EMC® VNX®

Release 31.5

Security Configuration Guide on VNX for Block

P/N 300-012-899

REV A01

July 14, 2011

This technical note contains information on these topics:

- Overview 2
- Security configuration settings 4
- Other security considerations 21
- Secure deployment and usage settings 23
- Secure maintenance 27
- Physical security controls 27
- Advanced management capabilities 28
- Special configurations 33
- What is affected by management network filtering 35
- Unisphere Management Suite white paper guide 36

Overview

This guide describes the Block security settings and features on the EMC® VNX ® storage systems. For File security settings and features, refer the *Security Configuration Guide on VNX for File* on Powerlink®.

This document also provides an overview of EMC Unisphere™, which is the unified management solution for VNX systems. It discusses security features available in different Unisphere products, and describes how to configure these features for optimum security. To get more information on Unisphere, refer to the white paper *EMC Unisphere: Unified Storage Management Solution* on Powerlink.

Unisphere Management Suite components

The Unisphere Management Suite provides the following products to help you manage VNX storage systems.

- **Unisphere** – This is one of the two main programs you use to configure, monitor, and manage VNX, CLARiiON and Celerra storage systems. Unisphere is a web-based GUI.
- **CLI -** CLI provides a command line interface; this is the other main program you use to manage VNX storage systems. Two different CLI products are available, one for Block storage and one for File storage.
- **Unisphere Service Manager (USM) –** This software allows you to update, install and maintain VNX storage system hardware and software as well as provide contact and storage system information to your service provider
- **Unisphere Host Agent** or **server utility –** These 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 Storage System Initialization Utility** – This optional software allows you to initialize Block-only VNX storage systems and network settings from a workstation.
- **VNX Installation Assistant (VIA) –** This software allows you to initialize Unified (Block and File) and File-only VNX storage systems and network settings from a workstation
- **SNMP management software –** This optional software allows you to monitor the state of VNX storage 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 storage systems. Many customers use this customer service software to allow EMC to help them configure and monitor their systems.
- **Unisphere Storage Management 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 Stations. This software can optionally be installed on Windows XP or Windows Server.

As shown in Figure 1, the various components communicate with the storage system both in band and out of band. In-band communication travels over the data connection to the storage system, while out-of-band communication travels over the management connection to the storage system.

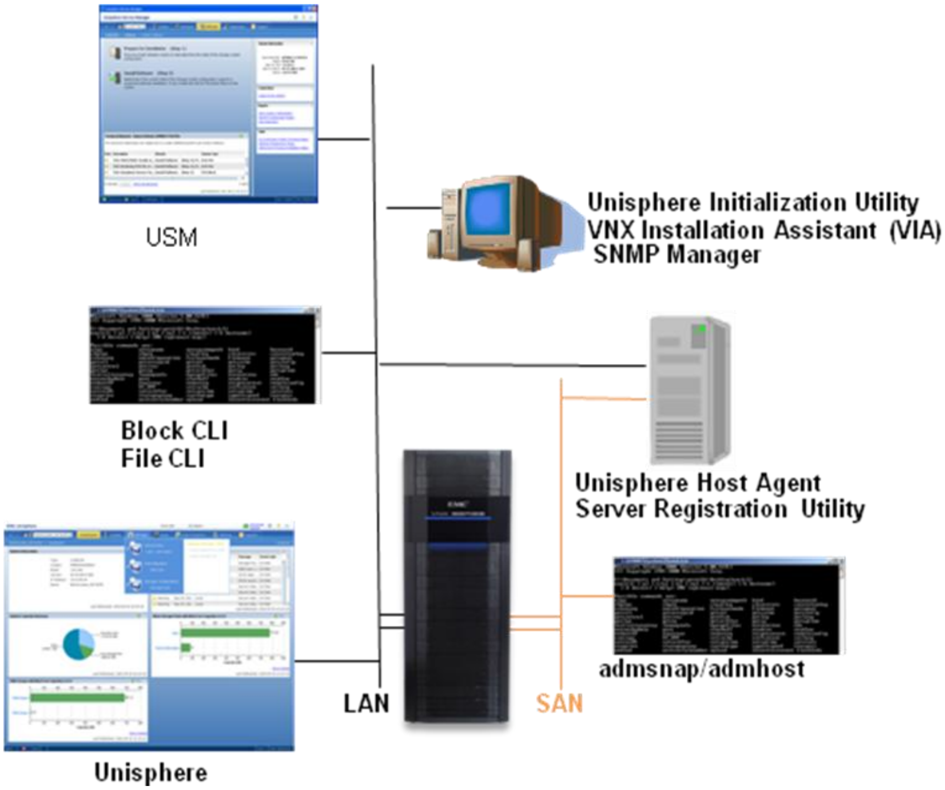

USM
Unisphere Initialization Utility
VNX Installation Assistant (VIA)
SNMP Manager
Block CLI
File CLI
Unisphere Host Agent
Server Registration Utility
admsnap/admhost
LAN
SAN
Unisphere

Figure 1 Unisphere Management Suite components

Security configuration settings

Access control settings

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

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

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. This applet establishes a secure connection with the Storage Management Server[1] software on the VNX storage system though `SSL/TLS (port 443)`. Note that even though even though `https://` is not displayed on your browser, the connection is secure.

