EMC® VNX™ Series
Release 7.1

Configuring and Managing CIFS on VNX™
P/N 300-013-429 Rev 02

Contents

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

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

Special notice conventions

EMC uses the following conventions for special notices:

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

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

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

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

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

Where to get help

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

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

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

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

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

Your comments

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

Please send your opinion of this document to:

`techpubcomments@EMC.com`

Introduction

EMC VNX has incorporated the Common Internet File System (CIFS) protocol as an open standard for network file service. CIFS is a file access protocol designed for the Internet and is based on the Server Message Block (SMB) protocol that the Microsoft Windows operating system uses for distributed file sharing. The CIFS protocol lets remote users access file systems over the network.

This document is part of the VNX documentation set and is intended for use by system administrators responsible for implementing CIFS on VNX in a Windows environment or a multiprotocol (Windows and UNIX) environment and managing VNX in their Windows network.

Topics included are:

- System requirements on page 12
- User interface choices on page 13
- Related information on page 13

System requirements

Table 1 on page 12 describes the EMC® VNX™ series software, hardware, network, and storage configurations.

Table 1. CIFS system requirements

Software	VNX version 7.1
Hardware	VNX

Network	Windows Server domain:
	
	 ◆ You must configure Windows Server domains with:
	
	      ◆ Active Directory (AD)
	
	      ◆ Kerberos or NT LAN Manager support
	
	      ◆ DNS server
	
	         The DNS server should support dynamic updates. If dynamic DNS (DDNS) is unsupported, you must manually update the DNS server. *Configuring VNX Naming Services* provides instructions on configuring a Data Mover to use naming services.
	
	      ◆ Network Time Protocol (NTP) server
	
	         Configuring Time Services on VNX provides instructions on configuring VNX as a client of an NTP server.

Note: VNX does not support the Samba software reimplementation of the SMB and CIFS protocols.

User interface choices

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

- EMC Unisphere™

- Microsoft Management Console (MMC) snap-ins (Windows Server only)

- Active Directory Users and Computers (ADUC) extensions (Windows Server only)

Note: The ADUC plug-in and the CIFS migration tools do not support 64-bit Windows editions. The MMC snap-in however, supports 64-bit Windows editions.

For additional information about managing your VNX:

- EMC VNX Documentation on EMC Online Support website

- Unisphere online help

Installing Management Application on VNX for File includes instructions on launching Unisphere, and on installing the MMC snap-ins and the ADUC extensions.

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

Related information

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

- *VNX Glossary*

- *EMC VNX Command Line Interface Reference for File*

- *Parameters Guide for VNX for File*

- *Configuring VNX Naming Services*

- *Configuring Time Services on VNX*

- *Configuring VNX User Mapping*

- *Configuring Virtual Data Movers on VNX*

- *Configuring and Managing Networking on VNX*

- *Installing Management Applications on VNX for File*

- *Managing a Multiprotocol Environment on VNX*

- *Managing Volumes and File Systems for VNX Manually*

- *Using VNX Replicator*

- *Using EMC Utilities for the CIFS Environment*

- *Using International Character Sets on VNX for File*

- *Using Windows Administrative Tools on VNX*

EMC VNX documentation on EMC Online Support

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

VNX wizards

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

Important: The *EMC VNX Command Line Interface Reference for File* explains advanced options supported by the server_cifs command.

Use of the term Windows Server

Because the CIFS implementation on VNX is virtually identical for Windows 2000 and and Windows 2012, the term Windows Server used in this document pertains to both the operating systems and later versions of Windows Server.

Concepts

VNX is a multiprotocol system that provides access to data through a variety of file access protocols including the Common Internet File Service (CIFS) protocol. CIFS is based on the Microsoft Server Message Block (SMB) and allows users to share file systems over the Internet and intranets, primarily by Windows platforms.

VNX implements CIFS inside the operating system kernel rather than as a user-mode application. This implementation allows VNX to deliver higher performance with native Windows Server functionality.

When a VNX is configured as a CIFS server, VNX provides file access features similar to those of a Windows Server. During configuration, VNX joins a specific Windows domain as a member server.

You might need to understand some or all of the following concepts when operating in a multiprotocol file sharing environment:

Active Directory

Active Directory (AD) lists resources and services available in a Windows network. When you configure CIFS on VNX, you create a VNX container for the CIFS server account in active directory users and computers (ADUC) or another AD container.

The AD account is created automatically when you create and join a CIFS server to the Windows domain. Create a CIFS server for Windows Server environments on page 65 and Join a CIFS server to a Windows domain on page 67 provide procedural information.

Windows environments

Figure 1 on page 17 shows VNX within a Windows domain. The Data Mover in this configuration provides CIFS file system operations for users in the Windows domain. The domain associated with the Data Mover is declared during Data Mover configuration.
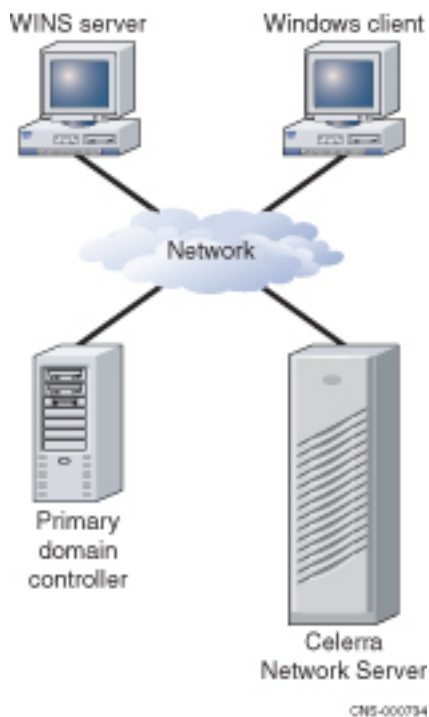
Figure 1. VNX in a Windows domain

Note: In a CIFS environment, the Data Mover performs the functions of a CIFS file server, but not those of a Windows application server, such as a print or DNS server.

DNS servers

VNX supports the following Domain Name System (DNS) features:

◆ DNS Service Resolution — Resolves service names instead of computer names. DNS returns a list of machines that run a specific service, such as the Light Weight Directory Access Protocol (LDAP) and Kerberos.

◆ DNS Dynamic Updates — Reduces administration complexity in DDNS environments.

Windows Server environments require a DNS server. The DNS domain name and IP address for the Data Mover are defined to the domain through the server_dns command.

In dual stack domains with both IPv4 and IPv6 DNS servers configured, you should ensure that at least one interface for each address type is configured on all CIFS servers for a Data Mover in that domain.

Configuring VNX Naming Services provides additional information on naming services.

You must configure more than one DNS domain per Data Mover when the Data Mover's CIFS configuration includes CIFS servers that are:

◆ For domains not in the same Windows forest

◆ Not served by the same DNS servers

For example, you could have two networks connected to the Data Mover—a public network and a private network with no communication between the two networks.

Note: The server_dns command can be repeated for different domains.

Note: Because most DNS requests are short messages, User Datagram Protocol (UDP) is the preferred protocol. When a DNS message is longer than 512 bytes, the Data Mover automatically switches to the Transmission Control Protocol (TCP) for a specific request processing. You should only force the TCP protocol when there is no DNS server close to the Data Mover.

NTP servers

Windows Server environments require a NTP server. It is strongly recommended that you set up a minimum of two NTP servers per domain to avoid single point of failure.

The date and time must be synchronized among the Data Movers and other time sources by using the server_date command. *Configuring Time Services on VNX* explains how to synchronize Data Movers.

IPv6 best practices

Avoid IPv6-only CIFS servers and Data Movers with only IPv6 interfaces.

If Data Movers with only IPv6 interfaces are desired, it is imperative that the DNS, NIS, and NTP servers for that Data Mover have IPv6 addresses configured for these services to work.

If IPv6 is being deployed, configure both IPv4 and IPv6 addresses for DNS, NIS, and NTP servers. This way, if an IPv6-only situation arises for any reason, then these services will still work.

Domain migration

VNX CIFS servers act as member servers in Windows domains and provide data storage for domain users. Data stored on CIFS file systems contain security metadata such as discretionary access control lists (DACLs), system access control lists (SACLs), and ownership associated with the domain security IDs (SIDs) from which the CIFS accounts are derived.

Due to Microsoft end-of-life policy, you might need to perform domain migration from one version of the domain to another. During and after a Windows domain migration process, any data generated by user accounts in the source domain must be accessible by user accounts in the target domain.

Note: Domain migration is a complex task that is not covered in this document. Microsoft documentation provides detailed information on domain migration.

VNX provides two server_cifs command options, -Migrate and -Replace, to meet the requirements of data availability during and after domain migration.

These options update the security IDs (SIDs) generated for resources created by CIFS users in one Windows domain (source) to another Windows domain (target).

Note: A trusted relationship must be established between the source and target domains. This is a Microsoft requirement for domain migration.

provides procedural information.

