -P cifs -name share10 -o type=Encrypted /fs42/protected_dir1**.

For encrypting all shares at the CIFS/VDM CIFS server level, new values, EncryptData and RejectUnencryptedAccess, have been added into the CIFS server registry (at HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > LanmanServer > Parameters).

Table 4 SMB encryption registry values

Registry Value	Type	Default Value	Description
EncryptData	DWORD	0 (disabled)	If enabled, all the sessions established from any SMB3 clients to the CIFS server should be encrypted.
RejectUnencryptedAccess	DWORD	1 (enabled)	If enabled, the SMB3 client must encrypt its message. If the client sends an unencrypted message instead, the server will return an ACCESS_DENIED error. Also, SMB1, SMB2.0, and SMB2.1 clients will not be able to access an encrypted share or a CIFS server that requires encrypted sessions.

Note: For more information about setting SMB encryption, refer to the *VNX Command Line Interface Reference for File*, and the *Configuring and Managing CIFS on VNX* technical module.

Incoming traffic and outgoing traffic are encrypted using two different secret keys. Both are computed once the user is authenticated successfully. The encryption and decryption 16-bytes keys are generated using the Key Derivation Function (KDF) algorithm in Counter Mode. SMB messages on the network are encrypted between the client and server using the AES128-CCM cryptographic algorithm. Any SMB2 message can be encrypted, except SMB2_NEGOTIATE and SMB2_SESSION_SETUP.

SMB also provides data integrity validation (signing). This mechanism ensures that packets have not been intercepted, changed, or replayed. SMB signing adds a signature to every packet and guarantees that a third party has not changed the packets. When signed, the SMB2 messages contained in the SMB2_HEADER buffer a 16-bytes signature that guarantees the integrity of the message. If SMB3 is negotiated, the sender must compute a 16-byte hash using the AES128-CCM cryptographic algorithm over the entire message, beginning with the SMB2 Header and using the signing key. The signing key is generated using the KDF algorithm in Counter Mode. The Pseudo Random Function (PRF) used in the key derivation must be HMAC-SHA256. The SMB signing policy can be changed through Global Policy Objects (GPOs) or Windows Registry settings.

Note: For more information about configuring SMB signing, refer to the *Configuring and Managing CIFS on VNX* technical module and the *Parameters Guide for VNX for File*.

VNX for file NFS network services

NFS network services are more straightforward than CIFS network services in many cases, but they do not offer the same level of authentication and tight integration with an enterprise environment. When a high-level NFS service is activated on VNX for file, a collection of network services or ports is activated on the Data Mover to support NFS client access and the standard services expected. The functionality and behavior of specific ports are described in VNX for file Data Mover network ports. The activated ports are:

- Port 1234 on the Data Mover for the mount service
- Port 2049 on the Data Mover for the NFS and NFSv4 services
- Port 31491 on the Data Mover for the Remote File Access (RFA) service

VNX provides a multinaming domain solution for the Data Mover in the UNIX environment by implementing a NFS server per Virtual Data Mover (VDM). This solution implements an NFS server per VDM named 'NFSendpoint'. The VDM is used as a container that includes the file systems exported by the NFS endpoint and/or the CIFS server. These file systems of the VDM are visible through a subset of the Data Mover network interfaces attached to the VDM. The same network interface can be shared by both CIFS and NFS protocols on that VDM. The NFS endpoint and

CIFS server are addressed through the network interfaces attached to that particular VDM. *Configuring Virtual Data Movers on VNX* provides more information about this feature.

Note: *Configuring NFS on VNX* provides information about NFS only. *Managing a Multiprotocol Environment on VNX* provides information about configuring the VNX to support both NFS and CIFS.

VNX for file Data Mover network ports

Note: Unisphere enables you to manage some network services. The Unisphere interface shows the current status of most network services (enabled or disabled) and provides a convenient means of enabling or disabling the services. Select your system then use **Settings for File** > **Network Services**. For more information about enabling and disabling network services, refer to the Unisphere online help.

Table 5 VNX for file Data Mover network ports

Port	Protocol	Default State	Service	Comments
20	TCP	Closed	FTP	Port used for FTP data transfers. This port can be opened by enabling FTP as described in the next row. Authentication is performed on port 21 and defined by the FTP protocol.

21	TCP	Closed	FTP	Port 21 is the control port on which the FTP service listens for incoming FTP requests.
				All Data Movers run the FTP service. You can enable the FTP service by using the following command:
				`server_ftp <movername> -service -start`
				You can disable the FTP service by using the following command:
				`server_ftp <movername> -service -stop`
				The authentication process is defined by the FTP protocol definition (RFC 959) and cannot be changed. It is possible to authenticate by using either UNIX names or a Windows domain and username (domain \user).
				Using FTP, TFTP and SFTP on VNX provides details about running and managing the FTP service on a Data Mover.

22	TCP	Closed	SFTP (FTP over SSH)	SFTP is a client/server protocol. Users can use SFTP to perform file transfers on a VNX system on the local subnet. The underlying SSH version 2 protocol provides well separated layers for secure file transfer between systems.

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				Using FTP, TFTP and SFTP on VNX provides details about running and managing the FTP service on a Data Mover.

69	UDP	Closed	TFTP	Initially, TFTP listens on the UDP port 69. After a request is read on port 69, a different port is randomly chosen for the TFTP data transfer. By definition (RFC 1350), TFTP does not authenticate requests.
				The TFTP service is not started by default; it must be manually started.
				You can enable the TFTP service by using the following command:
				`server_tftp <movername> -service -start`
				You can disable the TFTP service by using the following command:
				`server_tftp <movername> -service -stop`
				Using FTP, TFTP and SFTP on VNX provides details about running and managing the FTP service on a Data Mover.

111	TCP UDP	Open	rpcbind (Network infrastructure)	This port is opened by the standard portmapper or rpcbind service and is an ancillary VNX for file network service. It cannot be stopped. By definition, if a client system has network connectivity to the port, it can query it. No authentication is performed.
123	UDP	Closed	NTP	This port is related to the NTP (Network Time Protocol). It can be opened when NTP is configured on the Data Mover.
135	TCP	Open	DCE Remote Procedure Call (DCERPC)	Multiple purposes for MicroSoft client.
137	UDP	Closed	NETBIOS Name Service (CIFS)	This port can be opened by using the following command: `server_setup <movername> -Protocol cifs -option start` This port can be closed by stopping CIFS services. Use the following command:

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				`server_setup <movername> -Protocol cifs -option stop` Note that this disables all CIFS-related services. The NETBIOS Name Service is associated with the VNX for file CIFS file sharing services and is a core component of that feature. If CIFS services are enabled, then this port is open. It is specifically required for earlier versions of the Windows OS (pre-Windows 2000). Clients with legitimate access to VNX for file CIFS services must have network connectivity to the port for continued operation.

138	UDP	Closed	NETBIOS Datagram Service (CIFS)	This port can be opened by using the following command:
				`server_setup <movername> -Protocol cifs -option start`
				This port can be closed by stopping CIFS services. Use the following command:
				`server_setup <movername> -Protocol cifs -option stop`
				Note that this disables all CIFS-related services.
				The NETBIOS Datagram Service is associated with the VNX for file CIFS file sharing services and is a core component of that feature. If CIFS services are enabled, then this port is open. It is specifically required for earlier versions of the Windows OS (pre-Windows 2000). Clients with legitimate access to VNX for file CIFS services must have network connectivity to the port for continued operation.

139	TCP	Closed	NETBIOS Session Service (CIFS)	This port can be opened by using the following command:
				`server_setup <movername> -Protocol cifs -option start`
				This port can be closed by stopping CIFS services. Use the following command:
				`server_setup <movername> -Protocol cifs -option stop`

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				Note that this disables all CIFS-related services. The NETBIOS Session Service is associated with the VNX for file CIFS file sharing services and is a core component of that feature. If CIFS services are enabled, then this port is open. It is specifically required for earlier versions of the Windows OS (pre-Windows 2000). Clients with legitimate access to VNX for file CIFS services must have network connectivity to the port for continued operation.

161	TCP/UDP	Closed	SNMP	This port is used to provide Simple Network Management Protocol (SNMP), which is a management and monitoring service used by many third-party management tools. 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.
				Authentication of SNMPv1 and v2c is based on a client system using the correct community string. The community string is "public" by default and should be changed by using the following command:
				`server_snmpd <movername> -modify -community <community>`
				SNMPv3 uses authentication and privacy passwords which can be configured using the following command:
				`server_snmpd <movername> -user -create <user> -authpw -privpw`
				SNMP is used for some communication between the Control Station and the Data Mover. If it is disabled, the `server_netstat` command will cease to function properly.
				The SNMP service on a Data Mover can be disabled using the following command:
				`server_snmpd <movername> -service -stop`

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				See *Using SNMPv3 on VNX* for more details on SNMP.
445	TCP	Open	CIFS	This port is the new default CIFS connectivity port for Windows 2000 and later clients. The port is opened by enabling CIFS services. Use the following command: `server_setup <movername> -Protocol cifs -option start` This port is closed by stopping CIFS services. Use the following command: `server_setup <movername> -Protocol cifs -option stop` Note that this disables all CIFS-related services. Clients with legitimate access to the VNX for file CIFS services must have network connectivity to the port for continued operation. Authentication is addressed on this port in accordance with Microsoft practices.
500	UDP	Closed	Iked	This port is for the Internet Key Exchange Daemon.
520	UDP	Open	Routing Information Protocol (RIP) (Network infrastructure)	This port can be closed by using the following command: `server_setup <movername> -Protocol rip -option stop` This port can be opened by using the following command: `server_setup <movername> -Protocol rip -option start` Routing Information Protocol (RIP) is a routing protocol optimized for creating routes within one organization (interior gateway protocol). RIP is a distance-vector protocol that uses hop count (max 15) as the metric. RIP-1 does not send the mask in updates. RIP-2 sends the mask in updates. *Configuring and Managing Networking on VNX* explains the purpose and configuration of RIP services on the Data Mover. Instructions for disabling the service are also included.
989	TCP	Closed	FTPS	FTPS data transfer port. Connections are initially established on port 990 and data connections are on this port. See RFC 4217: *Securing FTP with TLS*.

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
990	TCP	Closed	FTPS	FTPS control port where FTPS sessions are initially established. The authentication process is defined by RFC 4217: *Securing FTP with TLS*. It is possible to authenticate using either UNIX names or a Windows domain and username (domain\user). Using FTP, TFTP and SFTP on VNX provides information about FTPS and TLS/SSL operations.
1020	TCP (defaults to a port number greater than 1024) UDP	Closed	CDMS nfs FileMover for NFS	This port can be used for the CDMS nfs migration or FileMover for NFS services. Clients of both services must have network connectivity to the port for continued operation. *VNX File System MigrationVersion 2.0 for NFS and CIFS* provides more information about file system migration operations. *Using VNX FileMover* provides more information about FileMover operations.
1021	TCP (defaults to a port number greater than 1024) UDP	Closed	CDMS nfs FileMover for NFS	This port can be used for the CDMS nfs migration or FileMover for NFS services. Clients of both services must have network connectivity to the port for continued operation. *VNX File System MigrationVersion 2.0 for NFS and CIFS* provides more information about file system migration operations. *Using VNX FileMover* provides more information about FileMover operations.
1234	TCP UDP	Open	mountd (NFS)	This port is used for the mount service, which is a core component of the NFS service (versions 2 and 3), and is an important component of the Control Station to Data Mover interaction, even if there are no NFS exports externally visible from the Data Mover. *Configuring NFS on VNX* explains several methods of controlling access to NFS exports. Authentication of users is AUTH_SYS by default. If stronger authentication is desired, Secure NFS is generally available. Secure NFS provides Kerberos authentication for end users
2049	TCP UDP	Open	NFS	This port is used to provide NFS services and is an important component of the Control Station to Data Mover interaction, even if there are no NFS exports externally visible from the Data Mover.

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				Configuring NFS on VNX explains several methods of controlling access to NFS exports. Authentication of users is AUTH_SYS by default. If stronger authentication is desired, Secure NFS is generally available. Secure NFS provides Kerberos authentication for end users. If AUTH_SYS authentication is used, only port 2049 need be open between VNX for file and NFSV4 clients.
2400	TCP UDP	Closed	FMP/Notify	This port is is used to provide FMP/notify service. This service is used by the VNX for file NFS Cluster product. To determine if any NFS Clusters are configured, use the `nas_server -l` command. The cluster has the type "group." To remove any NFS clusters, use the following command: `nas_server <cluster_name> -delete`
4647	UDP	Open	lockd forward (Infrastructure for NFS Cluster)	This is not a public service. It is used only on the VNX for file interconnection network. External clients will not need to reach this service. It can be blocked by a firewall. This service is used by the VNX for file NFS Cluster product. To determine if any NFS Clusters are configured, use the `nas_server -l` command. The cluster has the type "group." To remove any NFS clusters, use the following command: `nas_server <cluster_name> -delete`
4656	TCP UDP	Closed	FMP	(Applicable only to systems running VNX OE for file earlier than version 8.x.) This port is associated with the Multi-Path File Services (MPFS) feature. It can be opened by using the following command: `server_setup <movername> -Protocol mpfs -option start` For the MPFS service to work, clients must be able to contact VNX for file on the FMP port and VNX for file must be able to contact the clients on their FMP port (Port 6907 for UNIX clients and port 625 for Windows clients).

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
4658	TCP	Open	Portable Archive Interchange (PAX) - (Backup Services)	PAX is a VNX for file archive protocol that works with standard UNIX tape formats. The protocol is used only between the Control Station and Data Mover. It is only used on the private network. This service may be disabled if local tape backup is not used. Details on how to disable this service are in Primus under ID emc49339. Background information on PAX is contained in the relevant EMC documentation on backups and NDMP. There are several technical modules on this topic to deal with a variety of backup tools.
5033	TCP	Open	Network Block Service (NBS)	An EMC proprietary protocol similar to (and a precursor of) iSCSI. The NBS service that opens this port is a core VNX for file service and cannot be stopped. Externally, NBS is used for snapshot and replication control functions. When used for Control Station to Data Mover communication, the private VNX for file interconnection network is used.
5080	TCP	Closed	HTTP (FileMover support and internal infrastructure)	HTTP is used as a transport medium for FileMover and for some Control Station to Data Mover information exchanges. FileMover traffic is for ILM-related policy engines to send commands to the Data Mover. The policy engines are authenticated by using the HTTP digest authentication method. This is described in the FileMover documentation. *Using VNX FileMover* explains the configuration and monitoring commands. HTTPS (HTTP over SSL) is also available on the Data Mover. Because the HTTP transport is also used for Control Station to Data Mover interactions, the service may not be disabled. However, this only requires that the Data Mover accept the HTTP requests from the Control Station over the private network within the VNX cabinet. Access to the HTTP service by external agents is disabled by default
5081	TCP	Open	Replication services	Data Mover-to-Data Mover replication commands.

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
5083	TCP	Open	Replication services	This port is associated with replication services.
5084	TCP	Open	Replication services	This port is associated with replication services.
5085	TCP	Open	Replication services	This port is associated with replication services.
7777	TCP	Open	Statistics monitoring service	This is the default port for the statistics monitoring service. It may be closed by running the following command: `server_stats <movername> -service -stop` *Managing Statistics for VNX* provides information about configuring this service.
8887	TCP	Closed	Replication services	This port is used for replication (on the primary side). It is opened by the replicator when a Data Recovery (DR) is requested. It is closed when the DR is completed. Clients (other VNX for file systems) that use the replication service must be able to communicate with this port.
8888	Replication services	Open	RCP (Replication services)	This port is used by the replicator (on the secondary side). It is left open by the replicator as soon as some data has to be replicated. After it is started, there is no way to stop the service. Clients (other VNX for file servers) that use the replication service must be behind the same firewall for continued operation.
10000	TCP	Open	NDMP (Backup services)	The Network Data Management Protocol (NDMP) enables you to control the backup and recovery of an NDMP server through a network backup application, without installing third-party software on the server. In VNX for file, the Data Mover functions as the NDMP server. The NDMP service can be disabled if NDMP tape backup is not used. The NDMP service is authenticated with a username/password pair. The username is configurable. The NDMP documentation describes how to configure the password for a variety of environments.
10001 through 10004	TCP	Closed	NDMP	For a single three-way backup/restore only, TCP connections between Data Movers use port 10001. If there are multiple

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				three-way backup/restore sessions, Date Mover uses ports 10001 to 10004.
12345	TCP UDP	Open	usermapper (CIFS)	The usermapper service opens this port. It is a core service associated with VNX for file CIFS services and should not be stopped in specific environments. This is the method by which Windows credentials (which are SID-based) are mapped to UNIX-based UID and GID values. It is possible to close this port. The command to do this is: `server_usermapper <movername> -disable` *Configuring VNX User Mapping* provides more information about configuring this service in Windows-only and multiprotocol environments.
31491	UDP	Open	Remote File Access (RFA) NFS functionality	The service that opens this port is RFA and is a core VNX for file service associated with NFS. It cannot be stopped.
38914	UDP	Closed	nfs forward (Infrastructure for NFS Cluster)	This is not a public service. It is used only on the VNX for file interconnection network. External clients do not need to reach this service. It can be blocked by a firewall. This service is used by the VNX for file Cluster product. To determine if any NFS Clusters are configured, use the `nas_server -l` command. The cluster has the type "group." To remove any NFS clusters, use the following command: `nas_server <cluster_name> -delete`
49152 through 65535	TCP UDP	Open	statd NFS support	statd is the NFS file-locking status monitor and works in conjunction with lockd to provide crash and recovery functions for NFS (which is inherently a stateless protocol). statd is a core VNX for file service, but it can be stopped. To stop this service: 1. Use vi to edit the following file: `/nas/server/<server_name>/netd` 2. Comment out the statd line. statd becomes #statd.

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				3. Restart the Data Mover. This may be reset automatically during an upgrade. Be sure to recheck. Clients with legitimate access to the VNX for file NFS services need to have network connectivity to this port.
49152 through 65535	TCP UDP	Open	rquotad Quota support	The rquotad daemon provides quota information to NFS clients that have mounted a file system. An NFS user who has mounted a VNX for file file system can access quota information for the file system by using the quota command. This command runs on the client side and interrogates the rquotad daemon on the Data Mover through RPC. To use this functionality, the client must have already mounted the file system. Authentication is AUTH_SYS, similar to that used for the NFS protocol. You must have root access to the file system to get the quota information for different users. rquotad can be stopped: 1. Use vi to edit the following file: `/nas/server/<server_name>/netd` 2. Comment out the rquotad line. rquotad becomes #rquotad. 3. Restart the Data Mover. This may be reset automatically during an upgrade. Be sure to recheck. Clients with legitimate access to the VNX for file NFS services need to have network connectivity to this port.
49152 through 65535	TCP UDP	Open	lockd NFS support	lockd is the NFS file-locking daemon. It processes lock requests from NFS clients and works in conjunction with the **statd** daemon. lockd is a core VNX for file service, but it can be stopped. To stop this service: 1. Use vi to edit the following file: `/nas/server/<server_name>/netd` 2. Comment out the lockd line. lockd becomes #lockd. 3. Restart the Data Mover.

Table 5 VNX for file Data Mover network ports (continued)

Port	Protocol	Default State	Service	Comments
				This may be reset automatically during an upgrade. Be sure to recheck.
49152 through 65535	TCP UDP	Open	MAC	MAC is a proprietary management protocol between the Control Station and Data Mover. It is used only on the private network between the two. This is a core service and cannot be stopped.

VNX for file Control Station network ports

Note: Unisphere enables you to manage some network services. The Unisphere interface shows the current status of most network services (enabled or disabled) and provides a convenient means of enabling or disabling the services. Select your system then use **Settings for File** > **Network Services**. For more information about enabling and disabling network services, refer to the Unisphere online help.

Table 6 VNX for file Control Station network ports

Port	Protocol	Default State	Service	Comments
22	TCP	Open	SSH	SSH is the default method of getting a shell to use the Control Station CLI. Telnet and other related services are not enabled by default. SSH is the recommended method to access the Control Station. Authentication is handled by the SSH daemon and uses the local user account information on the Control Station. **Note:** Although this port can be closed by running the command `/sbin/service sshd stop` followed by `/sbin/chkconfig -levels 2345 sshd off`, this is not recommended.
80	TCP	Open	HTTP	This is the standard HTTP port. All HTTP management traffic directed to this port is automatically redirected to the HTTPS port (443). No services are offered over port 80.
111	TCP UDP	Open	rpcbind	The standard portmapper or rpcbind process opens this port and is an ancillary network service; it cannot be stopped. If a client system has network connectivity to the port, the client can query it. There is no authentication performed.
123	UDP	Closed	NTP	This port is related to the NTP (Network Time Protocol). It can be opened when NTP is configured on the Control Station.

Table 6 VNX for file Control Station network ports (continued)

Port	Protocol	Default State	Service	Comments
161	TCP/UDP	Closed	SNMP Management infrastructure	SNMP is a management and monitoring service used by many third-party management tools. The Control Station uses SNMP version 1 as defined by RFC 1157. This version of SNMP does not support modification of any of the monitored values. Authentication is based on a client system using the correct community string. The community string is "public" by default and should be changed. Use the command `/sbin/service snmpd start` followed by `/sbin/chkconfig snmpd on` from the root account to enable SNMP. The SNMP service can be disabled by running the command `/sbin/chkconfig snmpd off` followed by `/sbin/service snmpd stop` from the root account. Disabling SNMP on the Control Station prevents external SNMP management platforms from communicating with the Control Station, including by means of auto-discovery. If you do not use an enterprise management software, you can disable SNMP on the Control Station.
199	TCP	Closed	SMUX	This port is related to the SNMP service.
427	TCP UDP	Open	SLP	Allows hosts (or other resources) to discover available services provided by a storage system.
443	TCP	Open	HTTPS	This is the standard HTTPS port and is used by both Unisphere and Celerra Monitor for HTTP-based management traffic to the Control Station. When used by Unisphere, an administrator must log in before they are granted access to the system. They are authenticated against the local Control Station administrative user accounts. Celerra Monitor has its own authentication protocol but uses the same set of local administrative user accounts.
631	TCP UDP	Closed	CUPS IPP	(Applicable only to systems running VNX OE for file earlier than version 8.x.) This port is related to the Common Unix Printing System (CUPS) or Internet Printing Protocol (IPP).
843	TCP	Open	FLEX/Flash	This port is associated with the crossdomain.xml policy file.