We recommend that you connect to Unisphere through `https ://<vnx_ip> (port 443),` although it is possible to connect through `http://<vnx_ip> (port 80).`

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. All subsequent requests that the applet sends contain the cached digest in the authentication header.

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.

[1] The Storage Management Server software performs the storage management functions described in this guide.

Block CLI authentication

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 Block CLI command without credentials, 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 passphrase; this ensures that the file cannot be copied to another machine or account and used by an unauthorized user.

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

Storage Management Server can authenticate users against an LDAP directory, such as *Active Directory (AD) service.* (AD is Microsoft's implementation of LDAP.) Authentication against an LDAP server simplifies management because you do not need a separate set of credentials to manage VNX storage systems.. It is also more secure because enterprise password policies can be enforced for the storage environment *and* the server environment.

This document describes how to set up LDAP for Block services. To learn how to set up LDAP for File services, refer to the *Security Configuration Guide on VNX for File* on Powerlink.

After you perform this setup, Unisphere is configured with connection information for the LDAP server and Unisphere roles are mapped to LDAP users or groups. Logins to Unisphere or Block CLI can be authenticated with an LDAP account. LDAP configuration information is replicated throughout the Unisphere domain, so all storage systems in the domain can be authenticated against the same LDAP service.

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 users or groups must be given access to Unisphere by mapping them to Unisphere roles The LDAP service merely 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.

For example, let’s assume that there is an LDAP group called "Storage Admins" of which Bob and Sarah are members. There is another LDAP group 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

The Storage Management Server locally caches credentials for an LDAP user once they have 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 the “Authentication configuration” section for information on default management accounts and how to change its password.

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

Authentication configuration

Security is initialized differently for VNX Unified (Block and File)/File-only systems and VNX Block-only systems.

Three management accounts are installed on VNX File-only and VNX Unified systems in the factory:

- **Root** – This is a File–only local account that provides root-level privileges on the control station.
- **nasadmin** – This is a File-only local account that provides administrator level privileges on the control station.
- **sysadmin** – This is a global *system* account that provides administrator level privileges for both File and Block.

A *system* account is a special global account that is needed for internal communication between Block and File services. VNX Unified/File-only systems require at least one system account. You can not delete this system account unless another global administrator account or global security administrator account is available.

VNX Initialization Assistant (VIA) is the utility for initializing VNX Unified/File-only systems. It is recommended to change the default password for the above 3 accounts when first initializing a VNX Unified/File-only system using VIA.

VNX Block-only systems do not have any default management accounts. You use the Unisphere Initialization wizard to initialize Block-only VNX systems. There are two different ways to initialize security on Block-only systems:

- You can create a global account when initializing the system using Unisphere Initialization wizard
- You can create a global account when you fist log into Unisphere.

A system account is not created on a VNX Block-only system as it is not needed. However if you add a Unified or File-only system to the local domain of a Bock-only system, a system account is required and you will be prompted to create one.

For all VNX systems (Unified, File-only, Block-only), at least one global account is required. This account must have the "administrator" or "security administrator" role. Then, 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 using Unisphere or Block CLI.

User actions performed without authentication

VNX systems will not permit any actions without authentication

User 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.

User account roles

Unisphere authorizes user activity based on the role of the user. Unisphere roles include seven main roles (Operator, Network Administrator, NAS Administrator, SAN Administrator, Storage Administrator, Administrator, Security Administrator), and three Data Protection roles (Local Data Protection, Data Protection and Data Recovery).

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 has the highest level of privileges.

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

As a security and system integrity best practice, Unisphere administrator accounts should not be used for day-to-day activities.. 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. Usually most IT personnel are assigned a global operator account so they can monitor every storage system in the domain. They can also be assigned local storage administrator accounts for each specific storage system they are authorized to configure.

Data Protection roles

Data Protection/Replication operations are often performed by third-party personnel. In the earlier releases, a user needed storage administrator-level privileges to perform data protection operations. However, allowing third-party personnel this level of access could pose a security risk. To solve this problem, VNX systems have three Data Protection roles

Please note that 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 only control *existing* data protection objects. They can view the domain for objects that they cannot control; this allows them to have a fuller understanding of their environment. The data protection roles are:

- **Local Data Protection** – Privileges for SnapView (snapshots and clones) and Snapsure (Checkpoints) operations; not allowed to do data recovery operations like rollback a snapshot or reverse synchronize a clone. Also, no privilege to create new storage objects.
- **Data Protection –** All local data protection privileges, MirrorView, and SAN Copy operations; not allowed to do data recovery operations such as promoting a secondary and fracturing a mirror not allowed. Also, not allowed to create new storage objects.
- **Data Recovery** - All local data protection and data-protection role privileges and the ability to do data recovery operations; not allowed to create new storage objects.

Please note that Unisphere roles and data protection roles can have global or local scopes.

Component access control

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

Component authentication

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

Component authorization

LUN masking – 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.

IP filtering – This adds another layer of security by allowing administrators and security administrators to configure the storage system to restrict administrative access to specified IP addresses. These settings can be applied to the local storage system or to the entire domain of storage systems.