Domain-joined and stand-alone CIFS servers

A CIFS server can participate as a member of a Windows domain or operate independently of any Windows domain as a stand-alone CIFS server. CIFS servers that are members of a Windows domain use domain-based Kerberos authentication of users, maintain their own identity (computer account) in the domain, and leverage domain site information to locate services such as domain controllers. Domain-based CIFS servers are appropriate for production use. Joining a CIFS server to a domain allows any user in the domain to connect to the CIFS server.

Note: You can join a CIFS server to a domain in a Windows environment where the active directory (AD) namespace is named independently from the DNS namespace.

Create a CIFS server for Windows Server environments on page 65 and Join a CIFS server to a Windows domain on page 67 provide procedural information.

In contrast, a stand-alone CIFS server does not have access to a domain and its associated services. The only users that can connect to a stand-alone CIFS server are those that use a local user account created and managed on the stand-alone CIFS server with the CIFS server itself performing all user authentications. Stand-alone CIFS servers are useful in test environments. Create a stand-alone CIFS server on page 75 provides procedural information.

Network interfaces and CIFS servers

The CIFS server created on a physical Data Mover with no interface specified becomes the default server. It is automatically associated with all unused network interfaces on the Data Mover and any new interfaces that you subsequently create. If you create additional CIFS servers on the Data Mover, you must specify one or more network interfaces with which to associate the server.

You can reassign network interfaces to other CIFS servers on the Data Mover as you create them, or later as required. The default CIFS server behavior is useful if you plan to create only one CIFS server on the Data Mover. It is recommended that you always explicitly associate network interfaces with the first CIFS server created on a Data Mover. This practice makes it easier to create more network interfaces in the future and avoids having CIFS traffic flow onto networks for which it is not intended. The default CIFS server cannot be created on a Data Mover having a loaded Virtual Data Mover (VDM).

You can use network interfaces to access more than one Windows domain by creating multiple network interfaces, each associated with a different domain, and assigning a different CIFS server to each interface. Use the server_ifconfig command to create an IP interface on the specified Data Mover. *Configuring and Managing Networking on VNX* provides more information.

Note: For security reasons, consider using a VDM or a separate Data Mover in environments with multiple Windows domains. *Configuring Virtual Data Movers on VNX* explains how to configure VDMs.

CIFS shares

You create a share by exporting the pathname of the file system by using the server_export command. After the share is created, you can access it from a Windows client by mapping a network drive to the share or by connecting to the UNC path of the share. Create shares for CIFS users on page 71 provides procedural information.

Table 2 on page 21 describes the server_export command options.

Table 2. server_export options

Option	Result
ro	Creates the share as read-only for CIFS clients.

Table 2. server_export options *(continued)*

Option	Result
rw=<client> [:<client>]...	Creates the share for CIFS clients as read-mostly. Read-mostly means exported read-only to most clients, but read/write to those specified. By default, the pathname is exported read/write to all. A client may be either a <user_name> or <group_name>. The <user_name> and <group_name> must be defined in the Data Mover's password file. Note: If user authentication on the Data Mover is set to NT, this option is ignored and file access is controlled by the share and file access control lists (ACLs).
maxusr=<maxusr>	Sets the maximum number of simultaneous users permitted for a share. The maxusr value cannot be set to zero.
netbios=<net-bios_Name> [,netbios=<netbios_Name>] ...	Associates a share on a single domain with one or more NetBIOS names created with server_cifs. By default, if a NetBIOS name is not specified for a share, the share is a global share visible to all NetBIOS names.

International character support

If Unicode support is enabled, the -name and -comment options of the server_export command accept any multibyte characters defined by the Unicode 3.0 standard. Otherwise, these options accept only ASCII characters. Note the following restrictions for the -name and -comment options:

* Share name length is limited to 12 characters unless Unicode support is enabled, in which case the limit is 80 characters.

* Share names cannot include the following characters: /, \, %, ", NUL (Null character), STX (start of header), SOT (start of text), and LF (line feed).

* Share names can contain spaces and other nonalphanumeric characters, but must be enclosed by quotes if spaces are used.

* Share names cannot begin with a - (hyphen) or @ symbol. '.' and '..' are not allowed as share names.

* Share names are case-insensitive but the case is preserved.

* Comment length is limited to 256 bytes (represented as 256 ASCII characters or a variable number of Unicode multibyte characters).

* A comment cannot include the following characters: NUL (Null character), STX (start of header), and SOT (start of text).

Enable internationalization support

Enabling internationalization support is for Windows Server only. If you are using UNIX or SHARE user authentication on the Data Mover, skip to Create a domain account in Active Directory on page 64.

Internationalization support must be provided on VNX by enabling Unicode.

Note: VNX must use the NT user authentication method when Unicode is enabled. NT security is the default user authentication method for VNX.

Best practices

As a best practice, enable Unicode as the default option during installation. If you do enable Unicode, enable it before populating the file system. When you first enable Unicode, the conversion process might cause an interruption in file system availability while the file system is scanned and converted.

⚠ CAUTION After enabling Unicode you cannot disable it and return to ASCII mode.

Notes on ASCII filtering

Be aware of the following issues with ASCII filtering:

◆ If ASCII filtering is enabled, you might be unable to administer CIFS servers by using the Microsoft management tools such as the Users and Computers MMC snap-in.

◆ When ASCII filtering is enabled, you cannot create or rename files with non-ASCII characters (characters with more than seven bits) in the filename. You can still access files with non-ASCII names; however, the filenames might contain strange characters.

◆ If the filtering parameter is set, ASCII filtering is applied to all Windows clients. If the parameter is set, and at least one compname is created, you cannot reset the parameter to 0 until you remove all the compnames.

Quotas

CIFS implementation of VNX supports disk quotas. Quotas can be configured by using the CLI of VNX, Unisphere, or the Windows Server user interfaces. *Using Quotas on VNX* provides detailed information on quotas.

If you plan to use quotas, activate them on a file system before populating the file system. When you first activate quotas, the entire file system is unavailable while it is being scanned by the quota initiation process.

Alias

An alias provides multiple, alternative identities for a given resource. The alias shares the same set of local groups and the primary NetBIOS name or computer name because an alias acts as the secondary name.

A NetBIOS alias registers the alternative name in Windows Internet Naming Service (WINS), not in domain name system (DNS). If you want the NetBIOS alias to appear in DNS, you must add it to DNS.

The client can connect to an alias through the Network Neighbourhood, Windows Explorer, or by using the Map Network Drive window.

Based on the Microsoft requirements, aliases must be unique across a domain for WINS registration and broadcast announcements. Aliases must also be unique on the same Data Mover to avoid WINS name conflicts.

For performance reasons, it is recommended that you limit the number of aliases to 10 per CIFS server. You can add aliases to an existing server or when creating a new server. The *EMC VNX Command Line Interface Reference for File* provides additional information on alias name restrictions.

NetBIOS compared with DNS alias

You might have a file server called Finance that has been removed and replaced with a new file server called Accounting_and_Finance. The existing users would continue to have their mapping to the old file server called Finance. To avoid every user to manually change the mapping to Accounting_and_Finance, you can create a NetBIOS alias called Finance. With the NetBIOS alias created, the old mapping will work.

DNS alias is slightly different than the NetBIOS alias. The DNS database would typically have:

◆ Address (A) resource records that map a computer name to an IP address. For example, a file server Finance mapped to 10.20.30.40.

◆ Canonical (CNAME) resource records that map a domain name to another domain name. For example, finance.emc.com mapped to accounting.emc.com.

provides procedural information.

Kerberos authentication

The Kerberos Key Distribution Center (KDC) stores and retrieves information about security principles in the AD database. Each domain controller in Windows 2000 or later is a Kerberos KDC that acts as a trusted intermediary between a client and a server. Kerberos authentication uses a KDC to confirm the identity of a CIFS server that is attempting to communicate with a domain or trying to access Windows network services.

Every computer, server, or client joined to a domain has a unique password associated with a computer account in the active directory (AD). A password authenticates the identity of a CIFS server that attempts to communicate with a domain controller.

After you join a CIFS server to a domain or change the computer account password of a CIFS server, Kerberos generates a set of encryption and decryption keys that it shares with the domain controller. When the KDC receives an authentication request from a CIFS server, it performs authentication by decrypting the preauthentication data sent by the Data Mover with the decryption keys. If the decryption succeeds and the preauthentication data is accurate, the CIFS server is authenticated. After a CIFS server is authenticated, the KDC generates an initial ticket called the Ticket-granting Ticket (TGT), as shown in Figure 2 on page 25. The TGT is a special ticket that enables the CIFS server to request services to the KDC.

① Presents key for authentication

② Verifies CIFS server and provides TGT

CNS-00679G

Figure 2. Kerberos authentication

The Microsoft website provides a detailed description of Kerberos authentication.