Table 6 VNX for file Control Station network ports (continued)

Port	Protocol	Default State	Service	Comments
5988	TCP	Open	SMI-S	By default, the EMC CIM server listens on ports 5988 (for http) and 5989 (for https). If these ports are in use by some other process, the CIM server will not start. *SMI-S Provider Programmer's Guide for VNX* provides more information about configuring this service.
5989	TCP	Open	SMI-S	See information in above row for details.
6389	TCP	Open	Naviagent	This port can be placed behind a firewall.
8000	TCP	Open	HTTP	This port can be used by Celerra Monitor if HTTPS is not desired for some reason. It is also used for replication commands that go between Control Stations. Celerra Monitor follows a protocol that requires all incoming traffic to be authenticated and to carry a valid session token. The Control Station to Control Station replication traffic requires that an explicit trust relationship between the Control Stations be established beforehand. Then, each HTTP request is cryptographically signed by the sending Control Station before being sent to the receiving Control Station. Without a valid signature, the HTTP requests will not be accepted. It is recommended that this port remain enabled.
8712	TCP	Open	NBS	This port is used by the NBS service for access to the Control Station file system on VNX for file. It is restricted to the private network between the Control Station and Data Mover.
9823	TCP	Open	nas_mcd	This port is used for the two nas_mcd processes to communicate with each other. It is used in two instances: • A standby CS asks the primary CS to post events for using port 9823 over the internal network. • In a VNX for file EMC SRDF® and EMC MirrorView™ configuration, the R1 and R2 Control Stations communicate over the IP network by using port 9823. The Master Control Daemon (MCD) functions as a monitor over the system, similar to a UNIX init process, but with a NAS focus and NAS-specific functionality.

Table 6 VNX for file Control Station network ports (continued)

Port	Protocol	Default State	Service	Comments
				While the port is strictly for communication between nas_mcd processes and provides a very limited interface, no additional authentication is performed (as with standard ancillary network services).
9824	TCP	Open	Common Cache	This service must bind to multiple internal network interfaces and as a consequence, it binds to the external interface as well. However, incoming requests over the external network are rejected. If desired, iptables can be used to block external access to this port.
9825	TCP	Open	Indication Manager	This service must bind to multiple internal network interfaces and as a consequence, it binds to the external interface as well. However, incoming requests over the external network are rejected. If desired, iptables can be used to block external access to this port.
9826	TCP	Open	Indication Manager	This service must bind to multiple internal network interfaces and as a consequence, it binds to the external interface as well. However, incoming requests over the external network are rejected. If desired, iptables can be used to block external access to this port.
* See Comments.	TCP UDP	Open	statd, lockd	* Native Linux NFS Remote Procedure Call (RPC) services, such as the **lockd** daemon that works with **statd**, running on the Control Station use dynamic ports. These dyanmic ports can be closed by running the command: `/sbin/service nfslock stop` followed by `/sbin/chkconfig --levels 2345 nfslock off` **Note:** Running these commands may prevent NFS from functioning properly.

VNX for file outgoing network connections

Primarily a server, VNX for file also functions as a network client in several circumstances, for example, in communicating with a directory server such as Microsoft Active Directory or an LDAP server. In these instances, VNX for file initiates communication and the network infrastructure will need to support these connections. Network connections that may be initiated by the Data Mover describes the ports that a Data Mover must be allowed to access for the corresponding service to function properly. Network connections that may be initiated by the Control Station describes the

ports that a Control Station must be allowed to access for the corresponding service to function properly.

Ports the Data Mover may contact

Table 7 Network connections that may be initiated by the Data Mover

Protocol	Port	Purpose	To what host(s)
TCP/UDP	53	DNS	All Windows 2000 and later Domain Controllers/DNS Servers
TCP	80	FileMover	Outgoing HTTP connections for FileMover
TCP/UDP	88	Kerberos Ticket	All Kerberos KDCs (Key Distribution Centers). This applies to Windows 2000 and later Domain Controllers as well as to UNIX and Linux KDCs.
TCP/UDP	111	Multiple purposes: • Portmapper • The Data Mover may contact this port as part of NFSv4 authentication	All NFS clients, VC Servers, and NIS servers
TCP/UDP	137	Multiple purposes: • WNS • The Data Mover may contact this port as part of NFSv4 authentication	All WINS servers
UDP	138	Multiple purposes: • NETBIOS Datagram Service • The Data Mover may contact this port as part of NFSv4 authentication	All CIFS clients (used for notifications and popups)
TCP	139	Multiple purposes:	All Windows NT Domain Controllers

Table 7 Network connections that may be initiated by the Data Mover (continued)

Protocol	Port	Purpose	To what host(s)
		• CIFS (on Domain Controllers) • The Data Mover may contact this port as part of NFSv4 authentication	
UDP	161	SNMP	All hosts to which the Data Mover will send SNMP traps
TCP/UDP	389	Multiple purposes: • LDAP • The Data Mover may contact this port as part of NFSv4 authentication	All Windows 2000 and later Domain Controllers or other LDAP Servers
TCP	443	FileMover	Outgoing HTTPS connections for FileMover
TCP	445	Multiple purposes: • CIFS (on Domain Controller) • The Data Mover may contact this port as part of NFSv4 authentication	All Windows Domain Controllers
TCP/UDP	464	Multiple purposes: • Kerberos Password • The Data Mover may contact this port as part of NFSv4 authentication	All Windows 2000 and later Domain Controllers or other KPASSWD servers
TCP/UDP	625	(Applicable only to systems running VNX OE for file earlier than version 8.x.) FMP	Windows MPFS clients
TCP/UDP	636	LDAPS	LDAP over SSL
TCP/UDP	6907	(Applicable only to systems running VNX	Unix MPFS clients

Table 7 Network connections that may be initiated by the Data Mover (continued)

Protocol	Port	Purpose	To what host(s)
		OE for file earlier than version 8.x.) FMP	
UDP	3268	LDAP	Queries to the Windows 2000 and later General Catalog
TCP/UDP	Dynamic	lOCKD	All NFS clients
TCP/UDP	Dynamic	Statd	All NFS clients
TCP/UDP	Dynamic	NIS	NIS servers

Ports the Control Station may contact

Table 8 Network connections that may be initiated by the Control Station

Protocol	Port	Purpose	To what host(s)
TCP	21	ConnectHome	Configured ConnectEMC FTP server
TCP	25	Notifications	SMTP server (if configured) for ConnectEMC or alerts
TCP/UDP	53	DNS	DNS server (if configured)
TCP	80	Multiple purposes: • Navisphere • Connect to VNX for block storage domain master using HTTP	• VNX for block management console • The designated storage domain master
TCP/UDP	123	NTP	NTP server (if configured)
UDP	162	SNMP trap	VNX for Block management console
TCP/UDP	389	LDAP	All Windows 2000 and later Domain Controllers or other LDAP Servers
TCP	443	Multiple purposes: • Navisphere • Connect to VNX for block storage	• Control Station to Control Station communication for some

Table 8 Network connections that may be initiated by the Control Station (continued)

Protocol	Port	Purpose	To what host(s)
		domain master using HTTP	replication related traffic • The designated storage domain master
TCP/UDP	636	LDAPS	All Windows 2000 and later Domain Controllers or other LDAP Servers that use SSL
TCP	2162	Connect to VNX for block storage domain master by using HTTP (optional, only required if domain is configured to use this port instead of port 80)	The designated storage domain master
TCP	2163	Connect to VNX for block storage domain master by using HTTPS (optional, only required if domain is configured to use this port instead of port 443)	The designated storage domain master
TCP	8000	Multiple purposes: • Navisphere • Connect to VNX for block storage domain master using HTTP	• Control Station to Control Station communication for some replication related traffic • The designated storage domain master
TCP	9998	Connect to VNX for block storage domain master by using HTTP (optional, only required if domain is configured to use this port instead of port 80)	The designated storage domain master
TCP	9999	Connect to VNX for block storage domain master by using	The designated storage master

Table 8 Network connections that may be initiated by the Control Station (continued)

Protocol	Port	Purpose	To what host(s)
		HTTPS (optional, only required if domain is configured to use this port instead of port 443)	

Network encryption

The storage management server provides 256-bit (128-bit is also supported) symmetric encryption of all data passed between it and the client components that communicate with it, as listed in Ports used by Unisphere components on VNX for block (Web browser, Secure CLI), as well as all data passed between storage management servers. The encryption is provided using SSL/TLS and uses the RSA encryption algorithm, which provides the same level of cryptographic strength as is employed in e-commerce. Encryption protects the transferred data from prying eyes-whether on the local LANs behind the corporate firewalls, or if the storage systems are being remotely managed over the Internet.

The storage management server supports SSL/TLS over the industry-standard port 443 to ease integration with firewall rule sets. For those customers who would like to use another port, instead of the industry standard, the storage management server also supports SSL/TLS over port 2163 (VNX for block only). Port selection is performed when the storage-system network settings are configured. EMC recommends that all storage management server installations in the same domain use the same port for SSL/TLS communications.

Note: Unisphere is a Java-based applet that runs inside a Web browser. Once the applet is downloaded, the applet (not the browser) communicates using SSL/TLS. The URL for the browser will not change.

VNX for file supports Secure Socket Layer (SSL) for Data Mover Hypertext Transfer Protocol (HTTP) and Lightweight Directory Access Protocol (LDAP) connections.

Instances of the storage management server installed on Windows hosts use the same communication security mechanisms as those that run on the SP; however, since the application is running on a host, additional security measures are taken to protect Unisphere domain configuration and security information. First, ACLs are set so that only administrator-level accounts can access the install directory. Second, the files are encrypted.

SSL configuration on VNX unified/file systems

SSL configuration on VNX for unified/file systems is contained in the /nas/httpd/conf/httpd.conf directory and controls SSL communications when the network area storage (NAS) service is up. EMC recommends using the existing SSL configuration; however, if it is necessary to make changes to the SSL configuration on your VNX for unified/file system, you must be root and you must modify /nas/httpd/conf/httpd.conf.

Note: Changes that are made to httpd.conf will be lost when an upgrade is performed. If you intend to use the previous changes to /nas/httpd/conf/httpd.conf, make note of the changes you made. You must reenter the previous changes to /nas/httpd/conf/httpd.conf after the upgrade has completed.

Using HTTPS

Currently, the VNX for file FileMover feature uses HTTPS and SSL's encryption and authentication features. *Using VNX FileMover* describes how to configure SSL with HTTP for use by FileMover. The keys and certificates used with SSL are managed by using PKI. PKI is available through Unisphere and the CLI. Planning considerations for Public Key Infrastructure on VNX for file provides an overview of the PKI feature.

Using SSL with LDAP

Currently, the VNX for file naming service support for OpenLDAP, iPlanet, and Active Directory uses LDAP and SSL's encryption and authentication features. *Configuring VNX Naming Services* describes how to configure SSL with LDAP for use by the OpenLDAP and iPlanet LDAP-based directory servers. The keys and certificates used with SSL are managed through PKI. PKI is available through the VNX for file CLI and Unisphere. Planning considerations for Public Key Infrastructure on VNX for file provides an overview of the PKI feature.

Management support for TLS communications on VNX2 systems

The Management communication into and out of the storage system is encrypted using SSL. As part of this process, the client and the storage system negotiate an SSL protocol to use. By default, the storage system supports TLS 1.0, TLS 1.1 and TLS 1.2 protocols for communication. The storage system includes an administrative setting to change the TLS mode from the system.

Setting the TLS mode as TLSv1.0 means that the storage system will support communication using the TLS 1.0, TLS 1.1 and TLS 1.2 protocols.

Setting the TLS mode as TLSv1.1 means that the storage system will only support communication using the TLS 1.1 and TLS 1.2 protocols, and TLS 1.0 will not be considered a valid protocol.

Setting the TLS mode as TLSv1.2 means that the storage system will only support communication using the TLS 1.2 protocol, while TLS 1.0 and TLS 1.1 will not be considered valid protocols.

Note: Changing the TLS mode to a higher level (from TLSv1.0 to TLSv1.1 or from TLSv1.0 to TLSv1.2) may impact existing client applications which are not compatible with TLS 1.1 or TLS 1.2 protocols. In this case, TLS 1.0 support should remain enabled. TLS mode should not be changed to a higher level. The following functionality will not work in TLSv1.1 and TLSv1.2 mode:

- Replication from/to VNX2 (versions *05.33.009.5.256/8.1.21.256*)
- Domain management containing a VNX/VNX2 Control Station (version *8.1.21.256* and earlier)
- Navisphere CLI (version *7.33.x.x.x* and earlier) cannot connect to Management Server. Replication Manager, RPA, ViPR SRM, AppSync, and ESA integrated with Navisphere CLI (version *7.33.x.x.x* and earlier) also cannot connect to Management Server.

If TLS 1.0 is disabled in the network environment (for example, block TLS 1.0 packets by switch), the following functions will be impacted:

- Unisphere Service Manager cannot receive software, drive firmware, and language pack upgrade notifications
- ESRS IP Client
- ESRS Device Client on Control Station and Storage Processors

Managing TLS mode on the storage system

On a Unified VNX2 or a Gateway VNX2, run the following command on Control Station with root user to manage TLS mode:

`/nas/bin/nas_tls -set TLSv1.0` Sets TLS protocol 1.0 as the lowest supported version.

`/nas/bin/nas_tls -set TLSv1.1` Sets TLS protocol 1.1 as the lowest supported version.

`/nas/bin/nas_tls -set TLSv1.2` Sets TLS protocol 1.2 as the lowest supported version.

`/nas/bin/nas_tls -info` Lists the current TLS protocol settings.

On a Block-only VNX2, run the following naviseccli command with Administrator or Security Administrator roles:

`naviseccli -h <sp_ip> security -tls -set TLSv1.0` Sets TLS protocol 1.0 as the lowest supported version.

`naviseccli -h <sp_ip> security -tls -set TLSv1.1` Sets TLS protocol 1.1 as the lowest supported version.

`naviseccli -h <sp_ip> security -tls -set TLSv1.2` Sets TLS protocol 1.2 as the lowest supported version.

`naviseccli -h <sp_ip> security -tls -get` Lists the current TLS protocol settings.

For more information about these commands, please refer to *VNX Command Line Interface Reference for File* and *VNX Command Line Interface Reference for Block.*

SSL certificates

Any time a client connects to a server over a network, it is important that the client can verify the identity of the server. Otherwise, any node on the network can impersonate the server and potentially extract information from the client. This is known as a man-in-the-middle attack.

Unisphere uses public key cryptography to verify the identity of the storage management server. Each VNX SP and Control Station contains a PKI certificate with a corresponding public key that the storage management server presents to a client. The certificates will be self-signed by default, but users have the ability to import certificates that have been signed by a trusted third party. If the client has the root certificate for that trusted third party (web browsers have certificates from common certificate authorities pre-installed) then it can inherently trust the server. This is the same mechanism by which your web browser inherently trusts most secure web sites.

Note: VNX systems inherently support SHA-1 certificates. For SHA-2 support, you must import your own SHA-2 certificates.

Certificates should contain 2048-bit RSA encrypted keys but keys containing as low as 1024 bits are allowed to be imported. For VNX for block, the interface for managing user certificates is found at:

`https://<SP_IP_address>/setup`, which requires username and password authentication, or with the `naviseccli security -pkcs12upload` switch.

Note: For more information about the interface for managing user certificates for VNX for block, see VNX for block SSL certificate import on page 137. For more information about the naviseccli commands, see the *VNX Series Command Line Interface Reference for Block*, located on mydocs.emc.com.

Unisphere not only verifies the certificate of the storage system it is connected to, it also verifies certificates for all the VNX systems in the domain. Other client software like Unisphere Service Manager (USM), CLI, and Unisphere Server Utility will perform certificate verification when connecting to the storage system. The management server that is running on the storage system will also verify certificates when connecting to external servers like LDAP and ESX/Virtual Center.

How it works

When a client (such as Unisphere, CLI, or USM) connects to a server (such as the Storage management server or LDAP) for the first time, it is presented with a certificate from the server. The user can check the details of the certificate and decide to accept the certificate or reject it. If the user rejects the certificate, the communication with the server is stopped. If the user decides to accept the certificate, the communication continues and the certificate is stored in a certificate store. The next time when the client communicates with that server, the server's certificate is verified with the certificate in the certificate store. The user is prompted the first time it communicates with a server. Once the certificate is stored, the certificate verification process will happen in the background.

The following options are presented to the user when connecting to a server for the first time:

- Accept for session - Accepts the certificate to manage the system for this session only. The user will be prompted again in future sessions to accept the certificate.
- Accept Always - By selecting this option, the certificate is stored in the certificate store on the client; for subsequent communications the certificate is verified as a background task. The user will not be prompted again.
- Reject - If the user does not trust the certificate, the user can opt to reject the certificate and the communication will be stopped.

Unisphere and USM use the Java certificate store for storing certificates. The certificates store can be managed using the Java control panel. Block CLI and Unisphere Server Utility create a certificate store on the user directory of the client. Unisphere, USM, and Unisphere Server Utility will enforce certificate verification when connecting to the storage system.

The storage management server also performs certificate verification when communicating with LDAP and the ESX/Virtual Center server. The certificates are stored on the storage system and appear in **Trusted Certificates for LDAP and VMware Servers** (in Unisphere use **Settings** > **Security** > **Server Certificates for Block**).

Connecting to the directory server using SSL

To protect LDAP traffic and improve client and server application security, the LDAP-based directory server can support and, in some cases, require the use of SSL. SSL provides encryption and authentication capabilities. It encrypts data over the network and provides message and server authentication. It also supports client authentication if required by the server. SSL uses digital certificates, whose authenticity is verified by a CA.

The LDAP client, using the underlying SSL client, authenticates the certificate received from the LDAP-based directory server. The CA certificate (for the CA that signed the directory server's certificate) must have been imported into the Control Station for the certificate verification to succeed, otherwise the certificate verification fails.

Note: The Control Station LDAP-based client implementation does not support mutual SSL client authentication.

Planning considerations for Public Key Infrastructure on VNX for file

The VNX for file Public Key Infrastructure (PKI) provides the software management and database systems to support the use of digital certificates for Data Mover LDAP and HTTP connections on which SSL is enabled. Certificates, whose authenticity is verified by a Certificate Authority (CA), are used by SSL to identify one or both ends of a connection, providing stronger security between clients and servers.

Note: The VNX for file PKI framework supports the X.509 certificate standard. Certificates are encoded using Distinguished Encoding Rules (DER) and may be further encoded in Privacy Enhanced Mail (PEM) format for ease of distribution through email systems.

Personas

Personas are used to provide an identity for a Data Mover when it is acting as a server or a client. When negotiating a secure connection with a client (such as the external policy and migration software used with FileMover), the persona provides a private key and certificate to the Data Mover (which is acting as a server). This certificate provides the means by which the client can identify and authenticate the server. When negotiating a secure connection with a server that is configured to require client authentication, the persona provides the private key and certificate to the Data Mover (which is acting as a client). The certificate provides the means by which the server can identify and authenticate the client.

By default, each Data Mover is configured with a single persona named default. To create the certificate that the persona provides to the Data Mover, you first generate the persona's public/private key set. You must then request a signed certificate from a CA. Certificate requests are generated in Privacy Enhanced Mail (PEM) format only.

Note: Currently, each Data Mover is allowed only one persona. VNX for file does not support a mechanism to create additional personas.

If you are using the Control Station as the CA, the Control Station automatically receives the certificate request, generates and signs the certificate, and returns the certificate to the Data Mover. The Control Station can sign certificates for all the Data Movers in the cabinet. It cannot be used to sign certificates for any external hosts.

If you are using an external CA, you must send the certificate request manually. The request to sign the public key is generated with the public/private key set. Display the persona's properties to verify its content. Obtain a copy of the certificate request and then send the request to the CA through that company's website or email.

When the CA returns a signed certificate, you must import it to the Data Mover. To import the signed certificate, you can either provide a path and import a file, or cut and paste the associated text. A file can be in either Distinguished Encoding Rules (DER) or PEM format. You can cut and paste text only in PEM format.

Each persona can be associated with up to two sets of keys and certificates (current and next), to allow generating new keys and certificates before the expiration of the current certificate. When the next certificate (which is already valid) is imported, it and its associated key set immediately become the current key set and certificate.

Because the next certificate is typically generated when it is needed, you typically do not see a next certificate associated with a persona. However, a next certificate may be waiting if there is a time difference between the Data Mover and the CA (or the Control Station if it is serving as the CA). For example, a CA might prepare a certificate in advance by assigning it a future start date. Merging companies could set up such a certificate to have it in place for the official merge date.

The next certificate becomes the current certificate (and the current key and certificate are deleted) when the certificate becomes valid (per Data Mover time), and one of the following happens:

- The persona is queried (by either the CLI or Unisphere).
- The persona's key and certificate are requested by a Data Mover function (such as SSL).

After a certificate expires, any attempt to use the certificate results in a failure, typically a loss of connection or a failure to reconnect. When a new certificate is available, PKI deletes the old certificate and provides the new certificate when requested. However, if you did not obtain a new certificate before the current certificate expires, the certificate request will fail. PKI will not provide an expired certificate for a persona.

There is no automated way to check for expired public key certificates. You must check for expired certificates manually by listing the personas and examining the expiration dates of the associated certificates. You can then take action based on your organization's business practices.

Certificate Authority (CA) certificates

When a VNX for file based client application requires a network connection with a server (such as FileMover's connection with its secondary storage), the server provides a certificate as part of the negotiation for a secure connection. The client application confirms the server's identity by validating the certificate. It does this by verifying the server certificate's signature with the public key from the CA certificate.

Obtaining the required CA certificates is a manual task. Typically, before actual operation, you must identify the appropriate CA. Then you must check the list of CA certificates that are available. If a new CA certificate is required and an external CA is being used, you can obtain the CA certificate from the company's website or from the person responsible for security. If the CA is local (enterprise-level or inhouse), obtain the CA certificate from the person who manages the CA.

To make the CA certificate known to system, you must import it. You can provide a path and import a file, or cut and paste the text. A file can be in either DER or PEM format. You can cut and paste text only in PEM format.

Using the Control Station as the CA

The system software automatically generates a key set and certificate for the Control Station when the system is installed or upgraded. The Control Station uses this key set and certificate to sign certificate requests from Data Movers. However, before the Control Station can successfully operate as a CA and be recognized by a Data Mover as such, you must complete several configuration tasks:

- Distribute the Control Station CA certificate to network clients. In order for a network client to validate a certificate sent by a Data Mover that has been signed by the Control Station, the client needs the public key from the CA certificate to verify the Data Mover certificate's signature.
- Import the CA certificate (with the CA certificates from external CAs).