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.

Log description

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

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 for VNX storage systems is contained within the event log on each SP. The log contains hardware and software debug 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 storage 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 storage 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 in the Event Monitor template to log events to the Syslog server. You can then archive these logs as required.

ESRS IP Client

The ESRS IP Client for VNX software monitors the operation of your VNX storage 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. 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 storage 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 IP client for VNX Requirements and Installation* on the EMC Powerlink.

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 -** RSA enVision can collect 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 -** RSA enVision compresses and encrypts log data so that it can be stored for later analysis, while maintaining log confidentiality and integrity.
- **Analyzes logs -** RSA enVision 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.

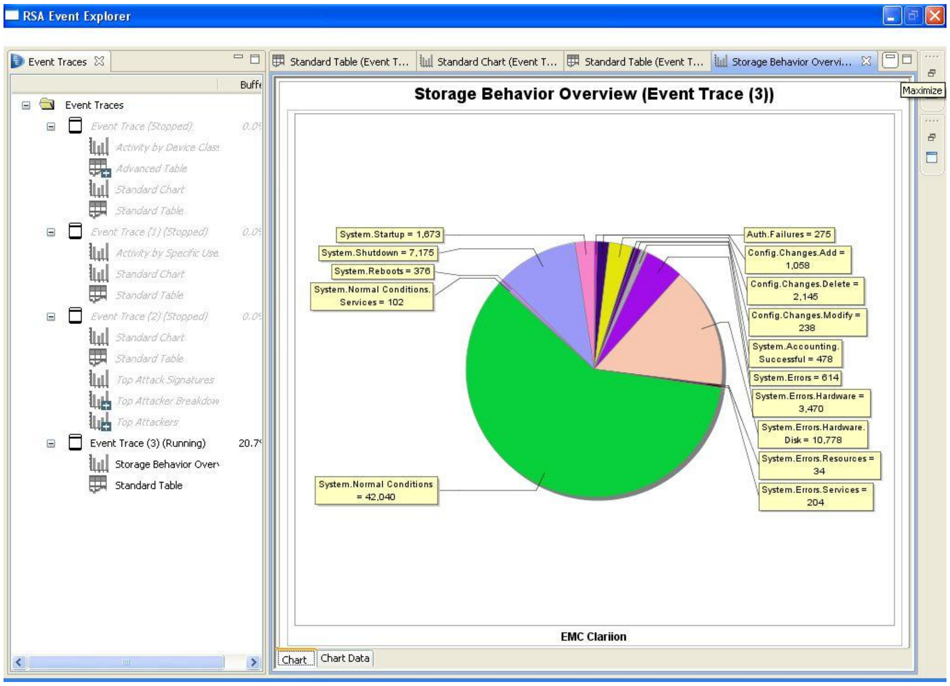

RSA Event Explorer
Event Traces
Buffe
Event Traces
Event Trace (Stopped) 0.0
Activity by Device Class
Advanced Table
Standard Chart
Standard Table
Event Trace (1) (Stopped) 0.0
Activity by Specific Use
Standard Chart
Standard Table
Event Trace (2) (Stopped) 0.0
Standard Chart
Standard Table
Top Attack Signatures
Top Attacker Breakdow
Top Attackers
Event Trace (3) (Running) 20.7
Storage Behavior Overv
Standard Table
Standard Table (Event T...
Standard Chart (Event T...
Standard Table (Event T...
Storage Behavior Overvi...
Maximize
Storage Behavior Overview (Event Trace (3))
System.Startup = 1,673
System.Shutdown = 7,175
System.Reboots = 376
System.Normal Conditions. Services = 102
System.Normal Conditions = 42,040
Auth.Failures = 275
Config.Changes.Add = 1,058
Config.Changes.Delete = 2,145
Config.Changes.Modify = 238
System.Accounting. Successful = 478
System.Errors = 614
System.Errors.Hardware = 3,470
System.Errors.Hardware. Disk = 10,778
System.Errors.Resources = 34
System.Errors.Services = 204
EMC Clariion
Chart
Chart Data

Figure 2 RSA enVision

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

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). Table 1 below lists the Unisphere components and the ports that are used for communication.

Table 1 Ports used by Unisphere components

Source component	Destination component	Network port	Protocol	Functionality	Type
Unisphere (Java applet)	Storage Management Server	80/443 or 2162/2163[2]	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
Admsnap	SnapView Provider	N/A	SCSI	SnapView	In band
Admhost	SAN Copy Provider	N/A	SCSI	SAN Copy	In band
Host Agent	SP Agent	N/A	SCSI	Host initiator	In band

[2] 2162/2163 are alternate port pairs that may be used to hide the CLARiiON storage system 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.

Source component	Destination component	Network port	Protocol	Functionality	Type
				registration	
Server Utility	FLARE	N/A	SCSI	Host initiator registration	In 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
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[3]	iSNS Server	3205	TCP	Internet storage naming service (iSNS)	In band or out of band
iSCSI initiator	FLARE	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	Responses 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	162	UDP	SNMP Traps	Out of band
Storage Management Server	ESX or Virtual Center server	443	HTTP/SSL	VM-aware Unisphere	Out of band

[3] iSNS registrations will be sent through whichever port can successfully route the packet to the iSNS server.