For domain configurations with multiple domain controllers, computer accounts and passwords are replicated to all domain controllers during AD replication. Because AD replication occurs at scheduled intervals, a delay in updating all the domain controllers with a new password can occur, possibly causing failed authentication attempts. The Data Mover retains a history of the new and old passwords of each CIFS server. When a Windows client attempts to open a new session with a Data Mover, the service ticket sent by the client is decrypted using the decryption key generated from the CIFS server computer account password. If the decryption fails, another attempt is made by using the key generated from the previous passwords. When a password is updated twice on the same domain controller or on different domain controllers without AD replication, the Data Mover only uses the first password update; it does not recognize the second password change.

Set maximum number of passwords to retain in Kerberos authentication on page 80 provides procedural information.

Kerberos SPN Mismatch

CIFS allows Windows clients to connect to the Data Movers and mount shares. For Windows Server domains, Kerberos authentication is used as an authentication mechanism, although NTLM (pre-Windows 2000) authentication is still available, for backwards compatibility.

When Kerberos authentication is not used or fails, the use of NTLM authentication significantly increases the load on the Windows domain controller. In addition, NTLM authentication is not considered to be as secure as Kerberos authentication.

The Kerberos Workstream feature addresses this. If Kerberos is not configured correctly, that is, if SPNs do not exist or are out of sync and do not match the DNS hostname entries, the Kerberos authentication fails and the client may revert to NTLM to connect to the Data Mover. If this happens, the user has to be notified to diagnose and fix the issue.

The *Parameters Guide for VNX for File* provides more information on the cifs.spncheck parameter. The *EMC VNX Command Line Interface Reference for File* provides more information on the -setspn option of the server_cifs command.

The incoming client CIFS connections are analyzed to determine whether a Kerberos authentication error has occurred. The CIFS Server FQDN and the received FQDN are cached. The Server FQDN cache is checked each time when the possible Kerberos failure occurs. When there are cache entries, an EventLog message will be generated for each entry once per hour, when configured. The EventLog for each entry contains a detailed description with recommended action, both to notify the user of the issue and to resolve it. It also includes two counts of occurrences, since the last set of EveltLog messages and since the last reboot.

LDAP signing and encryption

In some instances, communication between VNX and the active directory (AD) is handled by using the LDAP. LDAP is used during a domain join and unjoin, server account password change, GPO updates, and when VNX is configured to use the AD for storing user mappings.

During an LDAP BIND procedure, the Data Mover (LDAP client) authenticates to a domain controller (LDAP server) through Kerberos by using the simple authentication and security layer (SASL) protocol. The SASL protocol provides a means for the Data Mover and the domain controller to negotiate a security layer for LDAP queries and answers.

A signed security layer checks the integrity of each LDAP packet on the network to ensure that an intermediate party did not tamper with its contents. An encryption security layer prevents the data in the LDAP packets from being sent in clear text between the client and the server.

The LDAP client (in this case, the Data Mover) makes the final decision on the security level to use. This negotiation of signing or encryption is on a per-LDAP connection basis.

By default, a domain controller does not enforce any form of data protection for LDAP traffic. A Registry attribute or a security policy controls whether the domain controller enforces LDAP message signing.

Note: Although Windows supports encryption of LDAP messages through other systems, such as VNX, it does not allow the configuration of LDAP message encryption.

Windows 2000 LDAP Registry setting

Table 3 on page 27 shows the Windows 2000 Registry setting required to enforce LDAP message signing for a domain controller.

Table 3. Registry parameter for LDAP message signing

Key path	HKLM\System\CurrentControlSet\Services\NTDS
Key	Parameter
Value name	LdapServerIntegrity
Format	REG_DWORD
Value	2 (Require signing); other values are 0 (Not defined) and 1 (None)

Note: Define the Registry parameter on each domain controller because Registry changes are not replicated among domain controllers in a domain.

Windows Server 2003 LDAP security policy

For Windows Server 2003, the LDAP security policy is defined as a group policy object (GPO) and can be configured on a domain controller or a domain. You can set this GPO security policy by going to **Administrative tools ➤ Domain Controller Security Policy (or Domain Security Policy) ➤ Security Settings ➤ Local Policies ➤ Security Options** and selecting **LDAP server signing requirements**.

Note: Applying the LDAP server signing requirements policy to a domain controller or domain overrides the Windows 2000 LdapServerIntegrity Registry parameter.

Table 4 on page 28 shows the Windows Server 2003 GPO LDAP security policy settings and the corresponding Windows 2000 LDAP LdapServerIntegrity Registry parameter settings.

Table 4. GPO and Registry LDAP security policy settings

GPO LDAP security policy settings	LDAP Registry parameter settings	Description
Not defined	0	LDAP signing is not enabled or disabled at the domain-controller level.
None	1	LDAP signing is not required to bind with the domain controller. If the Data Mover requests data signing, the domain controller supports it.
Require signing	2	LDAP signing is negotiated between the Data Mover and the domain controller unless the Transport Layer Security/Secure Socket Layer (TLS/SSL) has started.

Change the LDAP security level on page 80 provides procedural information.

Combining Windows settings with VNX ldap SecurityLayer

Table 5 on page 28 shows the security actions taken when combining the Windows GPO LDAP security policy or LDAP Registry setting with the VNX ldap SecurityLayer parameter settings.

Table 5. Combining Windows settings with VNX ldap SecurityLayer settings

	VNX ldap SecurityLayer parameter settings			
	0 No security layer	1 Same as LDAP server	2 Integrity protection	4 Privacy protection
Windows LDAP security policy/Registry settings				
0 (Not defined)	No signing or encryption	Uses security layer proposed by the domain controller	Uses LDAP message signing	Uses LDAP message encryption
1 (None)				
2 (Require signing)	Rejects LDAP BIND			

User authentication methods

Before configuring the CIFS service, you must define the user authentication method for the Data Mover. The user authentication method defines the way the Data Mover validates

users logging in to the Data Mover. When a Windows user logs in, a security access token is created; it contains the security ID (SID) for the user, the SID for the user group, and access rights but not the permissions. This token is compared with the security descriptor of any CIFS object such as a share to determine access.

The user authentication method and the dialect parameter that defines the protocol level VNX supports is set per Data Mover and applies to every interface on the Data Mover. Therefore, all CIFS servers on the Data Mover must use the same user authentication method and dialect. When creating a computer name, you can limit authentication to Kerberos only; otherwise, NTLM or NTLMSSP and Kerberos are allowed.

Data Movers use NT user authentication as the default authentication method. Set maximum number of passwords to retain in Kerberos authentication on page 80 provides procedural information.

Note: EMC recommends to use a CIFS stand-alone server instead of Data Movers with SHARE authentication. Create a stand-alone CIFS server on page 75 provides procedural information.

A stand-alone server provides all advantages that the NT authentication offers.

Table 6 on page 29 summarizes and compares NT, UNIX, and SHARE user authentication methods.

Important: You should review the CIFS user authentication methods to understand the proper usage and limitations.

Table 6. CIFS user authentication methods

NT	UNIX	SHARE
Overview: ♦ Allows access to shares only after authentication by a domain controller. ♦ In case of NTLM, the client sends a username and encrypted password to the Data Mover for authentication. ♦ Checks file, directory, and share-level ACLs. ♦ Default user authentication method. ♦ Recommended.	Overview: ♦ Authentication is done on the Data Mover by using the local files (passwd and group) or NIS. ♦ Uses plain-text passwords. ♦ ACLs unchecked. ♦ Not recommended.	Overview: ♦ Uses no passwords or uses plain-text passwords. ♦ Asks for read-only or read/write password. ♦ ACLs unchecked. ♦ Not recommended.

Table 6. CIFS user authentication methods *(continued)*

NT	UNIX	SHARE
How it works: ◆ The client sends a username and encrypted password to the Data Mover or Kerberos tickets. User authentication is done by the domain controller by using NTLM V0.12 (default in Windows Server) and LDAP. ◆ Access-checking is against user and group security IDs (SIDs).	How it works: The client sends a username and a plain-text password to the Data Mover. The Data Mover verifies ID information by checking the passwd file on the Data Mover or NIS.	How it works: ◆ If you do not specify a password when creating the share, any user connecting to the share is granted access. ◆ If you do specify a password, the user must provide the specified password when connecting to the share.
Limitations: None.	Limitations: ◆ No Unicode. ◆ No VDM. ◆ No Common AntiVirus Agent (CAVA). ◆ Maximum file size 4 GB.	Limitations: ◆ No Unicode. ◆ No VDM. ◆ No CAVA. ◆ Maximum file size 4 GB.
Requirements: Requires a UNIX-style UID and GID for each Windows user.	Requirements: ◆ Requires a UNIX-style UID and GID for each Windows user. ◆ Plain-text password support must be enabled on clients.	Requirements: Plain-text password support must be enabled on clients.
When to use: ◆ Most useful for configurations requiring a high degree of security and that are accessed primarily by CIFS users. ◆ Recommended.	When to use: ◆ Typically used when there is no Windows domain available. ◆ Not recommended.	When to use: ◆ Only useful for configurations with few security requirements. ◆ Not recommended.