A copy of the Control Station certificate can be obtained only by using the CLI. If the Control Station key set and certificate are compromised, you can regenerate them. This task can be accomplished only through a CLI command. After regenerating the Control Station key set and certificate, you have to regenerate a new key set and certificate request, and then import the signed certificate for any personas whose certificates are signed by the Control Station.

Note: The Control Station continues to generate a separate key set for the SSL-based connection between the Apache web server (on behalf of Unisphere) and a user's web browser. However, the Control Station now uses the CA key set to sign the Apache web server's certificate, meaning the certificate is no longer self-signed. *Installing Management Applications on VNX for File* describes how to manage certificates for Unisphere.

Customer-Supplied Certificates for Control Station

To satisfy more stringent requirements, VNX users are allowed to install and configure their own X.509 certificate on the Control Station for HTTPS communication.

The form and content of customer-supplied X.509 certificates are up to the users. The certificate should be PEM-encoded and should not have an associated password. Otherwise, the Apache web server will not be able to start unattended which will interfere with failover and restart operations.

Note: See Request and Install Customer-Supplied Certificates for Control Station on page 127 for an example of how to request and install a customer-supplied certificate.

The customer-supplied private key should be copied to the directory `/nas/http/conf/ssl.key` and the certificate should be copied to `/nas/http/conf/ssl.crt` to avoid potential data loss after failover. When the new private key and certificate are in place, make sure the current key and certificate in the directory `/nas/http/conf` are updated to point to the newly installed private key and certificate, respectively.

Note: The private key must be owned by user root and have permissions set to 600 (-rw-------). The public certificate also needs to be owned by user root, but have permissions set to 644 (-rw-r--r--).

You must restart Apache after renewing the certificate and the private key to take the changes into effect. Refer to the last step in the Request and Install Customer-Supplied Certificates for Control Station on page 127 example for instructions.

Note: You can verify the new server certificate by viewing the characteristics of the HTTPS connection after pointing the supported web browser to the Control Station.

IP packet reflect on VNX for file systems

IP packet reflect provides your network with an additional security level. Because the majority of network traffic on a Data Mover (including all file system I/O) is client-initiated, the Data Mover uses Packet Reflect to reply to client requests. With Packet Reflect, there is no need to determine the route to send the reply packets. Because reply packets always go out the same interface as the request packets, request packets cannot be used to indirectly flood other LANs. In cases where two network devices exist, one connected to the Internet and the other connected to the intranet, replies to Internet requests do not appear on the intranet. Also, the internal networks used by VNX for file are not affected by any packet from external networks.

Configuring and Managing Networking on VNX describes how to configure this feature.

Effect of filtering management network

VNX systems can limit management requests to only trusted IP addresses. The goal of the filter is to target only the relevant components and therefore have a minimal effect on the rest of the environment. IP filtering is designed to limit management of a storage system or domain of storage systems to management hosts with a specific set of IP addresses. It is not a firewall and does not cover all access points to the storage system.

IP filtering restricts access to:

- The Unisphere management port (UI, CLI)
- The Unisphere setup page
- The Unisphere initialization tool
- High availability validation tool (HAVT) reports
- RemotelyAnywhere

IP filtering does not restrict access to:

- iSCSI ports
- Unisphere service and serial ports
- Unisphere communication with the peer SP
- Unisphere Agent (port 6389) requests

vSphere Storage API for Storage Awareness (VASA) support

VASA is a VMware-defined, vendor-neutral API for storage awareness. It is a proprietary SOAP-based web interface and is consumed by VMware clients rather than Unisphere clients. VASA is a reporting interface only and is used to request basic information about the VNX and the storage devices it exposes to the virtual environment in order to facilitate day-to-day provisioning, monitoring, and troubleshooting through vSphere.

For Unisphere, the VASA Provider (VP) component is embedded on the VNX, on both the Control Station (for VNX for file/unified) and the Storage Processors (for VNX for block). You as the vSphere user must configure these VP instances as the provider of VASA information for each storage system.

Note: When you set up a connection to the VNX for block VP, you should target only one SP. Either SP A or SP B will return the same information to VASA. In the event that an SP goes down, the client will lose its connection to the VP (that is, no automatic failover will occur). The client can either wait for the failed SP to come back up, or it can try establishing a new connection to the peer SP. You are not prevented from targeting both SPs, but the information that is returned would be redundant and could result in duplicate events and alarms depending on VMware's client implementation.

In order to initiate a connection from vCenter to the Unisphere VP, you must use the vSphere client to enter three key pieces of information:

- the URL of the VP
- the username of a Unisphere user with the administrator, securityadmin or vmadmin role (local, global, or LDAP scope)
- the password associated with this user

The Unisphere credentials used here are only used during this initial step of the connection. If the Unisphere credentials are valid for the target VNX, the vCenter Server's certificate is automatically registered with the VNX. It is this certificate that is used to authenticate all subsequent requests from vCenter. No manual steps are required to install or upload this certificate to the VP.

vCenter Session, Secure Connection and Credentials

A vCenter session begins when a vSphere administrator uses the vSphere Client to supply the vCenter Server with the VASA VP URL and login credentials. The vCenter Server uses the URL, credentials, and the VASA VP's SSL certificate to establish a secure connection with the VP. A vCenter session ends when an administrator uses the vSphere Client to remove the VP from the vCenter configuration and the vCenter Server terminates the connection.

A vCenter session is based on secure HTTPS communication between a vCenter Server and a VP. The VASA architecture uses SSL certificates and VASA session identifiers to support secure connections. Both the vCenter Server and the VP adds the other's certificate to its own trust store.

Special configurations

Unisphere provides strong security for managing VNX storage systems anywhere and anytime. But there are still some network configurations, such as proxy servers and network address translation (NAT), that need to be identified and dealt with.

Proxy servers

Unisphere does not support proxy servers. Browsers must be configured not to use a proxy server to access the IP addresses of Management Servers.

Unisphere Service Taskbar supports accessing the Internet through a proxy server. This is important so that the tool can access the EMC Powerlink website to obtain the latest software for VNX for block Operating Environment (OE) upgrades.

Unisphere client/server and NAT

Network address translation (NAT) rewrites IP packet source and/or destination addresses as the packet passes through a router. The main use of NAT is to mask internal hosts from an external network. This may be for security purposes or to allow many internal hosts to have class C IP addresses and masquerade under a single external IP address. NAT can be troublesome for many communication protocols, including those that the Unisphere tools use.

Unisphere Client/Server supports managing a single storage system through a NAT gateway. Only that one storage system will be visible. Domains are not supported as that would require the user to enter the NAT address for every node in the domain.

NAT connections are not supported when Unisphere is launched directly from the storage system or with other tools such as CLI and Unisphere Service Manager.

Other security considerations

Potential cyber security threats are announced almost daily by IT product vendors and security-monitoring agencies. EMC is committed to providing customers with a timely response to each vulnerability. Responses include any potential impact on EMC products and any corrective or preventative measures. Knowledgebase articles for each EMC response are available on the EMC Online Support website at http://Support.EMC.com. For your convenience, a comprehensive list of published vulnerabilities and EMC responses called the Security Alerts Master List (kb article 83326) is also available on the EMC Online Support website.

CHAPTER 5

Data Security Settings

Note: The information presented in this chapter is pertinent only to VNX systems running VNX operating environment (OE) for block versions 5.33 and later.

Data security settings enable definition of controls to prevent data permanently stored by the product to be disclosed in an unauthorized manner.

Topics include:

Data at Rest Encryption overview

Data at Rest Encryption (D@RE) is provided through controller-based encryption (CBE) at a physical disk drive level. A unique data encryption key (DEK) is generated for each drive and is used to encrypt data as it is sent to the drive. The goal of this feature is to ensure that all customer data and identifying information will be encrypted with strong encryption, primarily to ensure security in the event of loss of a disk drive.

Note: Some unencrypted data could be in the system partition (for example, hostnames, IP addresses, dumps, and so on). In addition, there is potential for small amounts of unencrypted user data as a result of writing diagnostic materials to the system partition. All the data written to the array by using regular I/O protocols (iSCSI, FC) are encrypted. Anything that comes into the array by using the control path will not be encrypted by this solution; however, information that is sensitive (for example, passwords) are encrypted by a different mechanism (as they are on non-encrypting arrays).

For new VNX systems that are ordered with the D@RE feature, encryption should be enabled on the systems during manufacturing. Verify whether D@RE has been enabled and activated. To view the status of the D@RE feature in Unisphere, select **System** and, from the task list under **System Management**, select **System Properties**. The status of the encryption appears on the **Encryption** tab in the **Storage System Properties** view. If **Encryption Mode** appears as **N/A**, you need to perform a non-disruptive upgrade (NDU) of the DataAtRestEncryption enabler and activate it. If **Encryption Mode** appears as **Unencrypted**, you only need to activate it using either Unisphere or the VNX for block CLI.

NOTICE Once activated, the encryption operation cannot be reverted. When possible, enable encryption prior to populating the system with data, RAID groups, and such. This action will avoid the data in place upgrade process and its effects on system cache and system performance.

For VNX systems that do not have D@RE enabled, enabling of encryption on the system requires a non-disruptive upgrade (NDU) of the DataAtRestEncryption enabler. This upgrade can be done upon request. A subsequent activate operation must be initiated through either Unisphere or the VNX for block CLI.

A new component, referred to as the VNX Key Management Server, is responsible for generating, storing and otherwise managing the encryption keys for the system. The keystore that is generated to store the encryption keys resides on a managed LUN in private space on the system. Keys are generated or deleted in response to notifications that a RAID group/disk drive have been respectively added or removed.

Changes to the configuration of the system that result in changes to the keystore will generate alerts that recommend key backups be created. When an operation that results in a change to the keystore occurs, an alert will appear and persist until the keystore has been retrieved from the system for backup. Backup the keystore by using either the Unisphere UI or a VNX for block CLI command.

In the event that the keystore becomes corrupted, the system will be nonfunctional. The system will enter a degraded state, only the operating system boots. In this state, attempts to access the system through Unisphere will return an error indicating that the keystore is in an inaccessible state. In this case, a service engagement is required for resolution.

A separate auditing function is provided for general key operations that track all key establishment, deletion, backup, and restore changes as well as SLIC addition.

For additional information about the Data at Rest Encryption feature, refer to the *EMC VNX2: Data at Rest Encryption* white paper.

Data at Rest Encryption feature activation

A user role of administrator, storageadmin, or sanadmin is required to activate the Data at Rest Encryption (D@RE) feature. Before activating this encryption feature, ensure that FAST Cache is destroyed on your system. Attempts to activate the D@RE feature on a system with FAST Cache created will return an error. You can recreate your FAST Cache after you activate the encryption feature.

Enabling of the D@RE feature on the system requires a non-disruptive upgrade (NDU) of the DataAtRestEncryption enabler. A subsequent activate operation must be initiated through Unisphere to activate this feature. As an alternative, you can use the VNX for block CLI command, `securedata -feature -activate`, to activate this feature. See the *VNX Series Command Line Interface Reference for Block* for detailed information about the `securedata` command.

NOTICE Once activated, the encryption operation cannot be reverted. This action will cause data encryption keys to be created and all user data will begin to be encrypted. EMC recommends that you have an up-to-date and verified backup of your array as well as an up-to-date configuration capture, created using either Unisphere or the `arrayconfig` VNX for block CLI command, before you execute the activate operation.

To activate the D@RE feature in Unisphere, select **System** and, from the task list under **Wizards**, select **Data At Rest Encryption Activation Wizard**. The activation wizard that appears directs you through the steps to activate encryption and to backup the generated keystore file to an external location. The keystore file that is generated to store the encryption keys resides on a managed LUN in private space on the system.

NOTICE EMC strongly recommends that you backup the generated keystore file to another location which is external to the system where the keystore can be kept safe and secret. In the event that the keystore on the system becomes corrupted, the system will be nonfunctional. The system will enter a degraded state, only the operating system boots. In this state attempts to access the system through Unisphere will return an error indicating that the keystore is in an inaccessible state. In this case the backup keystore file and a service engagement are required for resolution.

NOTICE For VNX systems that do not have D@RE enabled or were received from EMC without D@RE activated, the Storage Processors must be rebooted once the D@RE activation process has successfully started. You must manually reboot each Storage Processor (refer to either Rebooting Storage Processors through Unisphere or Rebooting Storage Processors through VNX OE for Block CLI). This action will finalize the installation and activation process.

Rebooting Storage Processors through Unisphere

Before you begin

Verify the D@RE activation process has successfully started and encryption is either In Process, Encrypted or Scrubbing. See Encryption status.

About this task

If your VNX system does not have D@RE enabled or was received from EMC without D@RE activated, the Storage Processors must be rebooted once the D@RE activation process has successfully started. It does not matter in which order the Storage Processors are rebooted (for example, SP A then SP B or SP B then SP A). It is critical, however, that you reboot the Storage Processors one at a time and you verify that the first SP is operational before rebooting the second SP.

Procedure

1. Open EMC Unisphere using your Storage Processor's IP address in a supported browser.
2. Click on the array and select **System Storage Hardware**.
3. Expand the tab for SPs.
4. Right-click the SP that you want to reboot (for example, SP A).
5. Select **Reboot**.
6. Select **Yes** at the confirmation window.
7. Prior to rebooting the second Storage Processor, you must first verify that you can log into Unisphere and manage the array.
8. Repeat steps 4, 5, and 6 for the other SP.

Rebooting Storage Processors through VNX OE for Block CLI

Before you begin

Verify the D@RE activation process has successfully started and encryption is either In Process, Encrypted or Scrubbing. See Encryption status.

About this task

If your VNX system does not have D@RE enabled or was received from EMC without D@RE activated, the Storage Processors must be rebooted once the D@RE activation process has successfully started. It does not matter in which order the Storage Processors are rebooted (for example, SP A then SP B or SP B then SP A). It is critical, however, that you reboot the Storage Processors one at a time and verify that the first SP is operational before you reboot the second SP.

Procedure

1. Reboot a Storage Processor using the command: `naviseccli -h <IP_address_of SP> -user <name> -password <password> -scope <scope> rebootSP`.

   This command reboots the SP to which the IP_address refers.
2. Prior to rebooting the second Storage Processor, you must first verify that you can log into Unisphere and manage the array.
3. Repeat the first step for the other SP.

Encryption status

The following D@RE feature status can be viewed either through Unisphere or a VNX for block CLI command:

- Encryption Mode: type of encryption in use; for example, Controller-Based Encryption
- Encryption Status: based on the actual encryption status:
  - Not started
  - In Process
  - Encrypted
  - Scrubbing
- Encryption Percentage: encryption percentage of the overall storage system

To view the status of the D@RE feature in Unisphere, select **System** and, from the task list under **System Management**, select **System Properties**. The status of the encryption appears on the **Encryption** tab in the **Storage System Properties** view.

Note: As an alternative, use the VNX for block CLI command `securedata -feature -info` to view the feature status. Also, use the `securedata -backupkeys -status` CLI command to view the status of the keystore and to determine whether any user operations are required. See the *VNX Series Command Line Interface Reference for Block* for detailed information about these CLI commands.

After enabling encryption on the system, you may notice that the encryption percentage remains at a certain level and does not increase. Several conditions may cause encryption to halt:

- Faulted disk
- Disk zeroing in progress
- Disk rebuild in progress
- Disk verify in progress
- Cache disabled

If this occurs, check the system logs to determine the cause. If corrective action is required, correct the condition. Encryption should complete after the correction has taken effect or the operation in progress completes.

Backup keystore file

A new component, referred to as the VNX Key Management Server, is responsible for generating, storing and otherwise managing the encryption keys for the system. The keystore that is generated to store the keys resides on a managed LUN in private space on the system. Keys are generated or deleted in response to notifications that a RAID group /disk drive have been respectively added or removed.

Changes to the configuration of the system that result in changes to the keystore generate alerts that recommend key backups be created. When an operation that results in a change to the keystore occurs, an alert appears and persists until the keystore has been retrieved from the system for backup.

NOTICE EMC strongly recommends that you backup the generated keystore file to another location which is external to the system where the keystore can be kept safe and secret. In the event that the keystore on the system is corrupted, the system will be nonfunctional. The system will enter a degraded state, only the operating system boots. In this state, attempts to access the system through Unisphere will return an error indicating that the keystore is in an inaccessible state. In this, case the backup keystore file and a service engagement are required for resolution.

A user role of administrator, storageadmin, or sanadmin is required to backup the keystore file.

To backup the keystore file to a location that is external to the system where the keystore can be kept safe and secret, select **System** and, from the task list under **Wizards**, select **Backup Keystore File**. The dialog box that appears directs you through the steps to backup the generated keystore file.

Note: As an alternative, use the VNX for block CLI command `securedata -backupkeys -retrieve` to backup the keystore file to a location that is external to the system where the keystore can be kept safe and secret. See the *VNX Series Command Line Interface Reference for Block* for detailed information about this CLI command.

Data in place upgrade

To encrypt a system with a data in place upgrade, the system must read the entire contents of the set of disk drives incrementally, then write those contents back to the drives. The keying process

will consume some percentage of the system cache. It will also consume a non trivial amount of system performance. This operation is scaled based on the I/O load of the system.

Upon activation, through either the Unisphere UI or the VNX for block `securedata -feature -activate` CLI command, the system will begin performing encryption operations. Data that is written before encryption is enabled is written in unencrypted form and will be encrypted later by the background encryption operation. This only occurs during the initial upgrade process. For any RAID group (RG) that is created after encryption is enabled, all data written to the RG will be encrypted.

When encryption is enabled, a key encryption key (KEK) will be generated as well as DEKs for all of the disk drives of the existing RAID groups. The system will begin the process of encrypting the existing data by reading the data, a stripe at a time, in unencrypted form and re-writing the data in encrypted form.

Certain conditions will delay or halt the data in place upgrade including:

- RG zeroing in progress
- RG rebuild in progress
- RG verify in progress
- Cache unavailable

The system will otherwise continue to operate normally, including encryption of already encrypted space on the drive.

NOTICE EMC strongly recommends enabling encryption prior to writing any data on the array or migrate to an array that has encryption already enabled. A sanitize operation is not performed on an HDD or SSD that is undergoing a data in place upgrade. Only the addressable space of the drive is overwritten. Any residual plaintext data that may be hidden in obscured locations within the drive will not be encrypted. This data is not readily retrievable through standard interfaces, but may be accessible through other means. If D@RE must be enabled through a data in place upgrade and if you prohibit unencrypted data, you will have to mitigate manually. For information concerning sanitization, refer to the latest version of the NIST publication, *Guidelines for Media Sanitization*, at http://csrc.nist.gov/.

Some unencrypted data could be in the system partition (for example, hostnames, IP addresses, dumps, and so on). In addition, there is potential for small amounts of unencrypted user data as a result of writing diagnostic materials to the system partition. All the data written to the array by using regular I/O protocols (iSCSI, FC) are encrypted. Anything that comes into the array by using the control path will not be encrypted by this solution. However, information that is sensitive (for example, passwords) are encrypted by a different mechanism (as they are on non-encrypting arrays).

If your security or compliance policies require sanitized drives, EMC recommends that after completing the data in place upgrade, you should migrate the encrypted data to a new or previously sanitized set of drives. One option to relocate the data is to use the MCx copy-to function, which is available through either Unisphere or the VNX for block CLI. This will move all the encrypted data from one disk drive to another drive of the same or larger capacity. After the MCx copy-to operation completes, perform your sanitization procedure on the original drive, which can then be returned to the system for reuse, if desired.

Special consideration for vault drives

If LUN or file system data exist on the vault drives (the first four drives) of the VNX after the data migration, you need to take special steps to replace those drives. Migrate the LUNs to another set of drives then insert a new, unused, compatible drive into position 0_0_0 and allow the system to fully rebuild the drive contents. This process should take less than an hour to complete. You need to repeat this procedure for each of the remaining three drives (positions 0_0_1, 0_0_2, and 0_0_3) ensuring that the rebuild is complete before proceeding to the next drive. After the drives

have been replaced, you can migrate the LUNs back to the vault drives and then perform your sanitization procedure on the original drives.

Special consideration for FAST Cache

FAST Cache must be destroyed before activating encryption. If your security policy requires special sanitize procedures, you should appropriately sanitize the FAST Cache drives after the FAST Cache is destroyed and before you re-enable it. FAST Cache can be re-enabled as soon as the encryption activation process completes.

If SSD hot spares are being used only for FAST Cache, you can sanitize those SSD hot spares immediately.

Note: If a SSD will also be used as a storage pool or RG hot spare, plaintext data may be written to it if it is for a rebuild during a data in place upgrade. If you prohibit unencrypted data, you will have to mitigate manually. For this reason, leave sanitization of these hot spares until after the data in place upgrade completes.

Hot spare operations

When a system is already configured with DEKs for all the disk drives in the system that are in RGs or storagepools, drives that are not currently in a RG or storagepool are considered unbound drives. Removal of unbound drives or unbound drives that become faulted have no affect on the keystore and therefore do not require a backup of the keystore file. Likewise, replacement of an unbound drive has no affect on the keystore and therefore does not require a backup of the keystore file.

Note: Disk drives that are not bound will be overwritten with default data to remove pre-existing data.

When a system is already configured with DEKs for all the drives in the system that are in RGs or storagepools, those drives are considered bound drives. If a bound drive is removed or the drive becomes faulted, and after a period of five minutes a permanent hot spare replaces the removed or faulted drive, a DEK is generated for the hot spare, and rebuild begins. The DEK from the removed drive will be removed immediately from the keystore. A keystore modified status will be set by the Key Manager at this point and will trigger an alert to back up the keystore because DEK modifications were made to the keystore.

If the removed disk drive is reinserted anywhere in the system before the five minute period has expired, a rebuild will not be required and modifications will not be made to the keystore. The DEK will remain the same because the key is associated with the disk drive, not the slot. Also, a keystore modified status alert will not be generated.

Note: If sanitizing or destruction of the removed drive is required, it should be done independently.

Adding a disk drive to a VNX with encryption activated

Inserting one or more new disks into the system does not trigger generation of a new DEK for each disk. This operation will not occur for a new disk until the disk is added to a RAID Group or storagepool. A keystore modified status will be set by the Key Manager at this point and will trigger an alert to back up the keystore because DEK modifications were made to the keystore.