Network encryption

The Storage Management Server provides 256-bit symmetric encryption of all data passed between it and the client components that communicate with it, as listed in the "Port Usage" section (Web browser, Secure CLI), as well as all data passed between Storage Management Servers. The encryption is provided via SSL/TLS and uses the RSA encryption algorithm, providing 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. 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.

Unisphere is a Java-based applet that runs inside a Web browser. The applet is downloaded by the browser over standard HTTP; once downloaded the applet (not the browser) communicates using SSL/TLS. The URL for the browser will not change.

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 certificate verification

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 is 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 preinstalled) then it can inherently trust the server. This is the same mechanism by which your web browser inherently trusts most secure websites.

All certificates contain 2048-bit RSA encrypted keys and will not allow keys of less than 1024 bits to be imported. The interface for managing user certificates is found at:

```
http://<SP IP address>/setup pages
```

or with the **naviseccli security –pkcs12upload** switch.

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 (Unisphere, CLI, USM etc) connects to a server (Storage Management Server, LDAP etc.) 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.

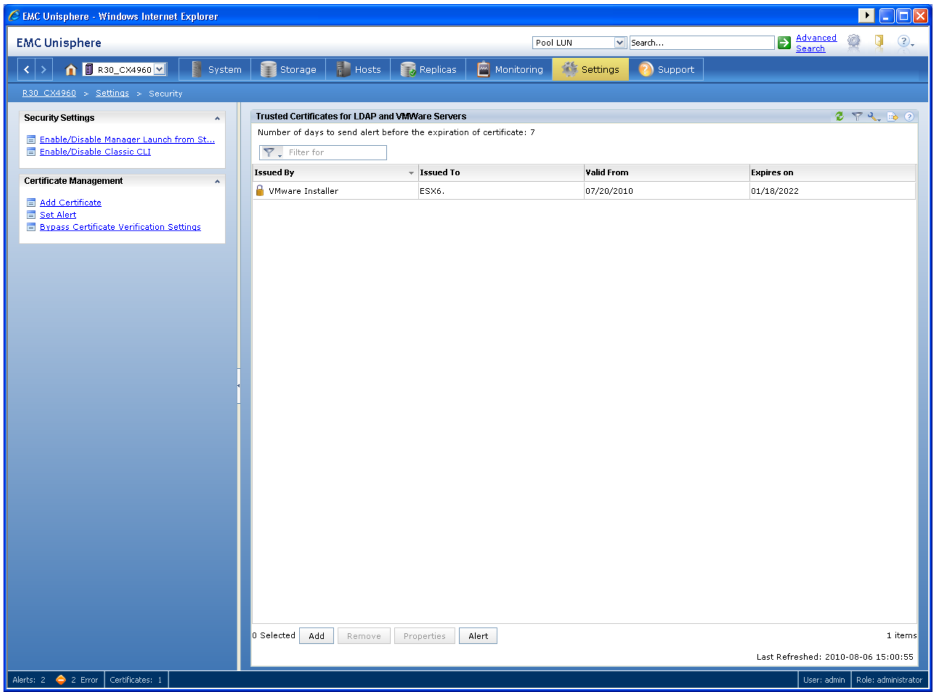
The following three options are presented to the user when connecting for the first time to a server:

1. **Accept for session** – This accepts the certificate for the user's session so that the user can manage the system. The user is prompted with the certificate the next time he logs in.
2. **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.

3. **Reject** – If the user does not trust the certificate, he 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 accessed 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. However, Block CLI provides the option to bypass certificate verification. This option is provided during installation on a client. The user is given the option to choose between two levels; Low (bypass certificate verification) and Medium (enforce certificate verification). Once the level is selected during installation, it cannot be changed. If it is necessary to change the level of certificate verification, the user will have to reinstall Block CLI on the client.

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 displayed in the **Settings > Security>Server certificates for block** screen in Unisphere. The screen also provides the option to bypass certificate verification for LDAP and ESX/Virtual Center servers.



Trusted Certificates for LDAP and VMWare Servers

Number of days to send alert before the expiration of certificate: 7

Issued By	Issued To	Valid From	Expires on
VMware Installer	ESX6.	07/20/2010	01/18/2022

0 Selected

1 items

Last Refreshed: 2010-08-06 15:00:55

Figure 3 Certificate store in Unisphere

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

Data erasure

For more information about data erasure, search for "*Certified Data Erasure for CLARiiON*" on the EMC Powerlink website.

Encryption of data at rest

For more information about encryption of data at rest, please see these documents on the EMC Powerlink website:

- *Approaches for Encryption of Data-At-Rest in the Enterprise*
- *EMC PowerPath Encryption with RSA*

Secure serviceability settings

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.

The username/password for the management port can be changed by visiting

```
https://<SP_ip>/setup
```

and clicking **Change Service Password**. Only administrators and security administrators can change the password. Note that if this password is changed, it will need to be provided to EMC Customer Service for certain maintenance and debug activities.