User mapping

Every user of VNX, either a Microsoft Windows user or a UNIX and Linux user, must be identified by a unique numeric user identifier (UID) and group identifier (GID). Windows, however, does not use numeric IDs to identify users. Instead, it uses strings called security identifiers (SIDs). Therefore, before you configure the Windows file-sharing service (CIFS) on VNX, you must select a method of mapping Windows SIDs to UIDs and GIDs.

Configuring VNX User Mapping provides additional information.

Local user and group accounts

Enabling local user support creates local user accounts in the local groups database on the CIFS server. When local users try to log in to the CIFS server, they are authenticated by NTLM V1/V2 against the local groups database. When you enable local user support on a CIFS server, the local groups database is automatically populated with two local user accounts—Administrator and Guest.

The local user feature allows you to create up to 128 local user accounts per CIFS server. Supporting local user accounts on a CIFS server accomplishes two goals:

◆ Provides access to the CIFS server even when the domain controller is unavailable for authentication. If the domain controller is unavailable, domain user accounts cannot access the CIFS server. In this situation, the local user feature lets you access the domain CIFS server by logging in through a local account.

◆ Enables the creation of a simple CIFS server configuration with no domain infrastructure. This type of CIFS server, called a stand-alone server, does not require external components such as a domain controller. Users log in to the stand-alone CIFS server through local user accounts.

A stand-alone server is a low-cost, low-overhead server that you can use for small environments or in place of servers using SHARE security mode. EMC recommends that you create a stand-alone CIFS server instead of using SHARE authentication. Create a stand-alone CIFS server on page 75 provides procedural information.

Note: Local user accounts are for CIFS access only and cannot be mapped to UNIX accounts. Local user accounts are not assigned UIDs with the mapping methods used for domain users; local user UIDs are assigned from a special range by VNX directly.

User authentication method must be set to NT and Unicode support must be enabled on the Data Mover for local users support.

Note: If a Windows Server compatible CIFS server is configured to accept Kerberos authentication only, local user accounts cannot log in to the server. Setting the server_cifs authentication to kerberos is a convenient way to disable local user login.

Important: After being enabled, local user support cannot be disabled. You can only disable individual local user accounts.

Create local user accounts

You can manage local user accounts through Windows User Manager or the User and Computer Management MMC snap-in. You cannot manage local user accounts by using

the VNX command line interface (CLI) or Unisphere. Local user accounts are stored in the local groups database on the CIFS server.

usrmgr.exe resources

For non-Windows NT platforms, the usrmgr.exe is available as a free download in the Windows Server Resource Kit Tools.

Supported account management functions

The following are the administrative functions supported for local user accounts on a Data Mover:

◆ Create a new user account

◆ Delete an existing user account

◆ Rename a user account

◆ Change user password from the Login window

◆ Reset a user password from any native Windows management interface

Supported username and password formats

Usernames and passwords must use these formats:

◆ Usernames can be up to 256 Unicode characters in length, cannot be terminated by a period, and cannot include the following characters:

" / \ [ ] : ; | = , + * ? < >

Note: Limits other than 256 characters may be imposed by the administration tools used to create user accounts. Windows User Manager and Computer Management MMC limit usernames to 20 characters.

◆ Passwords can be up to 255 Unicode characters in length.

◆ Comments can contain spaces and other nonalphanumeric characters, but must be enclosed by quotes if spaces are used.

Supported user properties

lists the supported and unsupported user properties when creating local user accounts on a Data Mover.

Table 7. Local user account features

Feature	Supported	Unsupported
New User dialog box: ◆ Username ◆ Full Name ◆ Description ◆ Password ◆ User must change password at next logon ◆ User cannot change password ◆ Password never expires ◆ Account disabled	All supported	
Group Membership	Supported	
User Environment profile: ◆ User profile path ◆ Logon script name ◆ Home directories		All unsupported
Dialin Information		Unsupported
Terminal Services profile: ◆ Terminal server profile path ◆ Terminal server home directory		All unsupported

Administrator accounts

The Administrator account is enabled by default and has full administrative rights to the CIFS server. The password you provide when you enable local users support becomes the initial password for the local Administrator account. You must change this password before logging in to the CIFS server with the Administrator account. Change the password for the local Administrator account on page 86 provides procedural information.

Note: You cannot disable the Administrator account on stand-alone servers.

Guest accounts

The Guest account has very limited user rights and is disabled by default. The Guest account provides a very simple access method for stand-alone CIFS servers. If you enable this account with an empty password, any user can access the CIFS server without authentication.

Important: The Guest account is not a member of the Authenticated Users group. Therefore, to ensure that your CIFS server remains secure, you should use the Authenticated Users group instead of the Everyone group when setting access control lists (ACLs) on shares.

If you have existing shares on the server with ACLs that use the Everyone group, change these ACLs to use the Authenticated Users group.

Note: The Administrator and Guest accounts can be renamed.

Other local user accounts

Local user accounts inherit the rights and privileges from the local groups to which they belong. Local user accounts can be created, deleted, and managed through Windows management tools.

Note: VNX supports the well-known Windows group names Everyone and Authenticated users. VNX does not support renaming these well-known groups.

Virtual Data Movers

A VDM is a software feature that allows administrative separation and replication of CIFS environments. A VDM houses a group of CIFS servers and their shares.

A VDM looks like a computer on the Windows network. It has its own event log, local user and group database, CIFS servers and shares, and usermapper cache. These are applicable when using NFS and CIFS to access the same file system on the same VNX file system.

EMC recommends that you create CIFS servers in VDMs. This provides separation of the CIFS server user and group databases, CIFS auditing settings and event logs. This is required if the CIFS server and its associated file systems are ever to be replicated by using VNX Replicator. An exception to creating a CIFS server in a VDM is when the CIFS server is to be used to route anti-virus activity.

Note: A default CIFS server and CIFS servers within a VDM or VDMs cannot coexist on the same Data Mover. A default CIFS server is a global CIFS server assigned to all interfaces, and CIFS servers within a VDM require specified interfaces. If a VDM exists on a Data Mover, a default CIFS server cannot be created. Avoid using a default CIFS server by specifying an interface for it to use.

Configuring Virtual Data Movers on VNX and *Using VNX Replicator* provide detailed information on VDMs.

Group policy objects

The Group Policy settings are stored in group policy objects (GPOs) that are linked to the site, domain, and organizational unit (OU) containers in the AD. The domain controllers replicate GPOs on all domain controllers within the domain.

Note: Data Mover security settings in the Unisphere online help provides more information on audit policy.

GPO support on VNX

VNX provides support for GPOs by retrieving and storing a copy of the GPO settings for each CIFS server joined to a Windows Server domain. VNX stores the GPO settings in a GPO cache on the Data Mover. Although there might be multiple CIFS servers on a Data Mover, there is only one GPO cache per Data Mover.

When you start the CIFS service on a Data Mover, VNX reads the settings stored in the GPO cache, and then retrieves the most recent GPO settings from the Windows domain controller. VNX also retrieves GPO settings whenever a CIFS server is joined to a domain. After retrieving the GPO settings, VNX automatically updates the settings every 90 minutes. Update GPO settings on page 117 provides procedural information.

CIFS servers on a Data Mover can have different GPO settings if they belong to separate organizational units. When a Data Mover has more than one CIFS server, the system processes the GPO audit and event log settings as explained in GPO conflict resolution on page 148.

Table 8 on page 35 summarizes the GPO settings that VNX supports.