When you add a new disk drive to a VNX, the drive is considered unbound. Disk drives that are not bound are overwritten with default data to remove pre-existing data. Only the addressable space of the drive is overwritten. Any residual plaintext data that may be hidden in obscured locations within the drive will not be overwritten.

NOTICE If the potential access to data remnants from the previous use of a drive violates your security policy, you must independently sanitize the drive before it is inserted in the VNX with encryption activated.

When you add or replace a SAS UltraFlex I/O module to a VNX with encryption activated, you must perform an additional manual reboot of the affected Storage Processor once the replacement process is completed. Use either Unisphere or the VNX OE for Block CLI command: `naviseccli -h <IP_address_of SP> -user <name> -password <password> -scope <scope> rebootSP`. This command reboots the SP to which the IP_address refers.

Removing a disk drive from a VNX with encryption enabled

When a system is already configured with DEKs for all the drives in the system that are in RGs or storagepools, those drives are considered bound drives. If a bound drive is removed and after a period of five minutes is not replaced, the DEK for the drive will not be removed from the keystore. The key will remain valid until the RG is deleted, or until a new drive is swapped in. If the removed disk drive is reinserted anywhere in the system before the five minute period has expired, a rebuild will not be required, as in the case of a replacement drive, and modifications will not be made to the keystore. The DEK will remain the same because the key is associated with the disk drive, not the slot. Also, a keystore modified status alert will not be generated. For hot spare replacement information, see Hot spare operations.

Note: If sanitizing or destruction of the removed drive is required, it should be done independently.

Replacing a chassis and SPs from a VNX with encryption enabled

The generated keystore has a relationship to the hardware in the storage system. Removing hardware improperly can cause data to become inaccessible. In situations where the chassis and both SPs need to be replaced, a special procedure is required. Do not replace both SPs simultaneously. Instead, replace one SP and wait until the storage system is back online before replacing the second SP. Alternatively, if the hardware was already replaced and a backup of the keystore is available, you can restore the keystore from the backup with the assistance of EMC Support.

CHAPTER 6

Security Maintenance

This chapter describes a variety of security maintenance features implemented on the VNX.

Topics include:

ESRS on Control Station

The ESRS on Control Station software monitors the operation of your VNX File/Unified systems for error events and automatically sends Connect Home notifications to your service provider. This software also provides a path for your service provider to use to securely connect to your specified VNX File/Unified system (through the associated control station).

This solution offers a secure architecture from end to end, including the following features:

- EMC issues X.509 digital certificates to authenticate the ESRS on Control Station to EMC.
- EMC professionals are authenticated using two unique factors.
- All EMC service professionals have a unique username that is logged with all their actions.
- All communication originates from the Control Station. The ESRS on Control Station does not accept unsolicited connections from EMC or the Internet.
- All communications between EMC and the ESRS on Control Station includes the latest security practices and encryption technologies, including certificate libraries based on RSA Lockbox technology, and Advanced Encryption Standard (AES) 256-bit encryption.
- Those who implement the ESRS on Control Station solution can further control remote access by using the Policy Manager. The Policy Manager gives full control of how EMC interacts with VNX systems. SSL is available between the ESRS on Control Station and the Policy Manager.

For more information about the ESRS on Control Station feature for VNX systems, refer to the *EMC Secure Remote Support for VNX* technical module on the EMC Online Support website at http://Support.EMC.com.

ESRS Device Client on Storage Processor

The ESRS device client on Storage Processor feature is included only in VNX operating environment (OE) for Block versions 5.32 that are later than version 05.32.000.5.209 or versions 05.33 that are later than version 05.33.000.5.051. This software monitors the operation of your VNX for Block systems for error events and automatically sends ConnectEMC notifications to your service provider. It also provides a path for your service provider to use to securely connect to your specified VNX for Block system (through the associated storage processor).

This solution offers a secure architecture from end to end, including the following features:

- EMC issues X.509 digital certificates to authenticate the ESRS device client on Storage Processor to EMC.
- EMC professionals are authenticated using two unique factors.
- All EMC service professionals have a unique username that is logged with all their actions.
- All communication originates from the Storage Processor. The ESRS device client on Storage Processor does not accept unsolicited connections from EMC or the Internet.
- All communications between EMC and the ESRS device client on Storage Processor includes the latest security practices and encryption technologies, including certificate libraries based on RSA Lockbox technology, and Advanced Encryption Standard (AES) 256-bit encryption.
- Those who implement the ESRS device client on Storage Processor solution can further control remote access by using the Policy Manager. The Policy Manager gives full control of how EMC interacts with VNX systems. SSL is available between the ESRS device client on Storage Processor and the Policy Manager.

For more information about the ESRS device client on Storage Processor feature for VNX for Block systems, refer to the *EMC Secure Remote Support for VNX* technical module on the EMC Online Support website at http://Support.EMC.com.

ESRS IP Client

The ESRS IP Client for VNX software monitors the operation of your VNX for block systems for error events and automatically notifies your service provider of error events. EMC strongly recommends the EMC Secure Remote Gateway solution for users who require customizable security options due to federal, industry, or corporate regulations. Enhanced security features such as encryption, access controls, authentication, audit, and authorization address today's stringent compliance regulations.

The ESRS IP Client for VNX software allows specified VNX for file control stations to send ConnectHome notifications to your service provider. This software also provides a path for your service provider to use to securely connect to your specified VNX for file system (through the associated control station).

This solution offers a secure architecture from end to end, including the following features:

- EMC issues X.509 digital certificates to authenticate the ESRS IP Gateway or ESRS IP Client for VNX to EMC.
- EMC professionals are authenticated using two unique factors.
- All EMC service professionals have a unique username that is logged with all their actions.
- All communication originates from the remote site. The ESRS IP Gateway or the ESRS IP Client for VNX does not accept unsolicited connections from EMC or the Internet.
- The heartbeat uses https and SOAP to ensure a firewall-friendly solution.
- All communications between EMC and the ESRS IP Gateway or ESRS IP Client for VNX includes the latest security practices and encryption technologies, including certificate libraries based on RSA Lockbox technology, and Advanced Encryption Standard (AES) 256-bit encryption.
- Those who implement the ESRS IP Gateway or ESRS IP Client for VNX solution can further control remote access by using the Policy Manager. The Policy Manager gives full control of how EMC interacts with VNX systems. SSL is available between the ESRS IP client and the policy manager.

For more information on ESRS Support for VNX systems, refer to the*EMC Secure Remote Support for VNX* technical module on the EMC Online Support website at http://Support.EMC.com.

Secure serviceability settings (block)

EMC Customer Service uses RemotelyAnywhere to gain direct access to a VNX SP through the TCP/IP management port, the TCP/IP service port, or the serial port.

You can change the username/password for the management port by going to the service port `https://<SP_IP_address>/setup` and clicking **Change Service Password**. Only administrators and security administrators can change the password.

Note: If you change this password, you need to provide EMC Customer Service with the new password for certain maintenance and debug activities.

In addition to providing the ability to change the password, RemotelyAnywhere provides additional security by providing IP filtering. This way you can limit the service access to only trusted IP addresses. You can manage IP filtering for Remotely Anywhere by going to `https://<SP_IP_address>/setup` and clicking **Set RemotelyAnywhere Access Restrictions**. By

logging in to the VNX for block system using RemotelyAnywhere, you generate a unique message in the event log.

If a VNX system requires service, but the service password is unavailable, there is a permanently fixed default username/password that allows access through the service and serial ports. You should not physically connect these ports to anything in the data center. EMC recommends leaving these ports disconnected unless specifically requested by service personnel. These ports should be secured by controlling physical access to the room and/or rack where the storage systems are located.

Secure remote support considerations

For reference see the Remote Hardware Support: A Detailed Review technical notes on the EMC Online Support website at http://Support.EMC.com for an overview of the components and approaches that are available for secure service.

The recommended approach for secure remote support is to work with EMC to install and configure the EMC Secure Remote Support Gateway and Policy Manager. As described in the Remote Hardware Support: A Detailed Review technical notes, this provides initiated channels from your customer site to authorized EMC and service partner personnel using the encrypted gateway channel. The customer provides the server(s) (and is responsible for security) for the gateway software and accompanying Policy Manager. The customer must set policies for access to the server with the Policy Manager as well as manage customer access to the Policy Manager itself and its audit logs.

Some customers elect to use modem-based access for legacy reasons. They should work with their EMC representative or service partner to configure EMCRemote on the ESRS IP client management station to choose the appropriate security options.

Other customers may leverage Cisco's WebEx for the remote support of the VNX environment. When using WebEx, the customer must initiate the WebEx connection or accept one that EMC or a service partner initiates. If the customer initiates the WebEx instance, the log remains on the customer's site for the support session.

Security-patch management

VNX systems do not support installation of third-party utilities or patches. EMC will provide an officially released VNX Operating Environment (OE) patch, if needed, to correct a security-related issue (or any other kind of issue).

Malware detection

Malware detection is performed during VNX engineering cycle. EMC ensures that VNX systems are free of malware before the product ships. Because the VNX system is an appliance, additional software cannot be installed; therefore, malware detection is not provided or needed in deployed VNX systems.

CHAPTER 7

Advanced Management Capabilities

This chapter describes security enhancements in VNX systems that can be used to expand management capabilities and deliver a more secure and efficient customer experience.

Major topics include:

Remote management

Unisphere has been designed to support a "securely manage from anywhere, anytime" capability, which enables an administrator to manage a storage system from any browser-equipped station without needing to preinstall any software or special hardware. This capability requires the security enhancements that have been put into Unisphere, which complement any mechanism a company may already be using to enable remote access to corporate resources (for example, SecureID, VPN).

Remote management provides the ability to manage data centers that have become more complex and are up and running 24x7, with minimal staff. It also provides the ability to troubleshoot from offsite.

Internet Protocol version 6 (IPv6) addressing for a management port

IPv6 is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol version 4 (IPv4). IPv6 contains numerous features that make it attractive from a security standpoint. It is reliable and easy to set up, with automatic configuration. Huge, sparsely populated address spaces make it highly resistant to malicious scans and inhospitable to automated, scanning, and self-propagating worms and hybrid threats. VNX systems can be accessed with either IPv4 or IPv6 for Unisphere, both VNX for block and VNX for file CLI, and RemotelyAnywhere. This dual stack IPv4/IPv6 mode supports interoperation with older systems.

Support for VLAN tagging

VLAN is supported for iSCSI data ports and management ports on VNX storage systems. In addition to better performance, ease of management, and cost benefits, VLANs provide security advantages since devices configured with VLAN tags can see and communicate with each other only if they belong to the same VLAN. So, you can set up multiple virtual ports on the VNX, and segregate hosts into different VLANs based on your security policy. You can also restrict sensitive data to one VLAN. VLANs also make it harder to sniff traffic because they require sniffing across multiple networks, which provides extra security.

Enabling VLAN tagging is optional on a per-port basis. When enabled, up to eight virtual ports can be configured for a 1GB/s port and 10 GB/s port, and one virtual port for a management port. VLAN tagging on a management port supports IPv4 and IPv6 protocols. For more information on VLAN support, refer to the VLAN Tagging and Routing on CLARiiON white paper on the EMC Online Support website at http://Support.EMC.com.

SNMP management

SNMP is used for communication between the Control Station and Data Mover, so disabling it can interfere with some functions. For example, the server_netstat command will not work. The SNMP community string provides 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 VNX for file. *Configuring Events and Notifications on VNX for File* describes how to configure this feature.

SNMP management software can be used to monitor the state of VNX for block systems. An SNMP community is the group to which devices and management stations running SNMP belong. It defines where information is sent. The community name identifies the group. It will not respond to requests from management stations that do not belong to this community. For more information

on SNMP support, refer to the Managing EMC CLARiiON with SNMP white paper on the EMC Online Support website at http://Support.EMC.com.

Management support for FIPS 140-2

Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal government requirements that IT products should meet for Sensitive, but Unclassified (SBU) use. The standard defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems. To learn more about FIPS 140-2, refer to FIPS 1402-2 publication.

VNX systems, starting with VNX for block OE 31.5 and VNX for file OE 7.1, support a FIPS 140-2 mode for the SSL modules on the Storage Processor (SP) and Control Station (CS) that handle client management traffic. Management communication into and out of the system is encrypted using SSL. As a part of this process, the client and the storage management server negotiate an agreed upon cipher suite to use in the exchange. The use of the FIPS 140-2 mode restricts the allowable set of cipher suites that can be selected in the negotiation to only those that are sufficiently strong. If the FIPS 140-2 mode is enabled, you may find that some of your existing clients can no longer communicate with the management ports of the system if they do not support a cipher suite of acceptable strength. FIPS Mode cannot be enabled on a VNX system when non-FIPS-compliant certificates exist in the certificate store for file or block. You must remove all non-FIPS compliant certificates from the VNX system before you enable the FIPS 140-2 mode.

Managing FIPS 140-2 mode on a VNX unified system

Only the Administrator or Security Administrator has the privileges to manage the FIPS 140-2 mode. Use either of the following block or file CLI commands to set the FIPS 140-2 mode on a VNX unified system. Using either command affects the entire VNX:

Block CLI:

```
naviseccli -h <SP_IP_address> security -fipsmode -set 0|1 [-o]

   0 will set it to non-FIPS 140-2 mode
   1 will set it to FIPS 140-2 mode
```

File CLI:

`nas_fipsmode -enable` will set it to FIPS 140-2 mode.

`nas_fipsmode -disable` will set it to non-FIPS 140-2 mode.

Use either of the following block or file CLI commands to determine the current FIPS 140-2 mode for the entire VNX:

Block CLI:

```
naviseccli -h <SP_IP_address> security -fipsmode -get
```

File CLI:

```
nas_fipsmode -info
```

When you set the FIPS 140-2 mode on a VNX unified system, the storage management server will restart. For that brief period, management commands to both SPs and the Control Station will be blocked. However, this action should not effect the input/output operations happening on the storage system.

Note: On systems with two Control Stations, CS0 will fail over to CS1 when you set the FIPS 140-2 mode.

Managing FIPS 140-2 mode on a VNX for block system

Only the Administrator or Security Administrator has the privileges to manage the FIPS 140-2 mode. Use the following block CLI command to set the FIPS 140-2 mode on a VNX for block system:

```
naviseccli -h <SP_IP_address> security -fipsmode -set 0|1 [-o]

   0 will set it to non-FIPS 140-2 mode
   1 will set it to FIPS 140-2 mode
```

Use the following block CLI command to determine the current FIPS 140-2 mode for the VNX for block system:

```
naviseccli -h <SP_IP_address> security -fipsmode -get
```

When you set the FIPS 140-2 mode on a VNX for block system, the storage management server will restart. For that brief period, management commands to both SPs will be blocked. However, this action should not effect the input/output operations happening on the storage system.

Managing FIPS 140-2 mode on a VNX for file or Gateway system

Only the Administrator or Security Administrator has the privileges to manage the FIPS 140-2 mode. Use the following file CLI command to set the FIPS 140-2 mode on a VNX for file or Gateway system.

`nas_fipsmode -enable` will set it to FIPS 140-2 mode.

`nas_fipsmode -disable` will set it to non-FIPS 140-2 mode.

Use the following file CLI command to determine the current FIPS 140-2 mode on a VNX for file or Gateway system.

```
nas_fipsmode -info
```

When you set the FIPS 140-2 mode on a Gateway system, the NAS service on the Control Station will restart. For that brief period, management commands to the Control Station will be blocked. However, this action should not effect the input/output operations happening on the VNX for file or Gateway system.

Note: On systems with two Control Stations, CS0 will fail over to CS1 when you set the FIPS 140-2 mode.

APPENDIX A

Secure deployment and usage settings

This appendix describes a few example network topologies with varying degrees of security requirements.

Topics include:

Implementing Unisphere in secure environments

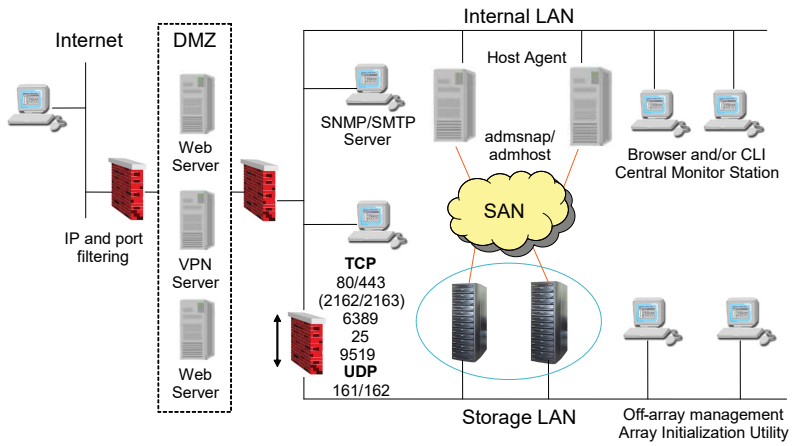
Security has become a high priority for many EMC customers. Understandably, many customers are actively securing their network infrastructure or are at least considering it. In addition, they may have varying security requirements and network topologies. However, securing the network without considering Unisphere network management requirements may cause problems when managing the storage system, including the loss of critical storage system events and inconsistencies in global Unisphere configuration data, such as the security database. By understanding the Unisphere architecture discussed throughout this paper, customers can have a secure network environment while still effectively managing their storage systems.

The following scenarios illustrate the flexibility of the Unisphere architecture in network topologies with varying degrees of security requirements. Each scenario employs commonly practiced IT security policies including the use of a de-militarized zone (DMZ) between the corporate network and the Internet.

Note: these examples are representative of different network topologies and how Unisphere may be implemented in different environments. The actual configuration at a customer site will depend on the customer's specific security requirements.

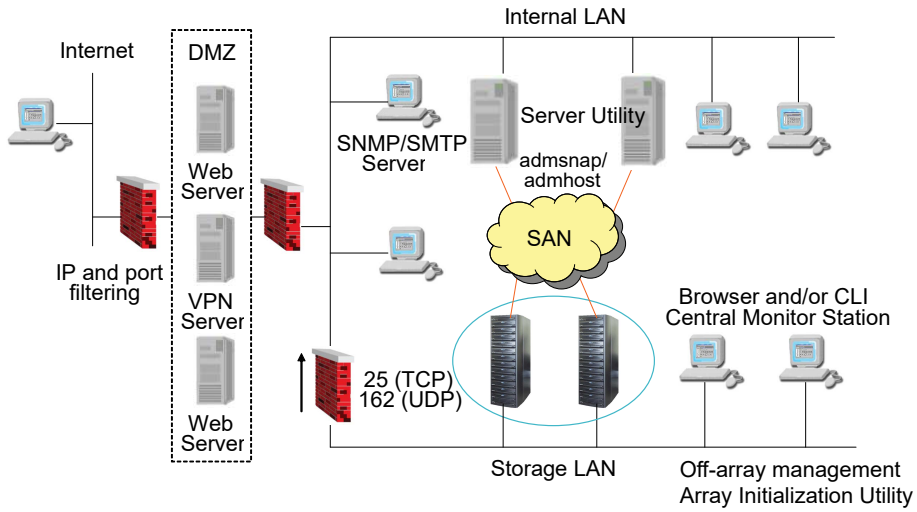
Minimally secure storage management network topology depicts an environment with minimal security measures in place. The corporate network is secure from the outside through the DMZ, while internally there are few restrictions for storage security. All VNX TCP/IP traffic (as listed in VNX for block - Ports used by Unisphere components) is allowed to flow in both directions between the internal LAN and the storage LAN. This configuration, which provides the most full-featured, easy-to-manage VNX environment, allows the user to manage storage systems from any location within the DMZ. The Unisphere Host Agent, which runs on SAN-attached servers, provides full host registration and LUN/volume mapping information. In addition, there are no restrictions for where a central monitoring station, SNMP server, Unisphere Client/Server management station, or ESRS IP client can be installed on the corporate network.

Figure 2 Minimally secure storage management network topology



Some customers may have more stringent security requirements in place, such as allowing storage systems to be managed only by management stations on the storage LAN, and not having management services or agents installed on production servers. As shown in Moderately secure storage management network topology , these requirements can be satisfied, without the loss of Unisphere management capabilities, by making a few minor changes to the configuration shown in Minimally secure storage management network topology. In the new configuration, the firewall between the storage LAN and internal LAN is modified to only allow outbound TCP/IP traffic that the VNX storage system initiates.

Figure 3 Moderately secure storage management network topology

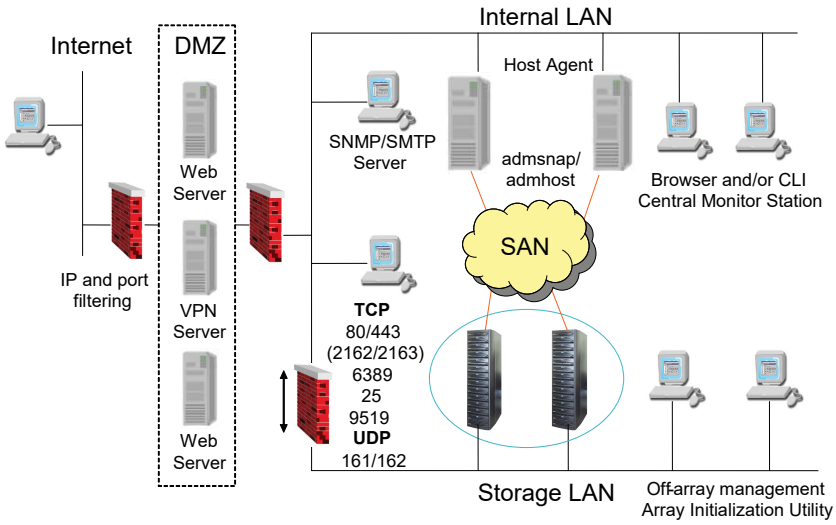


As a result of this modification, all Unisphere management and monitoring must be performed on the storage LAN, including management performed by Unisphere, CLI, central monitoring stations, Unisphere Client/Server management stations, and the ESRS IP Client. Note that SNMP traps and email notifications can still be sent to the corporate SMTP/SNMP server, as well as EMC Customer Service with ESRS IP Client. Finally, the Unisphere Host Agent is replaced by the Unisphere Server Registration Utility. All host management functionality is now in-band and no additional services are running on the production servers. However, LUN/volume mapping information is not available through Unisphere or Secure CLI; this information is available only through the server registration utility.