In addition to changing the password, RemotelyAnywhere provides additional security by providing IP filtering. This way you can limit the service access to only trusted IP addresses. IP filtering for Remotely Anywhere can be managed by visiting *https://<vnx_ip>/setup* and clicking on *Set RemotelyAnywhere Access Restrictions* button**.** Logging in to the VNX storage system using RemotelyAnywhere generates a unique message in the event log.

If a VNX storage 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. For normal storage-system operations, you do not need to 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 Powerlink 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 technical notes referenced above, this provides initiated channels from your customer site to authorized EMC and service partner personnel via 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.

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 Powerlink. 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 Powerlink.

Secure deployment and usage settings

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 that 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.

Figure 4 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 Table 1) 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 his/her 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.

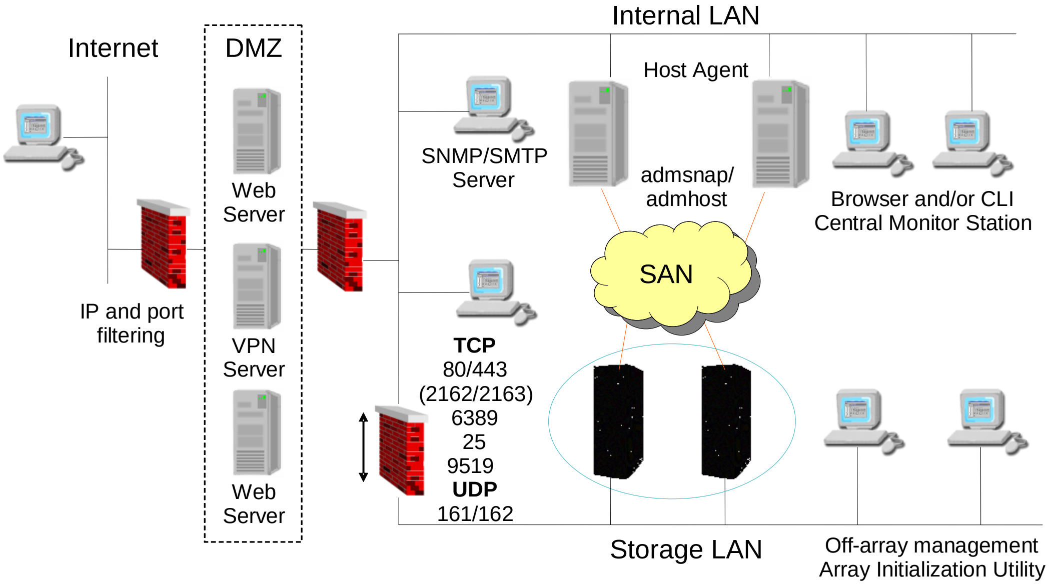


Figure 4 Minimally secure storage management network topology

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 Figure 5, these requirements can be satisfied, without the loss of Unisphere management capabilities, by making a few minor changes to the configuration shown in Figure 4. 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.

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.

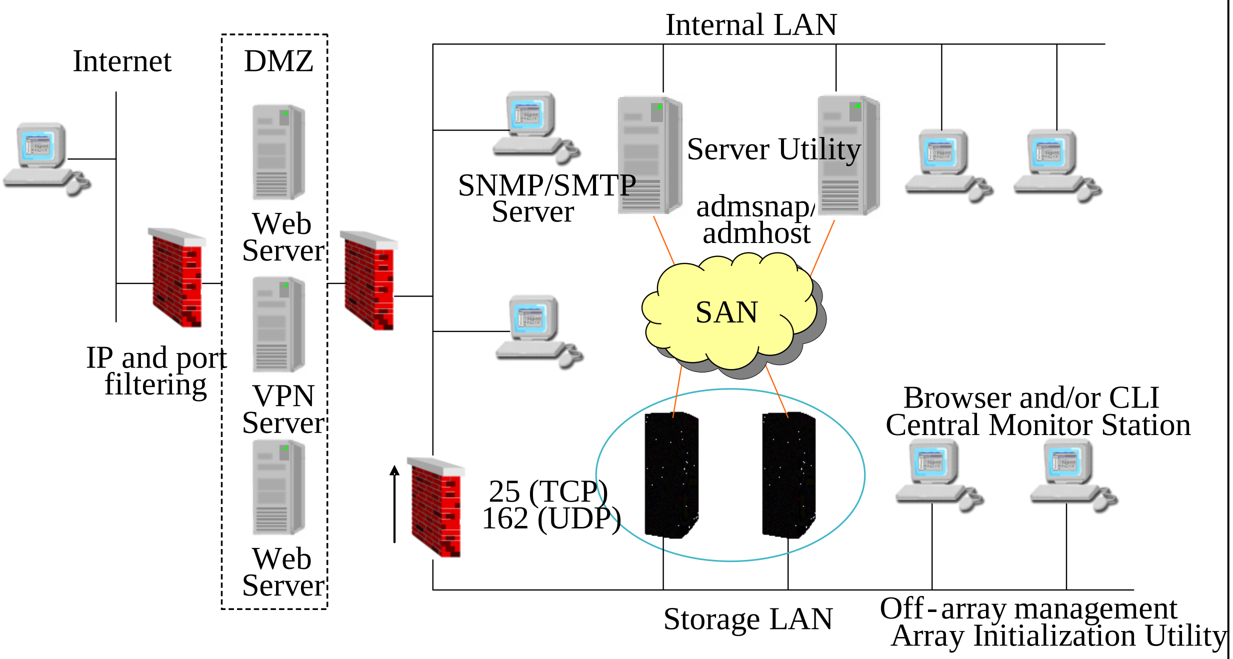


Figure 5 Moderately secure storage management network topology

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.