Table 8. GPO settings

Setting	Default Values
Kerberos Max Clock Skew (min-utes)	5 minutes
LAN Manager Auth Level	From VDM registry LMCompatibilityLevel default: 1=Use NTLMv2 session security if negotiated

Table 8. GPO settings *(continued)*

Setting	Default Values
Digitally sign client communications (always)	Disabled
Digitally sign client communications (if server agrees)	Disabled
Digitally sign server communications (always)	Disabled
Digitally sign server communications (if client agrees)	SMB1 disabled, SMB2 enabled
NTLM SSP Minimum Client Security	From VDM registry NtlmMinClientSec default: 0
NTLM SSP Minimum Server Security	From VDM registry NtlmMinServerSec default: 0
Send unencrypted password to connect to third-party SMB servers	Not used
Disable machine account password changes	Password changes not disabled except if parameter cifs.srvpwd updtMinutes is 0
Maximum machine account password age	Parameter cifs.srvpwd updtMinutes (0: no password change)
Default Owner for Administrator Objects	Disabled
Audit account logon events	Disabled
Audit account management	Disabled
Audit directory service access	Disabled
Audit logon events	Disabled
Audit object access	Disabled
Audit policy change	Disabled
Audit privilege use	Disabled
Audit process tracking	Disabled
Audit system events	Disabled

Table 8. GPO settings *(continued)*

Setting	Default Values
Back up files and directories	Administrators; Backup Operator
Restore files and directories	Administrators; Backup Operator
Bypass traverse checking	"All supported local groups"
Generate security audits	Administrators
Manage auditing and security log	Administrators
Access this computer from the network	Enabled
Deny access to this computer from the network	Disabled
Take ownership of files or other objects	Administrators
EMC Virus Checking	Privilege disabled
EMC CEPP Bypass Event	Privilege disabled
Maximum security log size	500 KB
Restrict guest access to security log	Disabled
Retention period for security log	10 days
Retention method for security log	Overwrite events by days
Maximum system log size	500 KB
Restrict guest access to system log	Disabled
Retention period for system log	10 days
Retention method for system log	Overwrite events by days
Maximum application log size	500 KB
Restrict guest access to application log	Disabled

Table 8. GPO settings *(continued)*

Setting	Default Values
Retention period for application log	10 days
Retention method for application log	Overwrite events by days
Disable background refresh of Group Policy	Background refresh is not disabled
Restricted Groups	None
Group Policy Refresh interval (minutes)	90
Refresh interval offset (minutes)	0

Note: The SMB2 signing is enabled by default because the SMB2 signing specification rule is different than the SMB1. For SMB2, the traffic is signed only when either the client or the server requires signing for the communication.

For SMB1, the traffic is signed, once both the client and the server enable signing. For this reason the SMB1 default value is disabled to avoid signing the traffic when the client does not require.

Note: Time synchronization is done per Data Mover, not per CIFS server. If you configure multiple CIFS servers on a Data Mover for multiple domains, then all the time sources for these domains must be synchronized.

provides procedural information.

Support for restricted groups

Restricted groups are GPO security settings that allow the administrators to easily define and control the default membership for security-sensitive groups. Restricted groups are primarily used to configure the membership of local groups on a workstation or member servers of the domain.

Restricted groups define two properties:

◆ Members - The Members list defines who belongs and who does not belong to the restricted group. When a restricted groups policy is enforced, any current member of a restricted group who is not on the Members list is removed. Any user on the Members list who is currently not a member of the restricted group is added.

◆ MemberOf - The MemberOf list ensures that the restricted group is added to the groups that are listed under the MemberOf property. It does not remove the group from the other groups of which it is a member.

Note: Restricted groups are automatically applied after the CIFS service is started.

Manage and enforce ACL

Windows administrators use the Microsoft Management Console (MMC) Group Policy Object (GPO) to set and configure their Windows environment. The file systems object can be used to enter Access Control Entries (ACEs) to grant and limit access to the file system objects in Windows to the users and groups. A group of ACEs for a file system is called an Access Control List (ACL). Windows updates the file system ACLs periodically, according to the security rules set up by the administrator. If a rule is not set, it will run the update cycle every hour and a half (90 minutes).

The update cycle can be computer resource intensive, especially if the file system is large, and deep, and has a lot of directory branches. Also, since it may not be immediately updated, a security loophole may exist between the time the ACL is updated, and the GPO rule is updated. For these reasons, the operating system can initiate an update event of the file system ACLs to provide immediate changes to the file systems.

VNX for file provides a GUI tool that directly applies the GPO security settings to the file systems. It will have the same effect as applying the security update from a Windows server, but it will take a significantly shorter time to do so on large directories, because the security

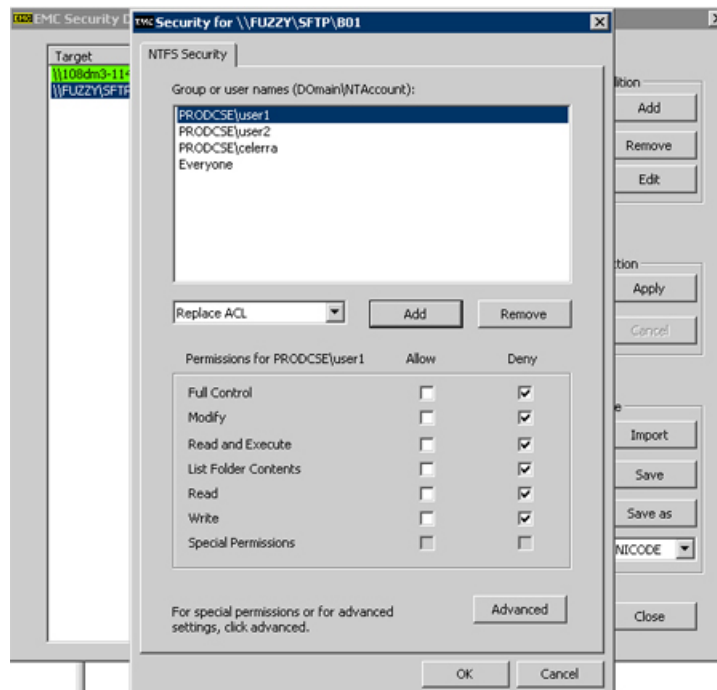settings are managed locally on the Data Movers. Figure 3 on page 40 shows how to add users and groups.

Figure 3. Adding users and groups

Delegating joins

In a delegate join, the active directory (AD) account creation is separated from the join action. Consequently, a user other than the one who created the computer account for a CIFS server in the AD can join the CIFS server to the domain.

Add the user performing the join to the local administrators group on page 136 and Delegate join authority on page 100 provide procedural information.

Table 9 on page 41 shows the domain join parameter values that you must set on VNX to perform a delegated join, in the same or disjoint namespace AD domain.

Note: Domains within the disjoint namespace forest that do not have the same hierarchical domain name are in a different domain tree. When different domain trees are in a forest, the tree root domains are not contiguous. Disjoint namespace is the phrase used to describe the relationship between different domain trees within the forest.

Table 9. Domain join parameter combinations

	djUseKpassword	djAddAdminToLg	djEnforceDhn
Join delegated to	1 (default)	0 (default)	1 (default)
Domain Admins Group Member (Microsoft default)			
Domain User Account			
Domain Global Group			
Domain Local Group	0		

Home directories

The VNX home directory feature lets you create a single share to which all users connect. You do not have to create individual shares for each user.

The home directory feature simplifies the administration of personal shares and the process of connecting to them by letting you associate a username with a directory that then acts as the home directory for each user. The home directory is mapped in each user profile so that upon login, the home directory is automatically connected to a network drive.

Note: If a client system (such as Citrix Metaframe or Windows Terminal Server) supports more than one Windows user concurrently and caches file access information, the VNX home directory feature might not function as desired. With the VNX home directory capability, the path to the home directory for each user appears the same to the VNX client.

If a user writes to a file in the home directory, and another user reads a file in the home directory, the second request is completed by using the cached data from the home directory of the first user. Because the files have the same pathname, the client system assumes they are the same file.

On Windows Server systems, you can enable and manage home directories through the VNX home directory management snap-in for MMC. *Installing Management Applications on VNX for File* provides information on installing the snap-in. The snap-in online help describes the procedures for enabling and managing home directories. provides procedural information.

Permissions and security

Before version 5.6.50.1, when a home directory was auto created by the system, the UNIX root (UID=0x0) was the owner of that directory and the permission applied to that directory was inherited from its parent folder or set to Everyone (group) Full_Control if nothing could be inherited.

Version 5.6.50.1 onward, the system provides new mechanisms to tighten control over access to home directories through the Access Control Lists (ACLs) applied to them. Specifically, this version adds a new registry flag that offers two new security options that apply to new, automatically created home directories. A third option for this flag is available for compatibility with its previous behavior.

Note: The default security applied to automatically created home directories has changed with version 5.6.50.1 and later versions. You can return to the previous security model by setting the registry entry to 0x2.

Important: EMC recommends to create a temporary VDM and file system to customize the ACL (registry entry value 0x1) with this new functionality before choosing an ACL for production use.

The registry entry can have the following values:

◆ 0x0 (default) - This option restricts the ACL to the owner. Only the user logging in will have access, and permission will be set to full control. The owner of the directory will be the user who logged in.

An Access Control Entry (ACE) on the parent folder ACL that grants the set of home directory users specific permissions within the parent folder only (not child folders) is required. It is recommended that you grant these permissions on the parent folder to the "Authenticated Users" group, which will include all homedir users, but will exclude unauthenticated users. Any group that contains the intended home directory users of a file system/folder may be utilized (such as "Domain Users"). The required permissions within the parent folder to be granted to this group are:

- Traverse Folder/Execute File
- List Folder/Read Data
- Create Folders/Append Data

◆ 0x1 - This option sets the ACL based on values inherited form the parent. Use the 0x0 setting only if inheritance from the parent is not allowed.