These changes greatly improve the overall security of the storage systems since all management activities must be initiated on the storage LAN. But this configuration is still vulnerable to a breach in the internal firewall. If the firewall is compromised from the internal LAN, any computer in the corporate network will be able to manage the storage systems. The use of VNX-based IP filtering eliminates this potential threat.

The final configuration, see Highly secure storage management network topology, provides a very high level of security for a company's storage systems. Potential threats are reduced to a breach of physical resources. In addition, enabling IP filtering for the VNX domain limits the management of the storage systems to a single Windows server, namely the Unisphere Client/Server management station. IP filtering allows each storage system or domain to have a list of trusted client IP addresses. The storage system(s) will accept management connections only from these trusted clients. IP filtering does not affect other traffic, such as Event Monitor polls, email notifications, or SNMP. IP filtering configuration can be found in the http://<SP IP address>/ setup pages or via the naviseccli security -trustedclient switch.

Figure 4 Highly secure storage management network topology



This configuration provides two layers of authentication. First, the user must have valid Windows credentials to log in to the management station. Second, the user must have valid Unisphere credentials to manage the storage system. The trade-off with this configuration is the loss of flexibility in terms of management options. Neither the ability to manage from anywhere in the system nor the ability to centrally monitor the entire network is available. Also, remote support of the storage system by using the ESRS IP Client is not possible in this environment. Note that ESRS IP Client can still send notifications to EMC Customer Service.

As is evident, the Unisphere architecture is very flexible in its ability to integrate into several secure environments. The key to a successful implementation of VNX management is an understanding of Unisphere network requirements, which are listed in VNX for block - Ports used by Unisphere components and described in the previous scenarios.

APPENDIX B

TLS cipher suites

This appendix lists the TLS cipher suites supported by VNX.

Topics include:

Supported TLS cipher suites

A cipher suite defines a set of technologies to secure your TLS communications:

- Key exchange algorithm (how the secret key used to encrypt the data is communicated from the client to the server). Examples: RSA key or Diffie-Hellman (DH)
- Authentication method (how hosts can authenticate the identity of remote hosts). Examples: RSA certificate, DSS certificate, or no authentication
- Encryption cipher (how to encrypt data). Examples: AES (256 or 128 bits) or 3DES (168 bits)
- Hash algorithm (ensuring data by providing a way to determine if data has been modified). Examples: SHA-2 or SHA-1

The supported cipher suites combine all these items. Default/Supported TLS cipher suites on VNX2 Control Station lists the cipher suites supported by VNX2 for the Control Station. Default/Supported TLS cipher suites on VNX2 Storage Processor lists the cipher suites supported by VNX2 for the Storage Processor. Default/Supported TLS cipher suites on VNX2 Data Mover lists the default/supported cipher suites used by VNX2 for the Data Mover. Default/Supported TLS cipher suites on VNX2 related to Replication lists the cipher suites supported by VNX2 for Replication. Default/Supported TLS cipher suites on VNX1 Control Station lists the cipher suites supported by VNX1 for the Control Station. Default/Supported TLS cipher suites on VNX1 Storage Processor lists the cipher suites supported by VNX1 for the Storage Processor. Default/Supported TLS cipher suites on VNX1 Data Mover lists the default/supported cipher suites used by VNX1 for the Data Mover. Default/Supported TLS cipher suites on VNX1 related to Replication lists the cipher suites supported by VNX1 for Replication.

The following lists give the OpenSSL names of the TLS cipher suites for the different VNX components and their associated ports.

Note: The cipher suites are listed alphabetically for readability only. The order does not represent the strength level.

The following restriction applies:

- Some cipher suites will not be accepted by VNX for file because of certificate size (if the certificate presented by the Data Mover has a 2048-bit key, ciphers with a smaller key will be rejected).

Table 9 Default/Supported TLS cipher suites on VNX2 Control Station

Cipher Suites	Protocols	Ports
AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	443
AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	443
CAMELLIA128-SHA	TLSv1, TLSv1.1, TLSv1.2	443
CAMELLIA256-SHA	TLSv1, TLSv1.1, TLSv1.2	443
DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	443
AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	5989
AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	5989
DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	5989

Table 10 Default/Supported TLS cipher suites on VNX2 Storage Processor

Cipher Suites	Protocols	Ports
AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	443
AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	443
DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	443

Table 11 Default/Supported TLS cipher suites on VNX2 Data Mover

Cipher Suites	Protocols	Ports
AECDH-AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
AECDH-AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
AECDH-DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
CAMELLIA128-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
CAMELLIA256-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
DHE-RSA-AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
DHE-RSA-AES128-SHA256 (CBC)	TLSv1.2	989, 990, 5080
DHE-RSA-AES128-SHA256 (GCM)	TLSv1.2	989, 990, 5080
DHE-RSA-AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
DHE-RSA-AES256-SHA256	TLSv1.2	989, 990, 5080
DHE-RSA-AES256-SHA384	TLSv1.2	989, 990, 5080
DHE-RSA-CAMELLIA128-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
DHE-RSA-CAMELLIA256-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
ECDHE-RSA-AES128-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
ECDHE-RSA-AES128-SHA256 (CBC)	TLSv1.2	989, 990, 5080
ECDHE-RSA-AES128-SHA256 (GCM)	TLSv1.2	989, 990, 5080
ECDHE-RSA-AES256-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
ECDHE-RSA-AES256-SHA384 (CBC)	TLSv1.2	989, 990, 5080
ECDHE-RSA-AES256-SHA384 (GCM)	TLSv1.2	989, 990, 5080

Table 11 Default/Supported TLS cipher suites on VNX2 Data Mover (continued)

Cipher Suites	Protocols	Ports
ECDHE-RSA-DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
EDH-RSA-DES-CBC3-SHA	TLSv1, TLSv1.1, TLSv1.2	989, 990, 5080
RSA-AES128-SHA256 (CBC)	TLSv1.2	989, 990, 5080
RSA-AES128-SHA256 (GCM)	TLSv1.2	989, 990, 5080
RSA-AES256-SHA256	TLSv1.2	989, 990, 5080
RSA-AES256-SHA384	TLSv1.2	989, 990, 5080

Note: Instances where cipher suites do not indicate the Key Exchange or Authentication entry use RSA.

If required, the Data Mover cipher parameter can be changed from the default setting either through Unisphere or through VNX CLI for File commands, `server_ftp` and `server_http`. For more information about setting the Data Mover cipher parameter, refer to the Unisphere online help or the *VNX Command Line Interface Reference for File*.

Table 12 Default/Supported TLS cipher suites on VNX2 related to Replication

Cipher Suites	Protocols	Ports
ADH-AES128-SHA	TLSV1, TLSV1.1, TLSv1.2	5085
ADH-AES128-SHA256	TLSv1.2	5085
ADH-AES128-GCM-SHA256	TLSv1.2	5085
ADH-AES256-SHA	TLSV1, TLSV1.1, TLSv1.2	5085
ADH-AES256-SHA256	TLSv1.2	5085
ADH-AES256-GCM-SHA384	TLSv1.2	5085
ADH-CAMELIA128-SHA	TLSV1, TLSV1.1, TLSv1.2	5085
ADH-CAMELIA256-SHA	TLSV1, TLSV1.1, TLSv1.2	5085
ADH-DES-CBC3-SHA	TLSV1, TLSV1.1, TLSv1.2	5085

Table 13 Default/Supported TLS cipher suites on VNX1 Control Station

Cipher Suites	Protocols	Ports
AES128-SHA	TLSv1	443
AES256-SHA	TLSv1	443
DES-CBC3-SHA	TLSv1	443
DHE-RSA-AES128-SHA	TLSv1	443
DHE-RSA-AES256-SHA	TLSv1	443
EDH-RSA-DES-CBC3-SHA	TLSv1	443
AES128-SHA	TLSv1, TLSv1.1	5989

Table 13 Default/Supported TLS cipher suites on VNX1 Control Station (continued)

Cipher Suites	Protocols	Ports
AES256-SHA	TLSv1, TLSv1.1	5989
DES-CBC3-SHA	TLSv1, TLSv1.1	5989

Table 14 Default/Supported TLS cipher suites on VNX1 Storage Processor

Cipher Suites	Protocols	Ports
AES128-SHA	TLSv1, TLSv1.1	443
AES256-SHA	TLSv1, TLSv1.1	443
DES-CBC3-SHA	TLSv1, TLSv1.1	443

Table 15 Default/Supported TLS cipher suites on VNX1 Data Mover

Cipher Suites	Protocols	Ports
AES128-SHA	TLSv1	990, 5080
AES256-SHA	TLSv1	990, 5080
CAMELLIA128-SHA	TLSv1	990, 5080
CAMELLIA256-SHA	TLSv1	990, 5080
DES-CBC-SHA	TLSv1	990, 5080
DES-CBC3-SHA	TLSv1	990, 5080
DHE-RSA-AES128-SHA	TLSv1	990, 5080
DHE-RSA-AES256-SHA	TLSv1	990, 5080
DHE-RSA-CAMELLIA128-SHA	TLSv1	990, 5080
DHE-RSA-CAMELLIA256-SHA	TLSv1	990, 5080
EDH-RSA-DES-CBC-SHA	TLSv1	990, 5080
EDH-RSA-DES-CBC3-SHA	TLSv1	990, 5080

Table 16 Default/Supported TLS cipher suites on VNX1 related to Replication

Cipher Suites	Protocols	Ports
ADH-AES128-SHA	TLSv1	5085
ADH-AES256-SHA	TLSv1	5085
ADH-CAMELLIA128-SHA	TLSv1	5085
ADH-CAMELLIA256SHA	TLSv1	5085
ADH-DES-CBC3-SHA	TLSv1	5085
ADH-DES-CBC-SHA	TLSv1	5085

APPENDIX C

LDAP-based directory server configuration

This appendix provides information about tools you can use to better understand the structure of your organization's information in the LDAP-based directory server and tips about how to interpret this information. You must understand where your users and groups are located. Use this information to set up the directory server, and to configure the connection between the Control Station's LDAP-based client and the directory server. Log in to Unisphere and use **Settings > Security Settings** (task list) **> Manage LDAP Domain**.

Topics include:

Active Directory Users & Computers

Active Directory user and group accounts can be managed with the Active Directory Users & Computers (ADUC) MMC Snap-in. This snap-in is installed automatically on every Windows domain controller. You access this tool from **Control Panel** > **Administrative Tools** > **Active Directory Users & Computers**.

About this task

Information required to connect to an Active Directory directory server lists the information you need for a successful connection to Active Directory.

Table 17 Information required to connect to an Active Directory directory server

Required connection information	Your values
Fully-qualified domain name (also known as the base distinguished name)	
Primary domain controller/directory server IP address or hostname	
Secondary domain controller/directory server IP address or hostname	
Account name (also known as the bind distinguished name)	

Procedure

1. Open ADUC and (if necessary) connect to the domain. Right-click the domain name, and then select **Find** from the menu.
2. Identify a domain user who will be a VNX for file user. To locate the user profile, type the user's name in the **Find** field and click **Find Now**.
3. Add the X.500 path to the displayed user information by selecting **View** > **Choose Columns**.
4. Select **X500 Distinguished Name** from the **Columns available** field and click **Add**.
5. The Find window now displays the X.500 distinguished name of this user. The X.500 distinguished name contains the user's name (CN=Joe Muggs) and the path to the container in the directory structure where this user is located: CN=Users,DC=derbycity,DC=local. Record the path.
6. Verify that all other VNX for file users use the same path by either:
   - Repeating the Find for all VNX for file user accounts
     or
   - Navigating to that area of the directory in ADUC, and locating all VNX for file user accounts
7. Repeat steps 1 through 6 to find the path to the container in the directory structure where the groups are located.

   If the user and group paths are both CN=Users,DC=<domain component>,DC=<domain component>[, DC=<domain component>...] (for example CN=Users,DC=derbycity,DC=local), you can use the **Default Active Directory** option in the Unisphere **Manage LDAP Domain** view. This option assumes that the users and groups are located in the default container (CN=Users), so you do not have to specify the user or group search path.

8. Users might not be in the default container (CN=Users). They may instead be located in other containers or organizational units within the directory, for example VNX for File Users. In this case, you need to use the **Custom Active Directory** option in the Unisphere **Manage LDAP Domain** view and manually enter the search paths.
9. Groups might not be in the default container (CN=Users), and they do not have to be located with the users. They may instead be located within other containers or organizational units within the directory.
10. The LDAP user and group search begins with the path specified, and searches that container and all containers below it. If VNX for file users and groups are not located within the same container or organizational unit, you must use the intersection (common parts) of their collective paths when you specify the user and group search paths. In some cases, this may need to be the root of the domain. For example, assume that VNX for file users are stored in the following two Active Directory locations:
    - Path 1: CN=Users,DC=derbycity,DC=local
    - Path 2: OU=VNX Users,OU=EMC VNX,DC=derbycity,DC=local

    In order for VNX for file to find all users, you need to use the intersection of the two paths as your search path, that is, the domain root DC=derbycity,DC=local. Type this value in the **User Search Path** field in the Unisphere **Manage LDAP Domain** view.
11. Use the **Find** window again to determine the full X.500 path of the account you will use to connect the VNX for file Control Station to the directory. In this case you should not remove the username from the path because you are specifying the path to an individual account.
    - If you are using the Default Active Directory option in the Unisphere **Manage LDAP Domain** view, type only the account name, for example VNX LDAP Binding, in the Account Name field. You do not need to provide the X.500 syntax because the VNX for file software constructs the full X.500 path.
    - If you are using the **Custom Active Directory** option in **Manage LDAP Domain**, then type the full X.500 path in the **Distinguished Name** field.

Ldap Admin

Unlike Active Directory, other LDAP-based directory servers do not typically ship with a GUI management interface. In this case you might use a tool like Ldap Admin to find the proper search paths on LDAP servers. The free Ldap Admin tool (a Windows LDAP manager available from ldapadmin.sourceforge.net) lets you browse, search, modify, create, and delete objects on a LDAP server. Ldap Admin's copy-to-clipboard functionality is especially useful for easily transferring values into the Unisphere **Settings > Security** (task list) **> Manage LDAP Domain** fields.

About this task

Information required to connect to a Customized Active Directory or Other Directory LDAP-based directory server lists the information you need for a successful connection to a customized Active Directory or other LDAP-based directory server such as OpenLDAP.

Table 18 Information required to connect to a Customized Active Directory or Other Directory LDAP-based directory server

Required connection information	Your values
Fully-qualified domain name (also known as the base distinguished name)	
Primary directory server IP address or hostname	

Table 18 Information required to connect to a Customized Active Directory or Other Directory LDAP-based directory server (continued)

Required connection information	Your values
Secondary directory server IP address or hostname	
Distinguished name (also known as the bind distinguished name)	
User search path	
User name attribute	
Group search path	
Group name attribute	
Group class	
Group member	

Procedure

1. Start Ldap Admin and create a new connection. Click **Test connection** to verify the connection.
2. Open the connection to the LDAP server, right-click the domain name, and then select **Search** from the menu.
3. Identify an LDAP user who will be a VNX for file user. To locate the user profile, type the user's name in the **Name** field and click **Start**.
4. Right-click the appropriate user from the results list, and then select **Go to** from the menu. You will use this user to determine the user and group search paths. Close the **Search** window.
5. On the main Ldap Admin window, notice that the status bar contains the distinguished name (DN) of the folder in which the user is located. Many LDAP servers follow the convention outlined in RFC2307 and put users in a People container.
6. Right-click the folder, and then select **Copy dn to clipboard** from the menu.
7. In the unisphere **Manage LDAP Domain** view, select the **Other Directory Servers** option. Paste the DN value in the **User Search Path** field.
8. Verify that all other VNX for file users use the same path by:
   - Repeating the Search for all VNX for file user accounts
     or
   - Navigating to that area of the directory in Ldap Admin, and locating all VNX for file user accounts
9. Repeat steps 2 through 8 to search on a group name to find the path to the container in the directory structure where the groups are located. When you search by group name, you have to use an advanced search and supply a search filter in the form cn=<group name>. Once the search is complete, right-click the appropriate group from the results list, and then select **Go to** from the menu.
10. The LDAP user and group search begins with the path specified, and searches that container and all containers below it. If VNX for file users and groups are not located within the same container or organizational unit, you must use the intersection (common parts) of their collective paths when you specify the user and group search paths. In some cases, this

may need to be the root of the domain. For example, assume that VNX for file users are stored in the following two Active Directory locations:

- Path 1: OU=People,DC=openldap-eng,DC=local
- Path 2: OU=VNX Users,OU=EMC VNX, DC=openldap-eng,DC=local

In order for VNX for file to find all users, you need to use the intersection of the two paths as your search path, that is, the domain root DC=openldap-eng,DC=local.

11. Use the Search window to locate the user account you will use to connect the VNX for file Control Station to the directory. Right-click the account name, and then select **Copy dn to clipboard**. Paste the DN value in the **Distinguished Name** field in the Unisphere **Manage LDAP Domain** view, for example uid=vnx,ou=People.

APPENDIX D

VNX for file CLI role-based access

This appendix provides information about how to set up role-based access for VXN for file CLI commands. It also contains lists of the different types of commands. The topics include:

CLI role-based access setup

A user account is always associated with a primary group and each group is assigned a role. A role defines the privileges (that is, the operations) the user can perform on a particular File object.

Defining role-based access for commands

This appendix provides information about how to setup role-based access for CLI commands. The first four tables list the CLI commands for which you can specify the privileges needed to perform different command actions. The object on which privileges are defined and the specific command actions available when Modify or Full Control privileges are selected are listed for each command. Using this information you can create a custom role (also known as a user role) that gives a user associated with this role exactly the privileges necessary to perform his job. Or you can associate a user with the predefined role that already includes Full Control privileges for the command. The first table lists the commands with the prefix cel. The second table lists the commands with the prefix fs. The third table lists the commands with the prefix nas. And the fourth table lists the commands with the prefix server.

You create and manage role-based administrative access with **Settings** > **Security** > **User Management** > **Local Users for File** > **Roles** or **Settings** > **Security** > **User Management** > **User Customization for File** > **Roles**. You must be root or a user associated with the Administrator or Security Administrator role to create a user account and to associate it with a group and role.

Read-only privileges

Regardless of the role with which he is associated, a user always has read-only privileges for all commands and command options that display information. Some of the command actions available with read-only privileges include info, list, status, and verify. The fifth table lists commands that users associated with any role can execute.

Commands not covered by the role-based access feature

The final table lists the commands that are not covered by the role-based access feature. Some of these commands invoke scripts, others are based on legacy executables, and others are associated with File objects that are not exposed. If the File object associated with a command is not exposed in **Create Role**, you cannot create a custom (user) role that allows you to specify the privileges needed to perform different command actions. Consequently these commands can only be performed by the default user accounts root and nasadmin or, in some cases, by a user account associated with the root and nasadmin roles.

cel commands

Note: **Object category** lists the field in the **Roles** dialogs where privileges can be set.

Note: All commands are also included in the NAS Administrator and Storage Administrator roles unless otherwise noted.

Table 19 cel commands

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
cel_fs	Storage>File Systems		extract import	FileMover Application

fs commands

Note: **Object category** lists the field in the **Roles** dialogs where privileges can be set.

Note: All commands are also included in the NAS Administrator and Storage Administrator roles unless otherwise noted.

Table 20 fs commands

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
fs_ckpt	Data Protection>Checkpoints	modify refresh	create restore	Data Protection Data Recovery Local Data Protection
fs_dhsm	Storage>FileMover	connection modify modify	connection create connection delete	FileMover Application
fs_group	Storage>File Systems		create delete shrink xtend	FileMover Application
fs_rdf	Storage>Storage Systems		info mirror restore	
fs_timefinder	Storage>File Systems		mirror restore snapshot	

nas commands

Note: **Object category** lists the field in the **Roles** dialogs where privileges can be set.

Note: All commands are also included in the NAS Administrator and Storage Administrator roles unless otherwise noted.

Table 21 nas commands

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
nas_ckpt_schedule	Data Protection >Checkpoints Data Protection >VTLU	modify pause resume	create delete	Data Protection Data Recovery Local Data Protection
nas_copy	Data Protection> Replication		create destination source interconnect	Data Recovery
nas_devicegroup	Storage>Storage Systems		acl resume	

Table 21 nas commands (continued)

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
			suspend	
nas_disk	Storage>Volumes	rename	delete	
nas_diskmark	Storage>Storage Systems		mark	
nas_fs	Storage>File Systems	modify rename translate access policy start xtend	acl create delete type	FileMover Application
nas_fsck	Storage>File Systems		start	FileMover Application
nas_license	System>Licenses	create delete init		Security Administrator (not included in the NAS Administrator and Storage Administrator roles)
nas_pool	Storage>Pools	modify shrink xtend	create delete	
nas_quotas	Storage>Quotas Storage>File System	edit on | off	clear	
nas_replicate	Data Protection>Replication	modify refresh	create delete failover reverse start stop switchover	Data Recovery
nas_server	System>Data Movers Protocols>CIFS	acl rename	create delete (System>Data Movers object category) vdm (Protocols>CIFS object category)	
nas_slice	Storage>Volumes	rename	create delete	

Table 21 nas commands (continued)

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
nas_storage	Storage>Storage Systems	modify rename	acl delete fallback sync	
nas_task	System>Task		abort delete	All users can abort and delete any task they own but only root user can abort and delete tasks owned by any user
nas_volume	Storage>Volumes	rename xtend	acl clone create delete	

server commands

Note: **Object category** lists the field in the **Roles** dialogs where privileges can be set.

Note: All commands are also included in the NAS Administrator and Storage Administrator roles unless otherwise noted.