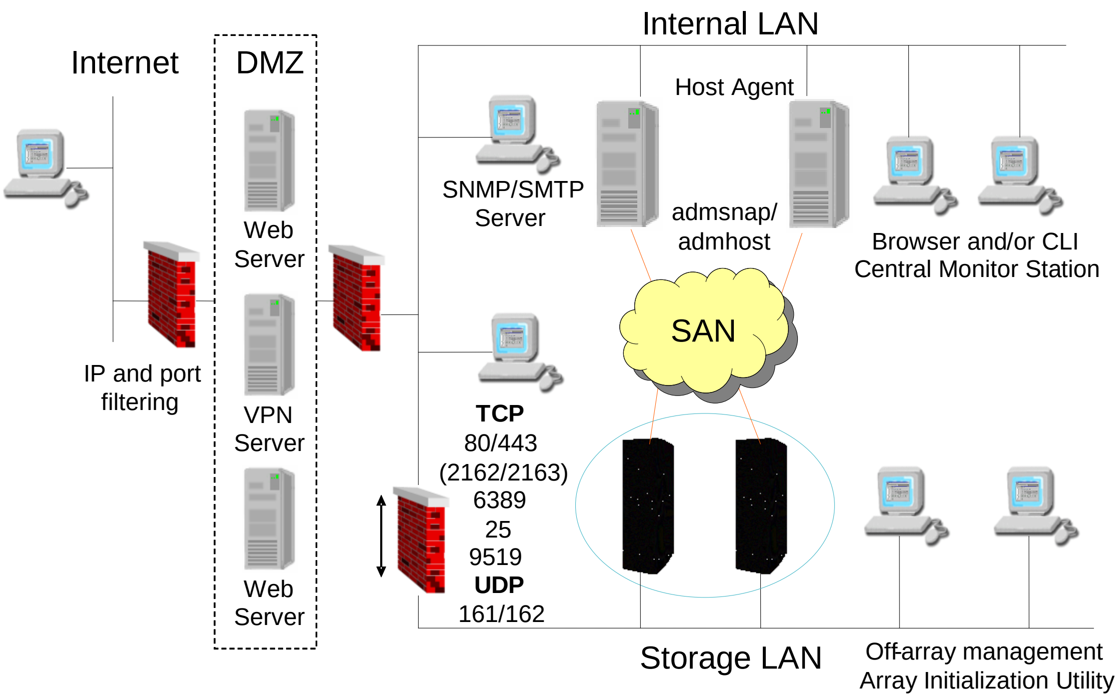


Figure 6 Highly secure storage management network topology

This final configuration 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.

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 via 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 Table 1 and described in the previous scenarios.

Secure maintenance

Security-patch management

VNX storage systems do not support installation of third-party utilities or patches. EMC will provide an officially released FLARE Operating Environment 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.

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 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 the “Secure serviceability settings” section 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.

Advanced management capabilities

The following security enhancements in VNX systems can be used to expand management capabilities and deliver more secure and efficient customer experience:

- Remote management
- Internet Protocol version 6(IPv6) addressing for a management port
- Support for VLAN tagging
- SNMP support for the user-settable community name
- Management Support for FIPS 140-2
- "Follow the sun" data center management
- Lights-out operation

Remote management

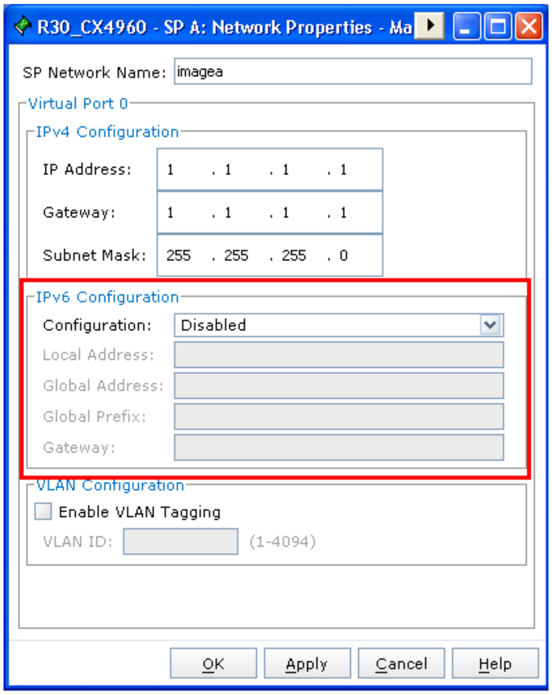
Unisphere has been designed to support a "securely manage from anywhere, anytime" capability, which enables an administrator to manage a storage system from any browser-equipped station without needing to preinstall any software or special hardware. This capability requires the security enhancements 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).

Customers should be pleased with this capability, since they are often faced with the challenge of how to manage data centers that have become more complex, with minimal staff. Services that are supposed to be up and running 24x7 make this situation worse. Hiring more staff is not the answer to budget restraints and a lack of qualified individuals.