You must set an inheritable ACE applied to the CREATOR OWNER SID in the parent folder's ACL. This CREATOR OWNER ACE must allow the users to create, modify, execute, and delete files and folders (or have Full Control) in their home directory. Set this ACE in the parent directory ACL and apply to 'Subfolders and files only' or 'This folder, subfolders and files'. Failure to apply this ACE will result in the home directory user being unable to use the home directory. Other ACEs may be applied and inherited from the parent ACL as desired.

Further, an ACE on the parent folder ACL that grants the set of home directory users specific permissions within the parent folder only (not child folders) is required. It is recommended that you grant these permissions on the parent folder to the "Authenticated Users" group, which will include all homedir users, but will exclude unauthenticated users. Any group that contains the intended home directory users of a file system/folder may be utilized (such as "Domain Users"). The required permissions within the parent folder to be granted to this group are:

- Traverse Folder/Execute File
- List Folder/Read Data
- Create Folders/Append Data

Note: Permissions granted by this ACE should not be allowed to propagate to subfolders through inheritance unless that is your specific intent.

◆ 0x2 - This option reverts to the old behavior (UNIX root owner, Inherit parent ACL or "Everyone Full Control" if nothing has been inherited). The UNIX root user will own the home directory folder.

When the home directory folder is created, it can inherit an ACE from the ACL of its parent folder provided the parent folder ACL contains ACEs that apply to subfolders. When the ACL is inherited, you need to ensure that there is an ACE inherited by the home directory ACL when it is created that gives read, write, execute, and delete permission (or Full Control) to a group in which the home directory user will be a member. This ACE should be set in the parent directory ACL and applied to 'Subfolders and files only' or 'This folder, subfolders and files'. Failure to apply this ACE will result in the home directory user being unable to use the home directory. Other ACEs may be applied and inherited from the parent ACL as desired.

If no ACE can be inherited from the parent folder ACL, then the Everyone group will be granted Full Control of the home directory when it is created.

EMC recommends that you use the 0x2 setting only when ACL inheritance from the parent folder is not allowed. If you wish for the home directory folder to inherit its ACL, EMC recommends that you use the 0x1 registry entry value so that the home directory folder's owner will be the actual home directory user (unless root ownership is specifically desired).

EMC recommends that you do not share or export the parent folder in 0x2 mode unless you manually adjust ACLs on home directories to exclude all users but those that should have access.

Each Data Mover or X-blade and VDM has its own registry, and therefore its own value for this security option. All have the same default value. The registry key and value are:

Key: **HKEY_LOCAL_MACHINE\Software\EMC\Homedir**

Value: **Flags**

Type: DWORD

Data: 0x0 (default)

To change this registry setting, use regedit or regedt32 from Windows to connect to the CIFS Server's registry and edit the Flags value. You do not need restart the CIFS service for the registry change to take effect.

Restrictions to using the home directory

A special share name, HOME, is reserved for the home directory feature. Because of this limitation, the following restrictions apply:

◆ The home directory feature is not available on CIFS servers configured with SHARE or UNIX-level security.

◆ If you have created a share called HOME, you cannot enable the home directory feature.

◆ If you have enabled the home directory feature, you cannot create a share called HOME.

Appendix A provides additional information.

Alternate data stream support

With the release of Windows NT, Microsoft introduced the Windows NT File System (NTFS) and the concept of alternate data streams (ADS). This feature is also known as multiple data streams (MDS). Data streams are independent resources that store data and information about the file. Unlike the file allocation table (FAT) file system, in which a file consists of only one datastream, NTFS uses different data streams to store the file and metadata such as file access rights, encryption, date and time information, and graphic information.

Microsoft originally created ADS so that a server that is using NTFS could act as a file server for Macintosh clients. Macintosh hierarchical file system (HFS) uses two basic elements to represent files, as shown in Table 10 on page 44.

Table 10. HFS elements

Element	Purpose
Data fork	Stores data for a file
Resource fork	Stores information about a file

NTFS files contain one primary data stream and, optionally, one or more alternate data streams. The primary data stream acts as the data fork and the alternate data streams act as the resource forks.

For files, you can view and set this additional information from the Summary tab in the file Properties dialog box as shown in Figure 4 on page 45.
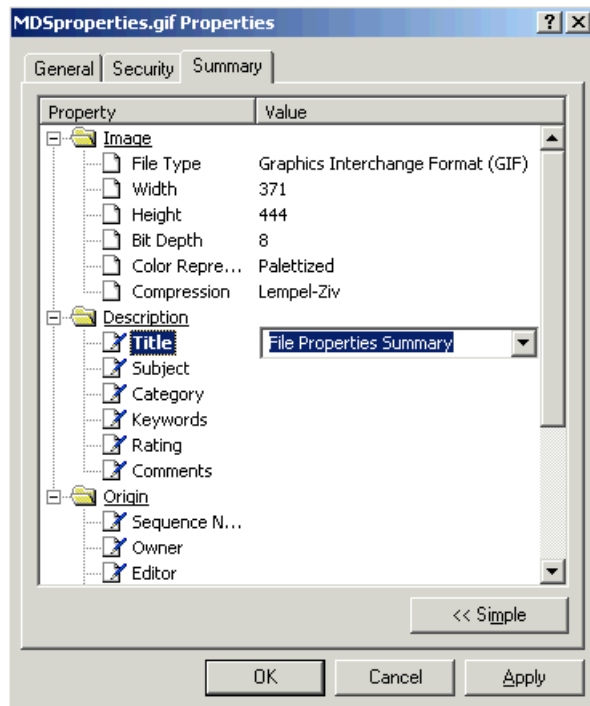
Figure 4. Properties dialog box — Summary tab

The VNX supports ADS for files and directories with the following restrictions:

◆ Directory streams are supported on mount points. If a file system is mounted on a mount point, only the root directory streams of the mounted file system are visible. If no file system is mounted, the streams of the mount point are visible.

◆ There is a limit of 64,000 streams per file or directory.

ADS support is enabled by default. Disable alternate data streams on page 120 provides procedural information.

SMB protocol support

Server message block (SMB) is the underlying protocol used by the CIFS protocol to request file, print, and communications services from a server over a network through TCP ports. The protocol level is negotiated by the client and server when establishing a new SMB connection. VNX supports both SMB1 and SMB2; SMB1 is enabled by default.

Note: SMB2 protocol support is available with Microsoft Windows Vista and Microsoft Windows Server 2008 systems. SMB2 has an improved performance over SMB1. With Windows 8 support, SMB3 protocol is supported by VNX from version 7.1.61.0 onwards.

Manage SMB2 and SMB3 protocols on page 124 provides procedural information.

SMB 2.1 features supported by VNX

VNX supports the following SMB 2.1 features with Microsoft Windows 7 and Windows 2008 Release 2 Server:

◆ The lease feature as compared to the oplock mechanism enables the client to keep the data cache synchronized with the server for a longer time. SMB2 leases are rarely broken as compared to oplocks, therefore, the performance improves by reducing the network traffic between the SMB2 client and the server. The parameter smb2.capabilities allows you to specify the SMB2 capabilities supported by the CIFS servers of the complete Data Mover including the Virtual Data Movers. Modifying this parameter affects the SMB negotiation when new SMB2 clients connect to the Data Mover. The *Parameters Guide for VNX for File* provides additional information on managing the SMB protocol.

◆ The unbuffered write option gives an opportunity for the client to write a file with no server-side buffering, regardless of how the file was opened. This prevents the client to reopen the file with the FILE_FLAG_WRITE_THROUGH option for performing the unbuffered write.

provides conceptual information.

SMB signing

SMB signing is a mechanism in the SMB protocol that is used to ensure that a packet has not been intercepted, changed, or replayed. SMB signing only guarantees that the packet has not been changed by a third party. Signing adds an 8-byte signature to every SMB1 packet. SMB2 uses a 16-byte signature. The client and server use this security signature to verify the integrity of the packet.

To use SMB signing, the client and the server in a transaction must have SMB signing enabled. By default, Windows Server domain controllers require that the clients use SMB signing. SMB signing is enabled by default on all CIFS servers created on Data Movers.

provides additional information.

Note: On Windows NT (SP 4 or later) SMB signing is set using the registry; Windows Server domains onward this is a GPO policy.

Data Movers use client-side and server-side SMB signing depending on the situation. The following are some examples of when a Data Mover uses each type of signing:

◆ Data Mover acts as a server:

   · When a client maps a share

   · With file migration service

◆ Data Mover acts as a client:

- When retrieving group policy objects (GPO) settings
- With file migration service

Configure SMB signing on page 121 provides procedural information.

Symbolic links

Symbolic links are special nodes created by UNIX clients that point to another node (a file or directory called the target node). The target node is defined in a symbolic link node as a pathname. Normally, NFS symbolic links have no meaning to Windows clients because the client must resolve or follow the symbolic link to its target. However, under certain circumstances, VNX resolves symbolic links for Windows clients so that these clients can access the same files and directories as UNIX clients through a symbolic link.