Table 22 server commands

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
server_arp	Networking>NIS		delete set	Network Administrator
server_cdms	Storage>Migration	convert halt start	connect disconnect	
server_certificate	Security>Public Key Certificates		cacertificate delete cacertificate import persona clear persona generate persona import	Security Administrator (not included in the NAS Administrator and Storage Administrator roles)
server_cifs	Protocol>CIFS	disable enable join rename	add delete migrate	

Table 22 server commands (continued)

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
		replace unjoin update		
server_cifssupport	Protocols>CIFS	acl secmap update	secmap create secmap delete secmap import secmap migration	
server_cpu	System>Data Movers		halt reboot	
server_date	System>Data Movers	timesvc hosts timesvc start timesvc update	timesvc delete timesvc set timesvc stop	
server_devconfig	Storage>Storage System	rename	create	
server_dns	Networking>DNS	option	delete protocol	Network Administrator
server_export	Protocols>NFS or Protocols>CIFS	unexport	protocol (NFS)	
server_ftp	Protocols>NFS	modify service stat reset	service start | stop	Network Administrator
server_http	Storage>FileMover	modify append remove service start | stop		FileMover Application
server_ifconfig	Networking>Interfaces	up down ipsec and noipsec (Applicable only to systems running VNX OE for file earlier than version 8.x.) mtu vlan	create delete	Network Administrator
server_ip	Networking>Routing		neighbor create | delete route create | delete	Network Administrator

Table 22 server commands (continued)

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
server_kerberos	Protocols>CIFS	keytab ccache kadmin	add delete	Security Administrator (not included in the NAS Administrator and Storage Administrator roles)
server_ldap	Networking>NIS	set	clear service start | stop	Network Administrator
server_mount	Storage>File Systems		all force options	FileMover Application
server_mountpoint	Storage>File Systems		create delete	
server_name	System>Data Movers	<new_name>		
server_nfs	Protocols>NFS	user v4 client v4 stats zero	service principal v4 service	command options mapper set and mapping can only be executed by root
server_nfsstat	Protocols>NFS	zero		
server_nis	Networking>NIS		delete	Network Administrator
server_param	System>Data Movers	facility		
server_rip	Networking>Routing	ripin noripin		Network Administrator
server_route	Networking>Routing		add delete flush deleteAll	Network Administrator
server_security	Protocols>CIFS	modify update	add delete	Security Administrator (not included in the NAS Administrator and Storage Administrator roles)
server_setup	System>Data Movers	load protocol load		
server_snmp	Networking>NIS		community location syscontact	Network Administrator

Table 22 server commands (continued)

Command	Object category	Actions available with modify privileges	Actions available with full control privileges	Included in predefined role
server_standby	System>Data Movers	activate restore	create delete	
server_stats	Storage>File Systems	monitor	noresolve service	
server_sysconfig	Networking>Devices	pci	virtual new virtual delete	Network Administrator
server_umount	Storage>File Systems	temp	all perm	FileMover Application
server_usermapper	Protocols>CIFS		disable enable import remove	Security Administrator (not included in the NAS Administrator and Storage Administrator roles)
server_vtlu	Data Protection>VTLU	service set storage extend storage export storage import tlu modify	drive umount storage delete storage new tape eject tape inject tlu delete	FileMover Application

Table 23 Commands all roles have privileges to execute

Command
nas_inventory
server_checkup
server_df
server_ping
server_ping6
server_sysstat
server_uptime
server_version

Table 24 Commands not covered by the role-based access feature

Command	Notes
cs_standby	Requires root privileges
nas_acl	Can be executed with nasadmin privileges

Table 24 Commands not covered by the role-based access feature (continued)

Command	Notes
nas_automountmap	Can be executed with nasadmin privileges
nas_ca_certificate	Requires root privileges to generate a certificate
nas_cel	Can be executed with nasadmin privileges
nas_checkup	Can be executed with nasadmin privileges
nas_connecthome	Requires root privileges to modify and test
nas_config	Requires root privileges
nas_cs	Requires root privileges
nas_emailuser	Can be executed with nasadmin privileges
nas_event	Can be executed with nasadmin privileges
nas_halt	Requires root privileges
nas_logviewer	Can be executed with nasadmin privileges
nas_message	Can be executed with nasadmin privileges
nas_mview	Requires root privileges
nas_rdf	Requires root privileges
nas_version	Can be executed with nasadmin privileges
server_archive	Can be executed with nasadmin privileges
server_cepp	Can be executed with nasadmin privileges
server_dbms	Requires root privileges to delete, compact, repair, and restore the database
server_file	Can be executed with nasadmin privileges
server_ipsec	Can be executed with nasadmin privileges
server_iscsi	Can be executed with nasadmin privileges
server_log	Can be executed with nasadmin privileges
server_mpfs	Can be executed with nasadmin privileges (Applicable only to systems running VNX OE for file earlier than version 8.x.)
server_mt	Can be executed with nasadmin privileges
server_netstat	Can be executed with nasadmin privileges
server_nfs	Requires root privileges to configure secure NFS mapping
server_pax	Requires root privileges to reset stats
server_snmpd	Can be executed with nasadmin privileges
server_stats	Can be executed with nasadmin privileges
server_tftp	Can be executed with nasadmin privileges
server_user	Can be executed with nasadmin privileges

Table 24 Commands not covered by the role-based access feature (continued)

Command	Notes
server_viruschk	Can be executed with nasadmin privileges

APPENDIX E

VNX for file CLI security configuration operations

This appendix describes the security configuration related operations that can be performed by using the VNX for file CLI.

Major topics include:

Configuring password policy

This feature enables the VNX for file root administrator to define password complexity requirements for all local users. Password policy provides a general description.

Note: This feature does not apply to domain-mapped users, whose passwords are governed by the policies within the domain. Also, you must be root to execute the **/nas/sbin/nas_config** command.

Define password policy interactively

About this task

Procedure

1. To initiate a script that prompts for password policy definitions, use this command syntax:

   ```
   # /nas/sbin/nas_config -password
   ```

   Output:

   ```
   Minimum length for a new password (Between 6 and 15): [8]
   Number of attempts to allow before failing: [3]
   Number of new characters (not in the old password): [3]
   Number of digits that must be in the new password: [1]
   Number of special characters that must be in a new password: [0]
   Number of lower case characters that must be in password: [0]
   Number of upper case characters that must be in password: [0]
   ```

2. The current value defined for each field is displayed in brackets. The original default values for each field are: length: minimum 8 characters, range 6-15 attempts: maximum of 3 attempts new characters: minimum of 3 characters digits: minimum of 1 digit special, lowercase, and uppercase characters: 0

   To change the value for each field, type a new value when prompted.

Define specific password policy definitions

About this task

Procedure

1. To set specific password policy definitions, use this command syntax:

   ```
   # /nas/sbin/nas_config -password[-min <6..15>] [-retries
   <max_allowed>] [-newchars <min_num>] [-digits <min_num>]
   [-spechars <min_num>] [-lcase <min_num>] [-ucase <min_num>]
   ```

   where:

   <6..15> = minimum length of the new password. The default length is 8 characters. The length has to be a value between 6 and 15 characters.

   <max_allowed> = number of attempts a user can make to define an acceptable new password before the command fails. The default value is 3 attempts.

   <min_num> = minimum number of characters that must be in the new password that were not included in the old password. The default value is 3 characters.

   <min_num> = minimum number of digits that must be included in the new password. The default value is 1 digit.

<min_num> = minimum number of special characters (such as !, @, #, $, %, &, ^, and *) that must be included in the new password. The default value is 0.

<min_num> = minimum number of lower-case characters that must be included in the new password. The default value is 0.

<min_num> = minimum number of upper-case characters that must be included in the new password. The default value is 0.

Example:

To set the minimum length of a new password to 10 characters, type:

```
# /nas/sbin/nas_config -password -min 10
```

Set password expiration period

About this task

The /etc/login.defs file contains the parameter used to set password expiration.

1. Log in to the CLI with your username and password. You must have root privileges to access the /etc/login.defs file.
2. Change the value of the pass_max_days parameter in the /etc/login.defs file using vi or another text editor.
   Note: The default expiration period is 120 days.

Configuring session timeout

VNX for file enforces a session timeout for both Unisphere sessions and Control Station shell sessions. You can change the default value of the Control Station session timeout by using the command `/nas/sbin/nas_config -sessiontimeout`.

Note: You must be root to execute the `/nas/sbin/nas_config -sessiontimeout` command.

The Control Station supports three shells:

- bash
- ksh
- tcsh

Each shell supports a session timeout feature. The Control Station session timeout option sets the session timeout value across the system, automatically updating the appropriate values in /etc/ environment for the bash and ksh shells, and the autologout variable in `/etc/csh.cshrc` for the tcsh shell.

After the value is set, newly created shells are affected (but not any currently running shells).

Note: You can change the session timeout value for individual users by setting the relevant variable in the user's shell configuration file (for example, `~/.bashrc`). Values are not restricted if you edit the configuration file directly.

Change the session timeout value

About this task

The default session timeout value for Control Station shell sessions is 60 minutes. Inactivity or idle time is defined as the time since a primary shell prompt was displayed and no input has been received. Therefore waiting at a prompt within a command for some indeterminate amount of time is not affected by the session timeout value.

Procedure

1. To change the session timeout value, use this command syntax:

   ```
   # /nas/sbin/nas_config -sessiontimeout<minutes>
   ```

   where:

   <minutes> = number of minutes for session timeout (in the range 5 through 240)

   Example:

   To change the session timeout value to 200 minutes, type:

   # /nas/sbin/nas_config -sessiontimeout 200

Disable session timeout

About this task

Procedure

1. To disable session timeout, use this command syntax:

   ```
   # /nas/sbin/nas_config -sessiontimeout 0
   ```

   or

   ```
   # /nas/sbin/nas_config -sessiontimeout off
   ```

Protect session tokens

About this task

The connection between a user and Unisphere and between two VNX for file systems uses SHA1 to generate checksums to protect the session tokens (cookies) that identify users after they log in. The SHA1 secret value used to generate the checksums is set at random during installation. However, to enhance security, you can change the default SHA1 secret value.

1. Log in to the CLI with your username and password. You must have root privileges to access the /nas/http/conf/secret.txt file.
2. Edit the /nas/http/conf/secret.txt file using vi or another text editor.
   Replace the default phrase with a new value and save the file.

   When you change this value, existing session tokens are no longer valid and current users of Unisphere will have to log in again.

Configuring network encryption and authentication using the SSL protocol

Secure Socket Layer (SSL) is a session level protocol used to encrypt network transmissions on the Internet. It encrypts data and provides message and server authentication. It also supports client authentication if required by the server. SSL is independent of higher level protocols so it can encapsulate any of the application level protocols such as HTTP and LDAP:

- Hypertext Transfer Protocol (HTTP) is a fast, stateless, and object-oriented protocol used on the web. It enables web clients and servers to negotiate and interact. Unfortunately it has minimal security features. HTTPS (Secure) is a variant of HTTP used by a server that is SSL-enabled.

- Lightweight Directory Access Protocol (LDAP) is an industry-standard access protocol that runs directly over TCP/IP. It is the primary access protocol for Active Directory and other directory servers such as the Sun Java System Directory Server (iPlanet) and OpenLDAP.

VNX for File supports SSL for Data Mover HTTP and LDAP connections.

Using HTTPS on VNX for file

You enable SSL on Data Mover HTTP connections through the **server_http** command. Currently, the VNX for File FileMover feature uses HTTPS and SSL's encryption and authentication features. *Using VNX FileMover* describes how to configure SSL with HTTP for use by FileMover. The keys and certificates used with SSL are managed by using PKI. PKI is available through the CLI and Unisphere. Planning considerations for Public Key Infrastructure on VNX for file provides an overview of the PKI feature. Configuring PKI and Managing PKI describe how to configure and manage PKI through the VNX for file CLI.

Using SSL with LDAP on VNX for file

You enable SSL on Data Mover LDAP connections through the **server_ldap** command. Currently, the VNX for File naming service support for OpenLDAP, iPlanet, and Active Directory uses LDAP and SSL's encryption and authentication features. *Configuring VNX Naming Services* describes how to configure SSL with LDAP for use by the OpenLDAP and iPlanet LDAP-based directory servers. The keys and certificates used with SSL are managed through PKI. PKI is available through the CLI and Unisphere. Planning considerations for Public Key Infrastructure on VNX for file provides an overview of the PKI feature. Configuring PKI and Managing PKI describe how to configure and manage PKI through the VNX for file CLI.

Change the default SSL protocol

About this task

VNX for file supports the following SSL protocol versions:

- SSLv3
- TLSv1

Procedure

1. To change the default SSL protocol, use this command syntax:

   ```
   $ server_param <movername> -facility ssl -modify protocol
   -value <new_value>
   ```

   where:

   <movername> = name of the Data Mover

   <new_value> = 0 (both SSLv3 and TLSv1), 1 (only SSLv3), or 2 (only TLSv1)

   Note: The default value is 0.

   Parameter and facility names are case-sensitive.

   Examples:

   To change the default SSL protocol to SSLv3 only, type:

   ```
   $ server_param server_2 -facility ssl -modify protocol -value 1
   ```

   To change the default SSL protocol to TLSv1 only, type:

   ```
   $ server_param server_2 -facility ssl -modify protocol -value 2
   ```

   Output:

```
server_2 : done
```

Change the default SSL cipher suite

About this task

A cipher suite defines a set of technologies to secure your SSL communications:

- Key exchange algorithm (how the secret key used to encrypt the data is communicated from the client to the server). Examples: RSA key or Diffie-Hellman (DH)
- Authentication method (how hosts can authenticate the identity of remote hosts). Examples: RSA certificate, DSS certificate, or no authentication
- Encryption cipher (how to encrypt data). Examples: AES (256 or 128 bits), RC4 (128 bits or 56 bits), 3DES (168 bits), DES (56 or 40 bits), or null encryption
- Hash algorithm (ensuring data by providing a way to determine if data has been modified). Examples: SHA-1 or MD5

The supported cipher suites combine all these items. Supported SSL cipher suites lists the SSL cipher suites supported by VNX for file.

Procedure

1. To change the default SSL cipher suite, use this command syntax:

   ```
   $ server_param <movername> -facility ssl -modify cipher
   -value <new_value>
   ```

   where:

   <movername> = name of the specified.

   <new_value> = string that specifies the new cipher value. If the value includes any special characters (such as a semi-colon, space character, or exclamation), it must be enclosed in quotation marks.

   Note: The default cipher suite value is ALL:!ADH:!SSLv2:@STRENGTH, which means that VNX for file supports all ciphers except the SSLv2, Anonymous Diffie-Hellman, and NULL ciphers, sorted by their “strength”, that is, the size of the encryption key.

   Parameter and facility names are case-sensitive.

   Example:

   To change the default SSL cipher suite to a strong cipher (mainly AES128 and AES256) to be used by each new SSL connection, type:

   ```
   $ server_param server_2 -facility ssl -modify cipher -value
   'HIGH:@STRENGTH'
   ```

   Output:

   ```
   server_2 : done
   ```

Postrequisites

After changing SSL parameter values, you must reboot the Data Mover for a SSL protocol and cipher suite change to take effect.

Configuring PKI

Planning considerations for Public Key Infrastructure provides a general description of this feature.

Creating the certificate provided by the persona

The procedure for creating the certificate provided by the persona to the Data Mover or Control Station varies slightly depending on whether the Certificate Authority (CA) that signs the certificate is an external CA or the Control Station:

1. Generate a key set and certificate request
2. Send the certificate request to the CA (not required if using the Control Station)
3. Import a CA-signed certificate (not required if using the Control Station)

Using the Control Station as the CA

The procedure for using the Control Station as the CA includes the following tasks:

1. Generate a new Control Station CA certificate
2. Display the certificate
3. Distribute the Control Station CA certificate

Note: The Control Station continues to generate a separate key set for the SSL-based connection between the Apache web server (on behalf of Unisphere) and a user's web browser. However, the Control Station now uses the CA key set to sign the Apache web server's certificate, meaning the certificate is no longer self-signed. *Installing Management Applications on VNX for File* describes how to manage certificates for Unisphere.

Obtaining CA certificates

The procedure for obtaining the CA certificates used to confirm the identity of a server includes the following tasks:

1. List the available CA certificates
2. Acquire a CA certificate
3. Import a CA certificate

Generate a key set and certificate request

To create the certificate provided by the persona to the Data Mover, you first generate the persona's public/private key set with a request for a CA to sign the certificate. The CA can be an external CA or the Control Station.

Create a certificate signed by an external CA

About this task

Procedure

1. To generate a key set and request for a certificate to be signed by an external CA, use this command syntax:

   ```
   $ server_certificate <movername> -persona -generate
   {<persona_name>| id=<persona_id>} -key_size <bits>
   {-cn|-common_name} <common_name>
   ```

   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

<persona_id> = ID of the persona. The ID is generated when the persona is created. You can determine the ID through the -persona -list command.

<bits> = key size, either 2048 or 4096 bits.

<common_name> = commonly used name, typically a hostname that describes the Data Mover with which the persona is associated. If the name includes any special characters (such as a semi-colon, space character, or exclamation), it must be enclosed in quotation marks.

Note: Certificate requests are generated in PEM format only.

Example:

To generate a key set and request for a certificate to be signed by an external CA, type:

$ server_certificate server_2 -persona -generate default -key_size 4096 -cn 'name;1.2.3.4'

Output:

```
server_2 :
Starting key generation. This could take a long time ...
done
```

Create a certificate signed by the Control Station

About this task

If you are using the Control Station to sign the certificate, you must specify the number of months the certificate is valid.

Procedure

1. To generate a key set and request for a certificate to be signed by the Control Station, use this command syntax:

   ```
   $ server_certificate <movername> -persona -generate
   {<persona_name>|id=<persona_id>} -key_size <bits>
   -cs_sign_duration <# of months>{-cn|-common_name} <common_name>
   ```

   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

   <persona_id> = ID of the persona. The ID is generated when the persona is created. You can determine the ID through the -persona -list command.

   <bits> = key size, either 2048 or 4096 bits.

   <# of months> = number of months the certificate is valid.

   <common_name> = commonly used name, typically a hostname that describes the Data Mover with which the persona is associated. If the name includes any special characters (such as a semi-colon, space character, or exclamation), it must be enclosed in quotation marks.

   Note: Certificate requests are generated in PEM format only.

   Example:

   To generate a key set and request for a certificate to be signed by the Control Station, type:

```
$ server_certificate server_2 -persona -generate default -key_size 4096 -
cs_sign_duration 13 -cn 'name;1.2.3.4'
```

Output:

```
server_2 :
Starting key generation. This could take a long time ...
done
```

Create a certificate specifying detailed information about the persona

About this task

When you generate the persona's public/private key set and certificate request, you can specify detailed information about the Data Mover. Typically this information includes details such as the organization that uses the Data Mover and where it is located. In addition, you have the option of saving the certificate request to a specific file.

Procedure

1. To generate a key set and request for a certificate signed by an external CA, specifying detailed information about the Data Mover and saving the certificate request to a specific file, use this command syntax:

   ```
   $ server_certificate <movername> -persona -generate
   {<persona_name>|id=<persona_id>} -key_size <bits>
   {-cn|-common_name} <common_name> -ou <org_unit>
   -organization <organization> -location <location>
   -state <state> -country <country> -filename <output_path>
   ```

   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

   <persona_id> = ID of the persona. The ID is generated when the persona is created. You can determine the ID through the -persona -list command.

   <bits> = key size, either 2048 or 4096 bits.

   <common_name> = commonly used name, typically a hostname that describes the Data Mover with which the persona is associated. If the name includes any special characters (such as a semi-colon, space character, or exclamation), it must be enclosed in quotation marks.

   <org_unit> = name of the organizational unit. If the name includes any special characters (such as a semi-colon, space character, or exclamation), it must be enclosed in quotation marks.

   <organization> = name of the organization.

   <location> = physical location of the organization.

   <state> = state where the organization is located.

   <country> = country where the organization is located.

   <output_path> = name and path where the generated request are written.

   Note: The -ou, -organization, -location, -state, and -country arguments are optional.

   Note: The -filename argument is only valid if the certificate will be signed by an external CA.

Note: Certificate requests are generated in PEM format only.

Example:

To generate a key set and request for a certificate signed by an external CA, specifying detailed information about the Data Mover and saving the certificate request to a specific file, type:

$ server_certificate server_2 -persona -generate default -key_size 4096 -cn 'name;1.2.3.4' -ou 'my.org;my dept' -organization EMC -location Hopkinton -state MA -country US -filename /tmp/server_2.1.request.pem

Output:

```
server_2 :
Starting key generation. This could take a long time ...
done
```

Send the certificate request to the CA

About this task

If you are using an external CA to sign the certificate, a request to sign the public key is automatically generated along with the public/private key set. You must then send the certificate request to the CA.

Note: This task is not required if you are using the Control Station to sign the certificate. The Control Station automatically receives the certificate request.

Procedure

1. Display the persona's properties to verify the content of the certificate request by using this command syntax:

   ```
   $ server_certificate<movername>-persona -info{-all| <persona_name>|
   id=<persona_id>}
   ```
   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

   <persona_id> = ID of the persona. The ID is generated when the persona is created.

   Example:

   To display the properties for the default persona, including the certificate request, type:

   $ server_certificate server_2 -persona -info default

   Output:

   ```
   server_2 :
   id=1
   name=default
   next state=Request Pending
   next certificate:
   request subject = CN=name;CN=1.2.3.4
   request:
   -----BEGIN CERTIFICATE REQUEST-----
   MIIB6TCCAVICAQYwDQYJKoZIhvcNAQEEBQAwWzELMAkGA1UEBhMCQVUxEzARBgNV
   BAgTClF1ZWVuc2xhbmQxGjAYBgNVBAoTEUNyeXB0U29mdCBQdHkgTHRkMRswGQYD
   VQQDExJUZXN0IENBICgxMDI0IGJpdCkwHhcNMDAxMDE2MjIzMTAzWhcNMDMwMTE0
   MjIzMTAzWjBjMQswCQYDVQQGEwJBVTETMBEGA1UECBMKUXVlZW5zbGFuZDEaMBgG
   ```

```
A1UEChMRQ3J5cHRTb2Z0IFB0eSBMdGQxIzAhBgNVBAMTGlNlcnZlciB0ZXN0IGNl
cnQgKDUxMiBiaXQpMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJ+zw4Qnlf8SMVIP
Fe9GEcStgOY2Ww/dgNdhjeD8ckUJNP5VZkVDTGiXav6ooKXfX3j/7tdkuD8Ey2//
Kv7+ue0CAwEAATANBgkqhkiG9w0BAQQFAAOBgQCT0grFQeZaqYb5EYfk20XixZV4
GmyAbXMftG1Eo7qGiMhYzRwGNWxEYojf5PZkYZXvSqZ/ZXHXa4g59jK/rJNnaVGM
k+xIX8mxQvlV0n5O9PIha5BX5teZnkHKgL8aKKLKW1BK7YTngsfSzzaeame5iKfz
itAE+OjGF+PFKbwX8Q==
-----END CERTIFICATE REQUEST-----
```

2. If you have not already done so, save the certificate request to a file (for example, server_2.1.request.pem).
3. Send the .pem file to the CA using that company's website or email.