A customer typically has one or two IT experts (gurus) on staff and must find ways to keep these gurus happy. Requiring the guru to be onsite to troubleshoot possible problems will not be tolerated for long. Providing the ability for the guru to troubleshoot from home or while traveling helps retain good personnel, and ensures success of the business.

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 storage systems can be accessed with either IPv4 or IPv6 for Unisphere, Block CLI, and RemotelyAnywhere. This dual stack IPv4/IPv6 mode supports interoperation with older systems.



SP Network Name: imagea

Virtual Port 0

IPv4 Configuration

IP Address: 1 . 1 . 1 . 1

Gateway: 1 . 1 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

IPv6 Configuration

Configuration: Disabled

Local Address:

Global Address:

Global Prefix:

Gateway:

VLAN Configuration

□ Enable VLAN Tagging

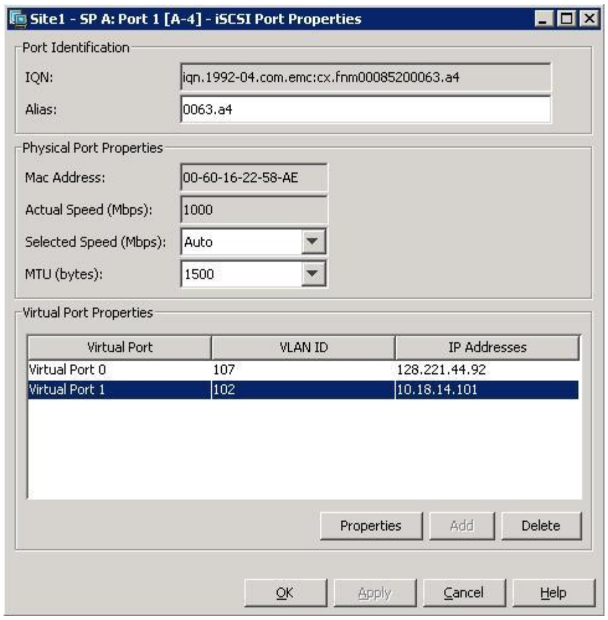
VLAN ID: (1-4094)

Figure 7 Configuring IPv6

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 1 GB/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. Figure 8 shows the iSCSI port properties for a port with VLANs enabled and two virtual ports configured. For more information on VLAN support, refer to the *VLAN Tagging and Routing on CLARiiON* white paper on EMC's Powerlink website.



Site1 - SP A: Port 1 [A-4] - iSCSI Port Properties

Port Identification

IQN: iqn.1992-04.com.emc:cx.fnm00085200063.a4

Alias: 0063.a4

Physical Port Properties

Mac Address: 00-60-16-22-58-AE

Actual Speed (Mbps): 1000

Selected Speed (Mbps): Auto

MTU (bytes): 1500

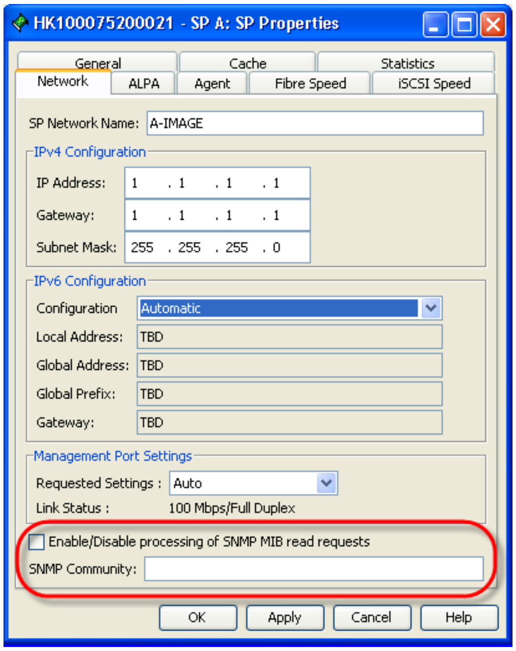
Virtual Port Properties

Virtual Port	VLAN ID	IP Addresses
Virtual Port 0	107	128.221.44.92
Virtual Port 1	102	10.18.14.101

Figure 8 iSCSI Port Properties with VLAN tagging enabled

SNMP support for the user-settable community name

SNMP management software can be used to monitor the state of VNX storage 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 EMC's Powerlink website.



SP Network Name: A-IMAGE

IPv4 Configuration

IP Address: 1 . 1 . 1 . 1

Gateway: 1 . 1 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

IPv6 Configuration

Configuration: Automatic

Local Address: TBD

Global Address: TBD

Global Prefix: TBD

Gateway: TBD

Management Port Settings

Requested Settings : Auto

Link Status : 100 Mbps/Full Duplex

□ Enable/Disable processing of SNMP MIB read requests

SNMP Community:

Figure 9 Setting the SNMP community name

Management Support for FIPS 140-2

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

VNX systems, starting with VNX block OE 31.5, support a FIPS 140-2 mode for the RSA BSAFE SSL modules on the Storage Processor (SP) that handle client management traffic. Management communication into and out of the array is encrypted using SSL. As a part of this process, the client and the Storage Management Server negotiate a 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 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 array if they do not support a cipher suite of acceptable strength.