By using symbolic links, CIFS clients can access multiple file systems on a Data Mover from a single share. This gives the appearance of one large namespace when it actually consists of individual file systems linked together with symbolic links. After enabling the shadow followabsolutpath parameter, a single CIFS share that provides access to multiple file systems on a Data Mover can be created. Access symbolic links through CIFS clients on page 130 provides procedural information.

If the Data Mover is able to access the target on behalf of the CIFS user, the user is able to see the target of the symbolic link rather than the link itself. The user does not realize that they a symbolic link has been followed. If the target is not accessible, the users see the symbolic link as a file but cannot access that file.

By default, VNX resolves symbolic links for Windows clients when:

- The target is relative to the directory in which the link itself resides. That is, the target does not contain an absolute path (full pathname).

- The target is within the same share as the link itself. The target does not have a pathname that refers upwards by using the '..' component.

> **⚠ CAUTION**
> When a Data Mover resolves symbolic links on behalf of CIFS clients, users cannot distinguish between the symbolic link itself and the target of the symbolic link. Therefore, if a symbolic link refers to a directory, and a Windows user attempts to delete the symbolic link, the link and the contents of the directory that the link references are deleted.

> **⚠ CAUTION**
> Do not use Microsoft Office applications on files represented by symbolic links. When a file is updated, Microsoft Office creates the updated file in the directory containing the symbolic link, instead of the symbolic link target directory.

> **⚠ CAUTION**
> When the target is unreachable, a symbolic link cannot be removed through a Windows client. During the removal process, Microsoft Explorer tries to open the file, which is unreachable, and fails. In that case, the symbolic link needs to be removed through a UNIX client.

Symbolic link limitations on page 146 provides additional information.

SMB2 support for symbolic links

The SMB2 protocol supports symbolic links like UNIX. This link is transparent for the application and allows access to the destination file system object (file or directory).

The different types of symbolic links that you can create on a system are:

- The target of the link can be a file or a directory. Both are supported. The creation of a link on a non-existing target is also supported.

- Absolute symbolic links are links that point to the absolute path of the file or folder, for example, C:\windows.

- Relative symbolic links are links that point to a file or directory using the relative path, for example, ..\..\file.txt.

- Universal naming conventions (UNC) symbolic links are links that point to a network file or directory, for example, \\server\share1\dir\foobar.txt.

provides procedural information.

Opportunistic file locking

Opportunistic file locks (oplocks) improve network performance by allowing CIFS clients to locally buffer file data before sending it to the server. These locks are configured per file system and are on by default. Unless you are using a database application that recommends oplocks be turned off, or if you are handling critical data and cannot afford any data loss, leave oplocks on. VNX supports level II, exclusive, and batch oplocks in the following ways:

- Level II oplocks: When held, a level II oplock informs a client that multiple clients are currently accessing a file, but no client has yet modified it. A level II oplock lets the client perform read operation and file attribute fetches by using cached or read-ahead local information. All other file access requests must be sent to the server.

- Exclusive oplocks: When held, an exclusive oplock informs a client that it is the only client opening the file. An exclusive oplock lets a client perform all file operations by using cached or read-ahead information until it closes the file. At this time the server must be updated with any changes made to the state of the file with respect to the contents and attributes.

- Batch oplocks: When held, a batch oplock informs a client that it is the only client opening the file. A batch oplock lets a client perform all file operations by using cached or read-ahead information including opens and closes. The server can keep a file opened for a client even though the local process on the client machine has closed the file. This mechanism curtails the amount of network traffic by letting clients skip the extraneous close and open requests.

Note: Filter oplocks are not applicable to a remote file server.

provides procedural information.

File change notification

Applications that run on Windows platforms, and use the Win32 API, can register with the CIFS server (or local OS) to be notified of file and directory content changes, such as file creation, modify, or rename. For example, this feature can indicate when a display needs to be refreshed (Windows Explorer) or when the cache needs to be refreshed (Microsoft Internet Information Server), without having to constantly poll the CIFS server (or local OS).

The Win32 API, and thus the CIFS protocol, supports the ability to specify the root of the directory tree that requires monitoring. If a subdirectory is specified, changes occurring above the specified directory will not notify the application.

To monitor changes occurring to directories beneath the specified directory, the application can also set the WatchSubTree bit. By default, monitoring for changes occurring in up to 512 directory levels beneath the root is supported. After receiving a change notification response, the application must reissue or reset the monitoring process to be notified of further modifications. Changes can also be buffered and notification can be satisfied by a single response to the client requesting the monitoring. Configure file change notification on page 102 provides procedural information.

Note: The file change notification feature can only be used in a pure CIFS environment. It is supported only when the user authentication method is set to NT on the Data Mover.

Event log auto archive

With Windows operating system, applications can use the event logging mechanism to log their own events. VNX currently supports three such event logs that is security, system, and applications.

The physical format of these logs use a Microsoft format called 'evt' that has a limitation of 4 GB in size because there are some fields stored on 32-bit integers. Windows Server 2008 has introduced a new format 'evtx' that does not have this limitation.

The event log auto archive feature allows to automatically archive an event log on a particular trigger policy and to continue the logging on a new event log without losing any events. The archive is triggered on a time or on an event log size basis defined by parameters in the Windows registry. This allows to overcome the 4 GB limitation of the 'evt' format by enabling the possibility to keep as many events as needed. The only limitation is the file system size. You can also specify a retention policy to keep the event log archives before they can be recycled based on the duration or the total archive disk size. Table 11 on page 50 provides more information.

All the parameters are stored in the Windows registry of each VDM. Therefore, each VDM will have its own configuration. The parameters can be viewed and edited with standard tools like regedit.

The archive files of a given log file are stored in the same directory as the active event log file.

Important: The auto archive will be effective only if the active log file is not located on the root file system or on a VDM root file system and if the event log retention is set to infinite. It is recommended to use a dedicated file system for performance reason.

The location of an active log file can be changed by modifying the registry entry:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Logname\File`

The retention of the event log can be set from the event viewer or in the following registry entry:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Logname\Retention`

Each time an archive is created, it is renamed with the following name:

Logname-YYYY-MM-DD-HH-MM-SS.evt

where:

* Logname is the name of the log, for instance, security
* YYYY: year
* MM: month
* DD: day
* HH: hour
* MM: minutes
* SS: seconds

The date part of the archive log file name is the GMT date when the file has been archived. No event in this file is later than this date. If the file system or the log file becomes full, then an event is sent to the Control Station so that the administrator can take appropriate actions.

The evt format of the file is readable by the standard Windows event viewer.

Note: Depending on the system memory, it may not be possible to view huge log files due to a limitation in Windows 2000, Windows XP, and Windows Server 2003 systems. However, Windows Vista, Windows 7, and Windows Server 2008 do not have this limitation.

Table 11. Windows registry parameters for event log auto archive

Key Name	Type	Comments
AutoArchiveEnabled	DWORD	1 = auto archiving is enabled for this log
		0 = auto archiving is disabled for this log

Table 11. Windows registry parameters for event log auto archive *(continued)*

Key Name	Type	Comments
AutoArchiveTriggerPolicyTime	STRING	Specify that the active log file is archived on a time interval. This field has the following format: ◆ Number of days followed by 'days', for example, 40days ◆ Number of hours followed by 'hours' for example, 300hours
AutoArchiveTriggerPolicySize	STRING	Specify that the active log file is archived if the log file size reaches a given size. This field has the following format: ◆ Percentage of the maximum event log size, for example, 50% . The maximum event log size is defined by using the Windows Event Viewer or directly in the log registry key 'MaxSize' ◆ Size in kilobytes followed by 'kb', for example, 512kb ◆ Size in megabytes followed by 'mb', for example, 128mb ◆ Size in gigabytes followed by 'gb', for example, 3gb
AutoArchiveRetentionPolicyTime	STRING	Specify the retention policy for when archive files can be removed is based on time duration. The format is either: ◆ Number of days followed by 'days', for example, 40days ◆ Number of hours followed by 'hours' for example, 300hours Note: If a retention policy is not set, then the archived files are not deleted. In this case, delete or move these files manually before the file system becomes full.
AutoArchiveRetentionPolicySize	STRING	Specify the retention policy for when archive files can be removed is based on the total size occupied by all archives of the event log. The format is either: ◆ <Percentage of the max size of the log file>%, for example, 400%. The maximum log size is the value that can be set in the Windows event viewer ◆ Size in kilobytes followed by 'kb', for example, 512kb ◆ Size in megabytes followed by 'mb', for example, 128mb ◆ Size in gigabytes followed by 'gb', for example, 3gb Note: If a retention policy is not set, then the archived files are not deleted. In this case, delete or move these files manually before the file system becomes full.

Table 11. Windows registry parameters for event log auto archive *(continued)*

Key Name	Type	Comments
AutoArchiveLastArchiveDate	STRING	GMT date of the last archive of this log. The format is YYYYMMDDHHMMSS. This field is read-only and is valid only if auto archive has been enabled.