Import a CA-signed certificate

About this task

You can import a signed certificate when the next signed certificate associated with the persona is available for download. As soon as the certificate is imported, it becomes the current certificate (assuming that the date is valid).

Note: This task is not required if you are using the Control Station to sign the certificate. The Control Station automatically returns the signed certificate to the Data Mover.

Procedure

1. Obtain the signed certificate (for example, cert.pem) from the CA.
2. Query all Data Movers to determine which personas are waiting for a signed certificate:

   ```
   $ server_certificate ALL -persona -list
   ```

   Output:

   ```
   server_2 :
   id=1
   name=default
   next state=Request Pending
   request subject = CN=name;CN=1.2.3.4
   server_3 :
   id=1
   name=default
   next state=Request Pending
   request subject = CN=test;CN=5.6.7.8
   ```

3. To determine to which persona to import the certificate, match the certificate's subject with the value of the Request Subject field for those personas whose Next State is Request Pending.
4. Import the signed certificate to the waiting persona by using this command syntax:

   ```
   $ server_certificate <movername> -persona -import {<persona_name>|
   id=<persona_id>}
   ```

   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

   <persona_id> = ID of the persona. The ID is generated when the persona is created.

   Note: The signed certificate can be in either DER or PEM format. You can only paste text in PEM format at the command prompt. If you specify -filename and provide a path, you can import a CA-signed certificate in either DER or PEM format.

Example:

To import the signed certificate, type:

$ server_certificate server_2 -persona -import default

Output:

```
server_2 : Please paste certificate data. Enter a carriage
return and on the new line type 'end of file' or 'eof'
followed by another carriage return.
```

Note: After the certificate text is pasted correctly, the system prompt is displayed.

5. Verify that the certificate has been imported successfully by using this command syntax:

   `$ server_certificate<movername>-persona -info{-all| <persona_name>| id=<persona_id>}`

   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

   <persona_id> = ID of the persona. The ID is generated when the persona is created.

   Example:

   To verify that the certificate for the default persona has been imported successfully, type:

   $ server_certificate server_2 -persona -info default

   Output:

```
server_2
id=1
name=default
next state=Not Available
Current Certificate:
  id              = 1
  subject         = CN=name;CN=1.2.3.4
  issuer          = O=Celerra Certificate Authority;CN=eng173100
  start date      = 20070606183824Z
  end date        = 20070706183824Z
  serial number   = 05
  signature alg.  = sha1WithRSAEncryption
  public key alg. = rsaEncryption
  public key size = 4096
  version         = 3
```

Note: Typically, after a certificate is imported, it immediately becomes the current key set and certificate, and the Next State field is shown as Not Available. If the imported certificate is not valid (for example, its time stamp is several minutes or more ahead of the Data Mover), the imported key set and certificate remain the next key set and certificate, and the Next State field is shown as Available until such time as the key set and certificate become valid.

List the available CA certificates

About this task

Procedure

1. To display all the available CA certificates, type:

$ **server_certificate ALL -ca_certificate -list**

Output:

```
server_2 :
id=1
subject=C=ZA;ST=Western Cape;L=Cape Town;O=Thawte Consulting
cc;OU=Certific
issuer=C=ZA;ST=Western Cape;L=Cape Town;O=Thawte Consulting
cc;OU=Certifica
expire=20201231235959Z

id=2
subject=C=US;O=America Online Inc.;CN=America Online Root
Certification Aut
issuer=C=US;O=America Online Inc.;CN=America Online Root
Certification Auth
expire=20371119204300Z

id=3
subject=C=US;ST=Massachusetts;L=Westboro;O=EMC;OU=IS;OU=Terms
of use at www
issuer=O=VeriSign Trust Network;OU=VeriSign, Inc.;OU=VeriSign
International
expire=20080620235959Z

id=4
subject=C=US;O=VeriSign,Inc.;OU=Class 3 Public Primary Certification
Author
issuer=C=US;O=VeriSign, Inc.;OU=Class 3 Public Primary Certification
Author
expire=20280801235959Z
```

Acquire a CA certificate

About this task

If a new CA certificate is required and an external CA is being used, you can obtain the CA certificate from the company's website or possibly from the person in your company responsible for security. If the CA is the Control Station (enterprise-level or inhouse), you can obtain the CA certificate from the person who manages the CA. Alternatively, you can display the text of the CA certificate through the nas_ca_certificate -display command.

Procedure

1. To display the Control Station's CA certificate, type:

   $ **/nas/sbin/nas_ca_certificate -display**

   Note: The certificate text is displayed on the terminal screen. Alternatively, you can redirect it to a file. The certificate text is enclosed by BEGIN CERTIFICATE and END CERTIFICATE.

   Output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: O=Celerra Certificate Authority, CN=eng173100
        Validity
            Not Before: Mar 23 21:07:40 2007 GMT
            Not After : Mar 21 21:07:40 2012 GMT
```

```
        Subject: O=Celerra Certificate Authority, CN=eng173100
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:da:b2:37:86:05:a3:73:d5:9a:04:ba:db:05:97:
                    d2:12:fe:1a:79:06:19:eb:c7:2c:c2:51:93:7f:7a:
                    93:59:37:63:1e:53:b3:8d:d2:7f:f0:e3:49:42:22:
                    f4:26:9b:b4:e4:a6:40:6d:8d:e7:ea:07:8e:ca:b7:
                    7e:88:71:9d:11:27:5a:e3:57:16:03:a7:ee:19:25:
                    07:d9:42:17:b4:eb:e6:97:61:13:54:62:03:ec:93:
                    b7:e6:f1:7f:21:f0:71:2d:c4:8a:8f:20:d1:ab:5a:
                    6a:6c:f1:f6:2f:26:8c:39:32:93:93:67:bb:03:a7:
                    22:29:00:11:e0:a1:12:4b:02:79:fb:0f:fc:54:90:
                    30:65:cd:ea:e6:84:cc:91:fe:21:9c:c1:91:f3:17:
                    1e:44:7b:6f:23:e9:17:63:88:92:ea:80:a5:ca:38:
                    9a:b3:f8:08:cb:32:16:56:8b:c4:f7:54:ef:75:db:
                    36:7e:cf:ef:75:44:11:69:bf:7c:06:97:d1:87:ff:
                    5f:22:b5:ad:c3:94:a5:f8:a7:69:21:60:5a:04:5e:
                    00:15:04:77:47:03:ec:c5:7a:a2:bf:32:0e:4d:d8:
                    dc:44:fa:26:39:16:84:a7:1f:11:ef:a3:37:39:a6:
                    35:b1:e9:a8:aa:a8:4a:72:8a:b8:c4:bf:04:70:12:
                    b3:31
                Exponent: 65537 (0x10001)

X509v3 extensions:
            X509v3 Subject Key Identifier:
            35:06:F2:FE:CC:21:4B:92:DA:74:C9:47:CE:BB:37:21:5E:04:E2:E6
            X509v3 Authority Key Identifier:
keyid:35:06:F2:FE:CC:21:4B:92:DA:74:C9:47:CE:BB:37:21:5E:04:E2:E6
            DirName:/O=Celerra Certificate Authority/CN=eng173100
            serial:00
X509v3 Basic Constraints:
            CA:TRUE
            X509v3 Subject Alternative Name:
            DNS:eng173100
Signature Algorithm: sha1WithRSAEncryption
        09:c3:13:26:16:be:44:56:82:5d:0e:63:07:19:28:f3:6a:c4:
        f3:bf:93:25:85:c3:55:48:4e:07:84:1d:ea:18:cf:8b:b8:2d:
        54:13:25:2f:c9:75:c1:28:39:88:91:04:df:47:2c:c0:8f:a4:
        ba:a6:cd:aa:59:8a:33:7d:55:29:aa:23:59:ab:be:1d:57:f6:
        20:e7:2b:68:98:f2:5d:ed:58:31:d5:62:85:5d:6a:3f:6d:2b:
        2d:f3:41:be:97:3f:cf:05:8b:7e:f5:d7:e8:7c:66:b2:ea:ed:
        58:d4:f0:1c:91:d8:80:af:3c:ff:14:b6:e7:51:73:bb:64:84:
        26:95:67:c6:60:32:67:c1:f7:66:f4:79:b5:5d:32:33:3c:00:
        8c:75:7d:02:06:d3:1a:4e:18:0b:86:78:24:37:18:20:31:61:
        59:dd:78:1f:88:f8:38:a0:f4:25:2e:c8:85:4f:ce:8a:88:f4:
        4f:12:7e:ee:84:52:b4:91:fe:ff:07:6c:32:ca:41:d0:a6:c0:
        9d:8f:cc:e8:74:ee:ab:f3:a5:b9:ad:bb:d7:79:67:89:34:52:
        b4:6b:39:db:83:27:43:84:c3:c3:ca:cd:b2:0c:1d:f5:20:de:
        7a:dc:f0:1f:fc:70:5b:71:bf:e3:14:31:4c:7e:eb:b5:11:9c:
        96:bf:fe:6f

-----BEGIN CERTIFICATE-----
MIIDoDCCAoigAwIBAgIBAzANBgkqhkiG9w0BAQUFADA8MSYwJAYDVQQKEx1DZWxl
cnJhIENlcnRpZmljYXRlIEF1dGhvcml0eTESMBAGA1UEAxMJZW5nMTczMTAwMB4X
DTA3MDMyMzIxMDc0MFoXDTEyMDMyMTIxMDc0MFowPDEmMCQGA1UEChMdQ2VsZXJy
YSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxEjAQBgNVBAMTCWVuZzE3MzEwMDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANqyN4YFo3PVmgS62wWX0hL+GnkG
GevHLMJRk396k1k3Yx5Ts43Sf/DjSUIi9CabtOSmQG2N5+oHjsq3fohxnREnWuNX
FgOn7hklB9lCF7Tr5pdhE1RiA+yTt+bxfyHwcS3Eio8g0ataamzx9i8mjDkyk5Nn
uwOnIikAEeChEksCefsP/FSQMGXN6uaEzJH+IZzBkfMXHkR7byPpF2OIkuqApco4
mrP4CMsyFlaLxPdU73XbNn7P73VEEWm/fAaX0Yf/XyK1rcOUpfinaSFgWgReABUE
d0cD7MV6or8yDk3Y3ET6JjkWhKcfEe+jNzmmNbHpqKqoSnKKuMS/BHASszECAwEA
AaOBrDCBqTAdBgNVHQ4EFgQUNQby/swhS5LadMlHzrs3IV4E4uYwZAYDVR0jBF0w
W4AUNQby/swhS5LadMlHzrs3IV4E4uahQKQ+MDwxJjAkBgNVBAoTHUNlbGVycmEg
Q2VydGlmaWNhdGUgQXV0aG9yaXR5MRIwEAYDVQQDEwllbmcxNzMxMDCCAQAwDAYD
VR0TBAUwAwEB/zAUBgNVHREEDTALggllbmcxNzMxMDAwDQYJKoZIhvcNAQEFBQAD
ggEBAAnDEyYWvkRWgl0OYwcZKPNqxPO/kyWFw1VITgeEHeoYz4u4LVQTJS/JdcEo
```

```
OYiRBN9HLMCPpLqmzapZijN9VSmqI1mrvh1X9iDnK2iY8l3tWDHVYoVdaj9tKy3z
Qb6XP88Fi3711+h8ZrLq7VjU8ByR2ICvPP8UtudRc7tkhCaVZ8ZgMmfB92b0ebVd
MjM8AIx1fQIG0xpOGAuGeCQ3GCAxYVndeB+I+Dig9CUuyIVPzoqI9E8Sfu6EUrSR
/v8HbDLKQdCmwJ2PzOh07qvzpbmtu9d5Z4k0UrRrOduDJ0OEw8PKzbIMHfUg3nrc
8B/8cFtxv+MUMUx+67URnJa//m8=
-----END CERTIFICATE-----
```

Import a CA certificate

About this task

To make the CA certificate known to the Data Movers, you must import it. You can provide a path and import a file or cut and paste the text.

Procedure

1. To import a CA certificate, use this command syntax:

   ```
   $ server_certificate <movername> -ca_certificate
   -import [-filename<path>]
   ```

   where:

   <movername> = name of the physical Data Mover with which the CA certificate is associated

   <path> = location of the file to be imported

   Note: The CA certificate can be in either DER or PEM format. You can only paste text in PEM format at the command prompt. If you specify -filename and provide a path, you can import a CA certificate in either DER or PEM format.

   Example:

   To import a CA certificate, type:

   $ server_certificate server_2 -ca_certificate -import

   Output:

   ```
   server_2 : Please paste certificate data. Enter a carriage
   return and on the new line type 'end of file' or 'eof'
   followed by another carriage return.
   ```

2. After the certificate text is pasted correctly, the system prompt is displayed.

Generate a new Control Station CA certificate

About this task

Note: This task is required only if the CA key set has been compromised or the CA certificate expires. The initial Control Station CA certificate is generated during a VNX for file software installation or upgrade.

You must be the root user to issue this command.

Procedure

1. To generate a new key set and certificate for the Control Station, type:

   # /nas/sbin/nas_ca_certificate -generate

   Note: By default, this certificate is valid for 5 years from the date it is generated and the certificate's name is the Control Station's hostname.

Output:

```
New keys and certificate were successfully generated.
```

Display the certificate

About this task

Display the text of the Control Station CA certificate so you can copy it for distribution to network clients.

Procedure

1. To display the Control Station's CA certificate, type:

   $ **/nas/sbin/nas_ca_certificate -display**

   Note: The certificate text is displayed on the terminal screen. Alternatively, you can redirect it to a file.

   Output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: O=Celerra Certificate Authority, CN=eng173100
        Validity
            Not Before: Mar 23 21:07:40 2007 GMT
            Not After : Mar 21 21:07:40 2012 GMT
        Subject: O=Celerra Certificate Authority, CN=eng173100
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:da:b2:37:86:05:a3:73:d5:9a:04:ba:db:05:97:
                    d2:12:fe:1a:79:06:19:eb:c7:2c:c2:51:93:7f:7a:
                    93:59:37:63:1e:53:b3:8d:d2:7f:f0:e3:49:42:22:
                    f4:26:9b:b4:e4:a6:40:6d:8d:e7:ea:07:8e:ca:b7:
                    7e:88:71:9d:11:27:5a:e3:57:16:03:a7:ee:19:25:
                    07:d9:42:17:b4:eb:e6:97:61:13:54:62:03:ec:93:
                    b7:e6:f1:7f:21:f0:71:2d:c4:8a:8f:20:d1:ab:5a:
                    6a:6c:f1:f6:2f:26:8c:39:32:93:93:67:bb:03:a7:
                    22:29:00:11:e0:a1:12:4b:02:79:fb:0f:fc:54:90:
                    30:65:cd:ea:e6:84:cc:91:fe:21:9c:c1:91:f3:17:
                    1e:44:7b:6f:23:e9:17:63:88:92:ea:80:a5:ca:38:
                    9a:b3:f8:08:cb:32:16:56:8b:c4:f7:54:ef:75:db:
                    36:7e:cf:ef:75:44:11:69:bf:7c:06:97:d1:87:ff:
                    5f:22:b5:ad:c3:94:a5:f8:a7:69:21:60:5a:04:5e:
                    00:15:04:77:47:03:ec:c5:7a:a2:bf:32:0e:4d:d8:
                    dc:44:fa:26:39:16:84:a7:1f:11:ef:a3:37:39:a6:
                    35:b1:e9:a8:aa:a8:4a:72:8a:b8:c4:bf:04:70:12:
                    b3:31
                Exponent: 65537 (0x10001)

X509v3 extensions:
            X509v3 Subject Key Identifier:
            35:06:F2:FE:CC:21:4B:92:DA:74:C9:47:CE:BB:37:21:5E:04:E2:E6
            X509v3 Authority Key Identifier:
keyid:35:06:F2:FE:CC:21:4B:92:DA:74:C9:47:CE:BB:37:21:5E:04:E2:E6
            DirName:/O=Celerra Certificate Authority/CN=eng173100
            serial:00
X509v3 Basic Constraints:
            CA:TRUE
            X509v3 Subject Alternative Name:
            DNS:eng173100
```

```
Signature Algorithm: sha1WithRSAEncryption
        09:c3:13:26:16:be:44:56:82:5d:0e:63:07:19:28:f3:6a:c4:
        f3:bf:93:25:85:c3:55:48:4e:07:84:1d:ea:18:cf:8b:b8:2d:
        54:13:25:2f:c9:75:c1:28:39:88:91:04:df:47:2c:c0:8f:a4:
        ba:a6:cd:aa:59:8a:33:7d:55:29:aa:23:59:ab:be:1d:57:f6:
        20:e7:2b:68:98:f2:5d:ed:58:31:d5:62:85:5d:6a:3f:6d:2b:
        2d:f3:41:be:97:3f:cf:05:8b:7e:f5:d7:e8:7c:66:b2:ea:ed:
        58:d4:f0:1c:91:d8:80:af:3c:ff:14:b6:e7:51:73:bb:64:84:
        26:95:67:c6:60:32:67:c1:f7:66:f4:79:b5:5d:32:33:3c:00:
        8c:75:7d:02:06:d3:1a:4e:18:0b:86:78:24:37:18:20:31:61:
        59:dd:78:1f:88:f8:38:a0:f4:25:2e:c8:85:4f:ce:8a:88:f4:
        4f:12:7e:ee:84:52:b4:91:fe:ff:07:6c:32:ca:41:d0:a6:c0:
        9d:8f:cc:e8:74:ee:ab:f3:a5:b9:ad:bb:d7:79:67:89:34:52:
        b4:6b:39:db:83:27:43:84:c3:c3:ca:cd:b2:0c:1d:f5:20:de:
        7a:dc:f0:1f:fc:70:5b:71:bf:e3:14:31:4c:7e:eb:b5:11:9c:
        96:bf:fe:6f

-----BEGIN CERTIFICATE-----
MIIDoDCCAoigAwIBAgIBAzANBgkqhkiG9w0BAQUFADA8MSYwJAYDVQQKEx1DZWxl
cnJhIENlcnRpZmljYXRlIEF1dGhvcml0eTESMBAGA1UEAxMJZW5nMTczMTAwMB4X
DTA3MDMyMzIxMDc0MFoXDTEyMDMyMTIxMDc0MFowPDEmMCQGA1UEChMdQ2VsZXJy
YSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxEjAQBgNVBAMTCWVuZzE3MzEwMDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANqyN4YFo3PVmgS62wWX0hL+GnkG
GevHLMJRk396k1k3Yx5Ts43Sf/DjSUIi9CabtOSmQG2N5+oHjsq3fohxnREnWuNX
FgOn7hklB9lCF7Tr5pdhE1RiA+yTt+bxfyHwcS3Eio8g0ataamzx9i8mjDkyk5Nn
uwOnIikAEeChEksCefsP/FSQMGXN6uaEzJH+IZzBkfMXHkR7byPpF2OIkuqApco4
mrP4CMsyFlaLxPdU73XbNn7P73VEEWm/fAaX0Yf/XyK1rcOUpfinaSFgWgReABUE
d0cD7MV6or8yDk3Y3ET6JjkWhKcfEe+jNzmmNbHpqKqoSnKKuMS/BHASszECAwEA
AaOBrDCBqTAdBgNVHQ4EFgQUNQby/swhS5LadMlHzrs3IV4E4uYwZAYDVR0jBF0w
W4AUNQby/swhS5LadMlHzrs3IV4E4uahQKQ+MDwxJjAkBgNVBAoTHUNlbGVycmEg
Q2VydGlmaWNhdGUgQXV0aG9yaXR5MRIwEAYDVQQDEwllbmcxNzMxMDCCAQAwDAYD
VR0TBAUwAwEB/zAUBgNVHREEDTALgglbmcxNzMxMDAwDQYJKoZIhvcNAQEFBQAD
ggEBAAnDEyYWvkRWgl0OYwcZKPNqxPO/kyWFw1VITgeEHeoYz4u4LVQTJS/JdcEo
OYiRBN9HLMCPpLqmzapZijN9VSmqI1mrvh1X9iDnK2iY8l3tWDHVYoVdaj9tKy3z
Qb6XP88Fi3711+h8ZrLq7VjU8ByR2ICvPP8UtudRc7tkhCaVZ8ZgMmfB92b0ebVd
MjM8AIx1fQIG0xpOGAuGeCQ3GCAxYVndeB+I+Dig9CUuyIVPzoqI9E8Sfu6EUrSR
/v8HbDLKQdCmwJ2PzOh07qvzpbmtu9d5Z4k0UrRrOduDJ0OEw8PKzbIMHfUg3nrc
8B/8cFtxv+MUMUx+67URnJa//m8=
-----END CERTIFICATE-----
```

Distribute the Control Station CA certificate

About this task

You must make the Control Station CA certificate available so it can be imported by network clients and used to recognize certificates sent by Data Movers signed by this Control Station.

1. Save the Control Station CA certificate text to a file (for example, cs_ca_cert.crt).
2. Make this .crt file available to network clients through an appropriate mechanism (FTP or email).
3. Regenerate a new key set and certificate request and import a signed certificate for any personas whose certificates are signed by the Control Station. Creating the certificate provided by the persona describes this procedure.
4. If a Data Mover is a client to another Data Mover, import the new CA certificate to the appropriate Data Mover. Obtaining CA certificates describes this procedure.

Request and Install Customer-Supplied Certificates for Control Station

About this task

By default, the Control Station utilizes 1024-bit encrypted certificate keys. 2048-bit encrypted certificate keys are used in the consideration of security at a higher level. The following example enables you to request and install a 2048-bit encrypted custom certificate on a VNX system with two Control Stations. You must run the following commands as user root.