FIPS 140-2 mode can be managed by the following CLI commands. Only the Administrator or Security Administrator has the privileges to manage the FIPS 140-2 mode.

Use this command to set FIPS 140-2 mode:

```
naviseccli -h <SP_IP> 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

When you set the FIPS 140-2 mode, the Storage Management Server will be restarted. For that brief period, management commands to the SPs will be blocked. However, this should have no effect on the IOs happening on the storage system.

Use this command to make sure FIPS 140-2 mode is enabled:

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

Follow the sun

Customers with geographically dispersed data centers can also benefit from the security enhancements in Unisphere.

Suppose a customer has data centers in New York, Japan, and England that must be operational 24x7. This customer can now use the "follow the sun" model of support, which means whichever site has the sun shining on it manages the other two sites. This model allows the customer to minimize staff. In addition, Unisphere enables secure, remote management over the Internet, without the additional costs associated with leased lines.

Lights-out operation

Customers with geographically dispersed data centers that are not required to be operational 24x7 (and so can absorb some downtime), may want to run some data centers in *lights-out* mode. Lights-out mode pushes the management responsibility to one or more central sites with the benefit of minimizing staff. Unisphere enables secure, remote management of lights-out data centers without the additional costs associated with leased lines. Refer to Figure 10 for an example of a lights-out configuration.

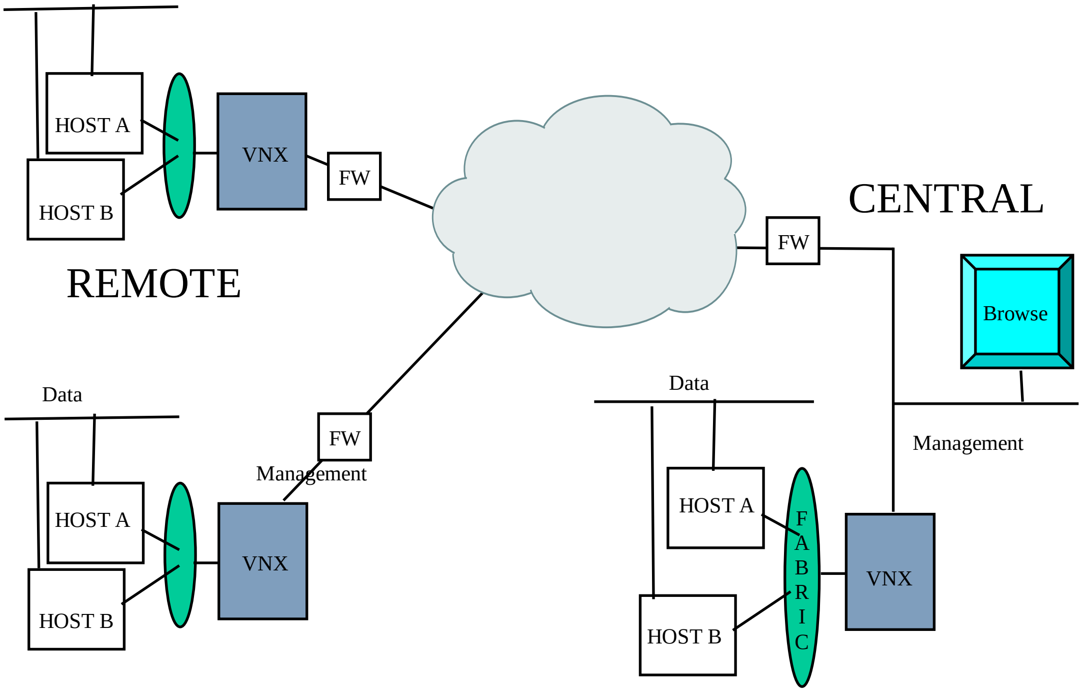


Figure 10 Lights-out operation

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 FLARE 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 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.

What is affected by management network filtering

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.

Components affected by IP filtering

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

Unisphere Management Suite white paper guide

Several white papers address major aspects of the Unisphere Management Suite, including security, domain management, host management, Secure CLI, SNMP, remote support, and Event Monitor. These papers supplement the standard Unisphere administrator and user documentation. These white papers are listed next along with a brief overview, and may be found on EMC.com and Powerlink, EMC's password-protected customer- and partner-only extranet.

White paper	Description
EMC Unisphere: Unified Storage Management Solution	This white paper provides an overview of EMC® Unisphere™, the single management interface for CLARiiON®, Celerra® and Unified VNX systems. It discusses all the features in Unisphere and lists the features supported by Unisphere v1.0, v1.1, and v1.1.25.
Security Configuration Guide on VNX for File	This paper discusses the File security settings and features for VNX storage systems
EMC Navisphere Secure Command Line Interface	This paper discusses the details of the Block CLI, including an overview of the Secure CLI, how to convert from the Classic CLI and Java CLI, and limitations of the Secure CLI.
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 .
EMC Secure Remote Support IP client for VNX Requirements and Installation	This paper describes the requirements for installing EMC Secure Remote Support (ESRS) IP client for VNX storage systems

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

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