Procedure

1. Create a new 2048-bit encrypted key.

   ```
   /usr/bin/openssl genrsa -out /nas/http/conf/ssl.key/ssl_2048_key
   2048
   ```

2. Ensure the key file is owned by user root and has permissions set to 600 (-rw-------):

   ```
   chown root:root <filename>
   ```

   ```
   chmod 600 <filename>
   ```

3. Update the symbolic link of the current key to the new key:

   ```
   rm -f /nas/http/conf/current.key
   ```

   ```
   ln -s /nas/http/conf/ssl.key/ssl_2048_key /nas/http/conf/
   current.key
   ```

4. Set the environment variables:

   ```
   export IP_ADDR=`/bin/hostname -i`
   ```

   ```
   export HOSTNAME_SHORT=`/bin/hostname -s`
   ```

   ```
   export HOSTNAME_LONG=`/bin/hostname -f`
   ```

5. Create a certificate request using the new 2048-bit encrypted key and the environment variables:

   ```
   /usr/bin/openssl req -new -key /nas/http/conf/current.key -config
   ```

   ```
   /nas/http/conf/celerrassl.cnf -out /home/nasadmin/cert_request
   ```

   Output (based on running cat command on file):

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIICzTCCAbUCAQAwgYcxKjAoBgNVBAoTIVZOWCBDb250cm9sIFN0YXRpb24gQWRt
   aW5pc3RyYXRvcjEXMBUGA1UEAxMOMTAuMTA4LjEyNS4xMDgxFzAVBgNVBAMTDmZp
   bGVzaW04MTYyY3MwMScwJQYDVQQDEx5maWxlc2ltODE2MmNzMC5kcm0ubGFiLmVt
   Yy5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJSXomphOnn8cg
   PxL/YHUzWF8IDyp8Teee3zdvYa5sScsp76eO9oxKKb6/B+ihYSgctSApF2d5ciO+
   P3Oe0HtU+YrVcjxbMT9I004PSDFJBum7Fhw/byvbrBVxNjOmjAt+8Wbdbi/3gIOv
   bSUG1j/x8UuBwMuy/C6K8Ojiz3OoatQkgn6qmqLN8S4CL/SD2eqD0sikvaubvVSX
   gA85V4fH95ZpshptKRx4e+0hLkIOdDVnn69u/Jdz2lFZ8XPp4CTv66FP/GOzWowB
   iPBLxNfs6PLWNhR4u/X1K2Wtb+cTVmjUGsJEPel2flzf3GmQtGChHAU1f5+mR08Q
   jRX0ACnFAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAl7IMNtFCLRaWbLv5mdkI
   6/mkHkwutkZJlMDgw4p1I86uJOZH6OHQsZRRM6ZfF42e+4cdz6qUmZKDmiHyiqPo
   Gh/DgYwIBNh3BVuPNdM/of4n4/ZZVcWmmQj84arjogfHnfeUV6uTWSWv82HvVEc6
   tyk9vYQ/MaOgvJ5c75KCpD+nmxDskVL97BuaondVKfCUR/ZT6q2N5pmlmPV6k7Jw
   g457pbBcYjaOqR3O6l8Fk4E5DgDwBAIfOmsCetqPklc+Dz7Fc3BLMbjqVhsC7gbh
   0a40Kn2sjEasenqpuoV7QNeawSTW4zCpFuD1H0i0vd+ZxyZy6z30ynMt5kLphMwb
   lA==
   -----END CERTIFICATE REQUEST-----
   ```

6. Submit the certificate text that is enclosed by `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` from the file `cert_request` to your local Certificate Authority:

   ```
   cat /home/nasadmin/cert_request
   ```

7. Upload or install the CA-signed certificate you received to the same location on both Control Stations, CS0 and CS1. For example, `/etc/httpd/conf`:

   ```
   [root@virgil conf]# ll /etc/httpd/conf/virgil*
   ```

   ```
   -rw-r--r-- 1 root root 1904 Dec 19 13:42 /etc/httpd/conf/virgil.cer
   ```

   ```
   -rw-r--r-- 1 root root 887 Dec 19 13:36 /etc/httpd/conf/virgil.key
   ```

This must be a base-64 encoded, PEM certificate. Also, ensure the public certificate is owned by user root and has permissions set to 644 (-rw-r--r--):

```
chown root:root <filename>

chmod 644 <filename>
```

8. Configure the Apache configuration file under `/nas/http/conf/httpd.conf`

   Load the custom certificate by modifying *SSLCertificateFile* and *SSLCertificateKeyFile* in `/nas/http/conf/httpd.conf`. Make it point to the custom crt file and key file, such as `/etc/httpd/conf/xxx.crt` and `xxx.key`:

```
[root@virgil conf]# grep ^SSLCe /nas/http/conf/httpd.conf

SSLCertificateFile /etc/httpd/conf/virgil.cer

SSLCertificateFile /etc/httpd/conf/virgil.cer
```

9. For a system with two Control Stations, copy the files in step 8 from the primary to the secondary Control Station:

```
[root@virgil /]# cd /etc/httpd/conf

[root@virgil conf]# scp virgil* emcnasotherIPMICS_i3:/etc/httpd/
conf

EMC VNX Control Station Linux release 3.0 (NAS 7.0.50)

root@emcnasotheripmics_i3's password:

virgil.cer 100% 1904 1.9KB/s 00:00

virgil.key 100% 887 0.9KB/s 00:00
```

10. On the secondary Control Station, mount the local NAS partition to a mount point and edit the httpd.conf file to specify the same SSLCertificateFile/SSLCertificateKeyFile pair as that on the primary:

```
[root@virgilcs1 /]# mount /dev/hda5 /mnt/source/

[root@virgilcs1 /]# vi /mnt/source/http/conf/httpd.conf

[root@virgilcs1 /]# grep ^SSLCe /mnt/source/http/conf/httpd.conf

SSLCertificateFile /etc/httpd/conf/virgil.cer

SSLCertificateKeyFile /etc/httpd/conf/virgil.key

[root@virgilcs1 conf]# ll /etc/httpd/conf

total 60

-rw-r--r-- 1 root root 33726 Jul 26 2011 httpd.conf

-rw-r--r-- 1 root root 12958 Jul 26 2011 magic

-rw-r--r-- 1 root root 1904 Jan 9 19:20 virgil.cer

-rw-r--r-- 1 root root 887 Jan 9 19:20 virgil.key

[root@virgilcs1 /]# umount /mnt/source/
```

11. Restart Apache on the primary Control Station (find the Apache process ID and then kill that process). Refer to the following example:

```
cat /nas/http/logs/start_apache.pid
```

```
3224

kill -9 3224
```

Note: In case of any problems related to the new certificate, run the following command to generate a new Control Station CA certificate to change back to a standard self-signed certificate: `/nas/sbin/nas_ca_certificate -generate`

Note: These instructions are provided for VNX users who need to use self-supplied certificates. There are no anticipated problems other than the potential issues listed below:

- If the server and key files are not stored in the `/nas/httpd/conf/` directory, they may not be available after a Control Station failover.
- The information used to identify the server and added to the certificate is solely the users' responsibility.

Managing PKI

Planning considerations for Public Key Infrastructure provides a general description of this feature.

The tasks to manage the persona key sets and certificates are:

- Display key set and certificate properties
- Check for expired key sets
- Clear key sets

The tasks to manage the CA Certificate are:

- Display CA certificate properties
- Check for expired CA certificates
- Delete CA certificates

Display key set and certificate properties

About this task

Procedure

1. To display the properties of a key set and certificate, use this command syntax:

   ```
   $ server_certificate<movername>-persona -info{-all| <persona_name>|
   id=<persona_id>}
   ```
   where:

   <movername> = name of the physical Data Mover with which the persona is associated.

   <persona_name> = name of the persona.

   <persona_id> = ID of the persona. The ID is generated when the persona is created.

   Example:

   To display the key set and certificate for the persona named default, type:

   ```
   $ server_certificate server_2 -persona -info default
   ```

Output:

```
server_2 :
     id=1
     name=default
     next state=Not Available
     CURRENT CERTIFICATE:
       id              = 1
       subject         = CN=test;CN=1.2.3.4
       issuer          = O=Celerra Certificate Authority;CN=eng173100
       start date      = 20070606183824Z
       end date        = 20070706183824Z
       serial number   = 05
       signature alg.  = sha1WithRSAEncryption
       public key alg. = rsaEncryption
       version         = 3
       public key size = 4096
```

Check for expired key sets

About this task

There is no automated way to check for expired key sets and certificates. Instead you must check for expired certificates by listing the personas and examining the expiration dates of the certificates associated with each persona.

Procedure

1. To list all the key sets and certificates that are currently available, type:

   $ **server_certificate ALL -persona -list**

   Output:

```
server_2 :
     id=1
     name=default
     next state=Request Pending
     request subject=CN=name;CN=1.2.3.4
server_3 :
     id=1
     name=default
     next state=Not Available
     CURRENT CERTIFICATE:
       id=1
       subject=CN=test;CN=1.2.3.4
       expire=20070608183824Z
       issuer=O=Celerra Certificate Authority;CN=eng173100
```

2. A current certificate's expiration date is listed in the Expire field. 20070608183824Z translates to Fri June 08 18:38:24 GMT 2007.

Clear key sets

About this task

You should clear a key set when it has expired, the service is not longer needed, or the certificate request will not be fulfilled. You can clear a persona's current key set and certificate, the next key set and certificate, or both.

Procedure

1. To clear a key set and the associated certificate, use this command syntax:

```
$ server_certificate <movername> -persona -clear
{<persona_name>|id=<persona_id>} {-next|-current|
-both}
```

where:

<movername> = name assigned to the physical Data Mover with which the persona is associated.

<persona_name> = name of the persona.

<persona_id> = ID of the persona. The ID is generated when the persona is created.

Example:

To clear both the current and next key set and certificate for the persona on server_2, type:

$ server_certificate server_2 -persona -clear default -both

Output:

```
server_2 : done
```

Display CA certificate properties

About this task

Procedure

1. To display the properties of a CA certificate, use this command syntax:

   ```
   $ server_certificate<movername>-ca_certificate -info{-all|
   <certificate_id>}
   ```
   where:

   <movername> = name of the physical Data Mover with which the CA certificate is associated.

   <certificate_id> = ID of the certificate.

   Note: Use the -all option to display the properties of all the CA certificates available to the Data Mover.

   Example:

   To display the properties of the CA certificate identified by certificate ID 2, type:

   $ server_certificate server_2 -ca_certificate -info 2

   Output:

   ```
   server_2 :
   id=2
   subject = C=US;O=VeriSign, Inc.;OU=Class 3 Public Primary
   Certification Authority
   issuer  = C=US;O=VeriSign, Inc.;OU=Class 3 Public Primary
   Certification Authority
   start   = 199601290000000Z
   expire  = 202808012359595Z
   signature alg.  = md2WithRSAEncryption
   public key alg. = rsaEncryption
   public key size = 2048 bits
   serial number   = 70ba e41d 10d9 2934 b638 ca7b 03cc babf
   version         = 1
   ```

Check for expired CA certificates

About this task

There is no automated way to check for expired CA certificates. Instead you must check for expired certificates by listing the CA certificates and examining the expiration dates.

Procedure

1. To list all the CA certificates that are currently available, type:

   $ **server_certificate ALL -ca_certificate -list**

   Output:

```
server_2 :
id=1
subject=O=Celerra Certificate Authority;CN=sorento
issuer=O=Celerra Certificate Authority;CN=sorento
expire=20120318032639Z
id=2
subject=C=US;O=VeriSign, Inc.;OU=Class 3 Public Primary
Certification Author
issuer=C=US;O=VeriSign, Inc.;OU=Class 3 Public Primary Certification
Author
expire=20280801235959Z

server_3 :
id=1
subject=O=Celerra Certificate Authority;CN=zeus-cs
issuer=O=Celerra Certificate Authority;CN=zeus-cs
expire=20120606181215Z
```

2. A certificate's expiration date is listed in the Expire field. 20120318032639Z translates to March 18 03:26:39 GMT 2012.

Delete CA certificates

About this task

You should delete a CA certificate when it has expired, been compromised, or is no longer needed for authenticating a server.

Procedure

1. To delete a CA certificate, use this command syntax:

   `$ server_certificate <movername> -ca_certificate -delete {-all|<certificate_id>}`

   where:

   <movername> = name of the physical Data Mover with which the CA certificate is associated.

   <certificate_id> = ID of the certificate. You can determine the ID through the `-ca_certificate -list` command.

   Note: Use the -all option to delete all the CA certificates available to the Data Mover.

   Example:

   To delete the CA certificate on server_2 identified by its ID number, type:

   $ **server_certificate server_2 -ca_certificate -delete 1**

Output:

```
server_2 : done
```

Customize a login banner

About this task

The /etc/issue file contains a login banner message or system identification, which appears before the login prompt. A login banner can be used for any informational purpose, but is most often used to warn users about unauthorized or improper use of the system.

1. Log in to the CLI with your username and password. You must have root privileges to access the /etc/issue file.
2. Edit the /etc/issue file using vi or another text editor.
   EMC suggests you add an extra carriage return at the end of the banner message.

   Use spaces, tabs, and carriage returns to format the message. In general, you should limit the size of the message to no more than a single screen.

   Note: Because the login banner appears with the login prompt, do not include any sensitive information in the banner message.
3. Log in to the CLI or Unisphere to view the login banner and verify your changes.

Note: You can also customize the login banner using **System (System Management tasks)** > **Control Station Properties**. You must have root privileges to access the Login Banner field. The *VNX Release Notes* describe how to log in to Unisphere as root.

Create a MOTD

About this task

The message of the day (MOTD) file, /etc/motd, is displayed after a user successfully logs in. It can be used for any informational purpose, but is particularly useful for sending messages that affect all users. The message might contain information about a server upgrade or an alert about an impending system shutdown. By default, this file is empty.

1. Log in to the CLI with your username and password. You must have root privileges to access the /etc/motd file.
2. Edit the /etc/motd file using vi or another text editor.
   EMC suggests you add an extra carriage return at the end of the banner message.

   Use spaces, tabs, and carriage returns to format the message. In general, you should limit the size of the message to no more than a single screen.
3. Log in to the CLI or Unisphere to display the MOTD and verify your changes.

Note: You can also customize the MOTD using the **System (System Management tasks)** > **Control Station Properties**. You must have root privileges to access the Message of the Day field.

Restrict anonymous root login

About this task

The term anonymous root login is used to indicate that the root user is allowed to login directly. When anonymous root login is restricted, to gain root privileges you must first log in as another user (nasadmin, for example) and then `su` to root. Restricting anonymous root login on the serial console and SSH enhances system security.

Procedure

1. Log in to the CLI with your username and password.

   You must have root privileges to access the /etc/securetty and the /etc/ssh/sshd_config files.

2. Edit the /etc/securetty file using vi or another text editor.

   Remove the **ttyS1** entry to restrict anonymous root login on the serial console.

3. Edit the /etc/ssh/sshd_config file using vi or another text editor.

   a. Un-comment the PermitRootLogin parameter and set the value to **no** to restrict anonymous root login using SSH.

   b. Restart the SSH daemon to re-read the configuration file.

      For example, **run: /etc/init.d/sshd restart**.

After you finish

Anonymous root access using SSH is required to complete a VNX OE for file upgrade. Set the value of the PermitRootLogin parameter back to yes and restart the SSH daemon before starting an upgrade.

Locking accounts after a specific number of failed logins

About this task

The pam_tally module can be used to help improve security on the system by locking a user account after a given number of failed logins. Follow this procedure if you want to lock user accounts after a specific number of failed logins and have them automatically unlocked after a period of time. Do not use this procedure if you need to implement a US DOD Security Technical Implementation Guide (STIG) configuration. For more information on implementing a STIG configuration refer to *EMC VNX Using nas_stig Utility on VNX Technical Notes P/N 300-013-819*.

Procedure

1. There are two lines that must be added to specific places in the `/etc/pam.d/system-auth` file to enable pam_tally. To restrict the user to <n> failed logins and unlock after <m> seconds add the line **auth required pam_tally.so per_user deny=<n> unlock_time=<m> onerr=fail** after the line **auth required pam_env.so** and add the line **account required pam_tally.so** after the line **account required pam_unix.so**.

Results

After the changes, the `/etc/pam.d/system-auth` file should look similar to the following file restricting users to three logins with a one hour unlock time.

```
auth  required pam_env.so
auth  required pam_tally.so per_user deny=3 unlock_time=3600
onerr=fail
auth  sufficient pam_unix.so nullok try_first_pass
auth  requisite pam_succeed_if.so uid >= 500 quiet
auth  required pam_deny.so

account required pam_unix.so
account required pam_tally.so
account sufficient pam_succeed_if.so uid < 500 quiet
account required pam_permit.so
```

```
password requisite pam_cracklib.so retry=3 lcredit=-0 dcredit=-1
minlen=8 difok=3 ucredit=-0 ocredit=-0
password sufficient pam_unix.so md5 shadow nullok try_first_pass
use_authtok
password required pam_deny.so

session optional pam_keyinit.so revoke
session required pam_limits.so
session [success=1 default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session required pam_unix.so
```

APPENDIX F

VNX for block SSL certificate import

This appendix describes how to upload SSL certificates to a VNX SP (with or without SHA2).

Topics include:

VNX for block SSL certificate requirements

Use one of the subsequent methods, Web browser or openssl, to do the following:

- Create a Certificate Request.
- Self sign or get a Certificate Authority (CA) to sign the certificate.
- Make a pkcs12 format including private key.
- Import the signed certificate to the Storage Processor (SP).

Ensure that the PKCS#12 file meets the following requirements:

- The PKCS#12 file must contain an X.509 certificate.
- The PKCS#12 file must contain the private key.
- The public/private keys must be an RSA key pair.
- The public RSA key must be at least 1024 bits long.
- The certificate's Common Name must be set to the SP's IP address. At least one of the common names must be set to the IP address or the host name of the storage system.
- The certificate must be FIPS-compliant if FIPS mode is enabled.
- The certificate must not have expired.
- The certificate must not be valid for more than 15 years

Adding or changing a Storage Processor SSL certificate using a Web browser

About this task

Note: For VNX for block, the interface for managing user certificates is found at: `https://<SP_IP_address>/setup`, which requires username and password authentication.

Procedure

1. Log in to the system as an administrator user like sysadmin using `https://<SP_IP_address>/setup`.

   NOTICE Do not select any local certificates on Windows PC if pop up appears.

2. Select **Manage SSL/TLS Certificate**.
3. Generate CSR (Certificate Signing Request)
4. Export (which will show basecode encoded data with - BEGIN and END) - copy the whole text
5. From outside the system, on a CA server, use the data copied (save it in a local file if necessary) to issue the certificate.
6. From outside the system, copy the certificate in PEM format, which will be viewable in Notepad with BEGIN and END lines, copy the whole text.
7. On the system, if not logged in to the system, repeat steps 1 and 2.
8. Click **Import the certificate** and paste the text copied in step 6, including BEGIN and END.

Adding or changing a Storage Processor SSL certificate using openssl

Before you begin

A system with openssl installed is required (easier on Linux including VNX control stations, which have openssl pre-installed, but can also be installed on any system including Windows).

Procedure

1. If this is new setup, create a private key. (Optional to set a passphrase for the key. If set, it is important to remember at later steps. In this example, emcemc is the passphrase used with server.key, specified in passin option.)

   Issue a command using the following syntax,

   ```
   openssl genrsa -des3 -out <server.key> 2048
   ```

2. To request a CSR (C=Country, ST=State, L=Location, O=Orginaisation, CN=CommonName - all are optional except the CN which must match the SP IP):

   Issue a command using the following syntax,

   ```
   openssl req -new -sha1 -key <server.key> -out <request.csr> -days
   <1825-5 years> -passin pass:emcemc -subj '/C=US/ST=Florida/L=Sarasota/
   O=MyCust/CN=10.0.0.1/'
   ```

3. When using an external CA, do the following, otherwise go to Step 4:

   a. Get the contents from request.csr certified by a CA.

   b. Have a copy of the CA signed certificate and go to step 6.

4. When using a self-signed certificate, do the following, otherwise go to Step 5:

   a. Issue a command using the following syntax, then go to step 6:

   ```
   openssl x509 -in <request.csr> -out <signed_cert.crt> -req -signkey
   server.key -days 1825
   ```

5. When using a private key obtained from a CA and sign. (This is a rare situation since a CA's private key usually will not be shared.)

   a. Issue a command using the following syntax, then go to step 6:

   ```
   openssl ca -cert <ca.cert> -keyfile <caprivate.key> -in <request.csr>
   -out <signed_cert.crt>
   ```

6. Pack the signed certificate and private key generated at step 1 (passout is for passphrase for the saved pfx file) using the following syntax:

   ```
   openssl pkcs12 -export -out <cert_with_key.pfx> -inkey server.key -in
   <signed_cert.crt> -passin pass:emcemc -passout
   pass:emcout
   ```

7. Import the PFX file on the Storage Processor using the following syntax:

```
# naviseccli -h <SP_IP> -user <admin_user> -scope 0 -password
<admin_password> security -pkcs12upload
-file <cert_with_key.pfx> -passphrase <emcout> -descert
```

If the above command reports any errors, corresponding action is required. Whole steps can be tried for SPB (and Control Station). For VNX Control Station, the certificate is stored in `/nas/http/conf/` - the private key without password should be in ssl.key and ssl.crt is the signed certificate.

Creating SHA2 certificate using openssl

Before you begin

A system with openssl installed is required (easier on Linux including VNX control stations, which have openssl pre-installed, but can also be installed on any system including Windows).

Procedure

1. To create a sha256 CSR, issue the following commands:

```
$ openssl genrsa -des3 -out pkey 2048
$ openssl req -new -sha256 -key pkey -out sha256.csr -days 1825 -passin
pass:emcin -subj '/CN=10.x.x.x/'
openssl req -in sha256.csr -noout -text |grep Algo
```

For the CSR, a template also can be used for openssl. The template file needs to created, such as the following example:

```
#cat mytemplate.txt
[req]
distinguished_name=req_distinguished_name
req_extensions = v3_req
[req_distinguished_name]
countryName=US
stateOrProvinceName=Florida
localityName=myCity
organizationName=MyCompany
commonName=10.20.16.252
[ v3_req ]
subjectKeyIdentifier=hash
subjectAltName= @alt_names
[alt_names]
DNS.1=vnxspa.domain.com
IP.1=10.0.0.1
```

To use this template file, the following command would be issued:

```
# openssl req -new -sha1 -key <server.key> -out <request.csr> -days
<1865> -config <mytemplate.txt> -passin
pass:emcemc
```

```
Public Key Algorithm: rsaEncryption
Signature Algorithm: sha256WithRSAEncryption
```

sha256.csr is the CSR, which can be sent to the CA for signing with sha2.

2. To create a sha256 self-signed certificate, issue the following command:

```
openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout
mykey -out certsha256.crt -subj "/CN=10.x.x.x"
```

This single line creates a new private key, mykey, and signs it with output file certsha256.crt with the sha256 algorithm.

The resulting certificate can be packaged in pfx format and imported on the SP using naviseccli.

INDEX

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X