SMB 3.0 protocol support

Windows Server 2012 introduces the new version 3.0 of the SMB protocol.

With Windows 2012, Microsoft will deliver file based storage for Hyper-V and SQL storage. Hyper-V can store virtual machine files, such as configuration, virtual hard disk (VHD) files, and snapshots in file shares over the SMB 3.0 protocol.

SMB in Windows Server 2012 includes the new SMB 3.0 protocol with new improvements in the features and functionality. Some of them can be listed as:

◆ Windows Server 2012 delivers on continuous availability of file based storage by efficiently utilizing industry standard storage, network and server components.

◆ SMB Encryption provides secure access to data on SMB file shares. It protects data on untrusted networks by providing end to end encryption of SMB data.

◆ MultiPath IO (MPIO) allows to optimize the usage of the bandwidth, by opening multiple Transmission Control Protocol (TCP) connections on different links.

SMB 3.0 protocol support for Continuous Availability

SMB 3.0 introduces several methods for achieving Continuous Availability for applications or network shares in the Windows environment:

◆ VNX File Server failover to Standby Server with transparent Client reconnect

◆ Windows 2012 Client cluster failover using Application ID

◆ Ability to configure multi-path IO (MPIO) with multiple TCP connections to CIFS server/shares/sessions

VNX File Server Active/Passive CA

The solution for providing Continuous Availability (CA) for the VNX File Server is to implement Active/Passive CA failover to a Standby Server. If the primary File Server fails, it will failover to a Standby Server, and SMB 3.0 capable clients will transparently reconnect if the failover occurs within 60 seconds or less. VNX File Server configuration for this method requires the establishment of a Standby Server for the Primary Server, and network Shares that are mounted and exported with a special 'smbca' flag, as shown below:

Mount File Server file systems with smbca option, and export Shares with type=CA option:

```
# server_mount server_2 -o smbca fs1

server_export server_2 -P cifs -name fileshare -option type=CA /fs1
```

Note: CA mount and Export options are not supported in the Unisphere GUI.

VNX Standby Server Failover Use Case

1. The SMB 3.0 client accesses the SMB 3.0 server on the production Data Mover.

2. The production Data Mover has a failure (software, hardware, or transparent upgrade) and is failed over the standby Data Mover.

3. The SMB 3.0 client reconnects to the standby Data Mover, to the same CIFS server and recovers the same context as before the failover.

Default VNX File Server CIFS Timeout

To support VNX File Server Active/Passive CA, the File server uses a CIFS parameter (smb2.maxCaTimeout), with a default timeout value of 120 seconds. This value can be configured from 0-180 seconds, depending on customer requirements. *Parameters Guide for VNX for File* provides more information on how to modify this parameter.

To address this issue, SMB 3.0 has introduced persistence for durable handles. Persistent handles allow a server to save most of metadata on disk associated to an open files. When the standby server restarts, it re-establishes all the open files that were present before the failover.

Note: VNX for Block does not have a single point of failure due to multiple access nodes and cannot share data across multiple hosts.

Windows 8 Cluster CA ApplicationID solution

To mitigate client failure, the SMB 3.0 client also runs on Windows cluster:

1. The application opens a file and sets lock on the SMB 3.0 server.

2. In case of a failure of one of the nodes (software or hardware), the cluster moves the application to the other node.

3. The application then re-opens its context on the SMB 3.0 server from the other node. Typical applications are SQL server, IIS, or Hyper-V VM.

To address this issue, SMB 3.0 has introduced the concept of application ID, so now the application after a failover to the other node will not conflict with its previous "session" from the first node because it is identified by an ID that does not change with the failover (in particular with its own resilient handles).

Performance improvements with Windows 8

Windows 8 also introduces some improvements to performance through the following features:

◆ Multi Path IO — Introduction of the Multi Path IO (MPIO). A user session can be associated to more than one TCP connections. If one TCP connection is broken, the user session can still continue using the remaining TCP sessions. Obviously, the TCP connections must not use the same NIC. Besides reliability, MPIO will also allow to optimize the usage of the bandwidth, by opening multiple TCP connections on different links.

   The basic process flow of the MPIO constitutes the client that establishes a standard TCP connection as usual. The client then requests all the available interfaces of the server (not necessarily registered to DNS). To establish an additional TCP connection, the process is repeated exactly the same way as the SMB2_SESSION_SETUP, except for specifying the sessionID of the user session on the first connection. Eventually, the client does the tree connection which is then valid on all TCP connections associated to the session. Thus the MPIO connection is very simple and requires little change from network protocol perspective.

◆ Directory Lease — The SMB2 client uses a directory cache associated to a timeout. This dramatically improves performance and avoids the numerous directories listing over the network. However the cache may be not up to date. To resolve this, SMB 3.0 extends the concept of lease to the directory. This way a client can set a lease on a directory and is automatically notified when there is a content change. There is no configuration required for VNX in order to support this capability.

◆ Branchcache V2 — SMB 3.0 also introduces BranchCache V2. BranchCache allows a client in branch offices to retrieve data locally when available instead of from the distant main office. For this release, the VNX File Server as a BranchCache "Content Server" has simplied the data hash mechanism. BranchCache on page 57 provides more information about BranchCache. BranchCache V2 is an extension of BranchCache V1, a feature delivered by Microsoft in Windows 7 & Windows Server 2008R2. A BranchCache V2 client requests a Hash File v2 when all the following conditions are met:

   • The SMB2_TREE_CONNECT is returning the flag SHI1005_FLAGS_ENABLE_HASH_V2

   • The GPO to force client using the BranchCache V1 format is not enabled

   • The client is configured in hosted cache mode.

There is a new format for the hash files. Microsoft documents on http://msdn.microsoft.com/en-us/library/dd303704.aspx provide more information about the hash files.

New GPO of Windows 8 domains

Domain Controllers of Windows 8 domain manages new GPO that need to be supported by the DART:

Location: "Computer Configuration\Policies\Administrative Templates\Network\Lanman Server\

Setting: "Hash Version support for BranchCache"

◆ Value: 1=support BranchCache V1 only

◆ Value: 2=support BranchCache V2 only

◆ Value: 3=supports BranchCache V1 and V2

Remote Volume Snapshot Service for SMB 3.0

In order to enable remote backup of an SMB 3.0 storage, Microsoft has extended its well known Snapshot framework named VSS. With this new version of Windows, VSS has been moved from WMI to MSRPC protocol to make it possible for third parties to support it. Remote Volume Snapshot Service (RVSS) not only allows taking remote snapshot but it allows taking a consistent set of snapshots across different servers and SMB shares.

This topic describes the Remote Volume Snapshot Service for SMB 3.0.In order to enable remote backup of a SMB 3.0 storage, Microsoft has extended its well known Snapshot framework named VSS.

The RVSS feature is implemented in the DART through a new MS-RPC interface. This interface contains 13 functions defined in the Microsoft document [MS-FSRVP].pdf, available at http://msdn.microsoft.com/en-us/library/hh554852(v=prot.10).aspx .

SMB encryption

SMB 3.0 in Windows 2012 provides secure data transfer by encrypting the data in-flight. This protects data transfer from untrusted networks.

The SMB3 encryption provides the following benefits:

◆ SMB encryption can provide a cost benefit, since it does not require IPSec, specialized hardware, or WAN accelerators.

◆ SMB encryption is easily configured on the VNX File Server, either on a per-share basis using a new server_export option, or on a per-CIFS server basis, after modifying various registry settings on the VNX CIFS server.

SMB messages on the network are encrypted by using the AES-CCM cryptographic algorithm. You can configure the message encryption per share by using a new share type with the

server_export command. *EMC VNX Command Line Interface Reference for File* provides more information about this. Once defined as encrypted, an SMB3 client needs to encrypt all the requests related to this share, and a share defined as encrypted is no longer accessible by default from SMB1 and SMB2 clients (that do not support the SMB encryption). The setting can also be configured through the CIFS server Registry.

Encryption Settings

The messages encryption per share is configured using a new share type with the server_export command. Once defined as encrypted, any SMB3 client should encrypt all the requests related to this share.

SMB encryption can be implemented on VNX by using one of the following methods:

◆ Set-up individual VNX File Shares for encryption using the new server_export option, "type=Encrypted":

```
# server_export server_2 -P cifs -name smben -o type=Encrypted
/smb30encrypt
server_2: done
```

◆ Set-up VNX File CIFS Server encryption by accessing the CIFS Server registry.

Open the Registry Editor from a Windows Administrative Management station, navigate to the following registry values, and change the values to those that match your required configuration.

New values added into the DART registry are:

Key: HKLM\CurrentControlSet\Services\LanmanServer:

Value	Type	Default	Description
EncryptData	DWORD	0	If set, all the sessions established from any SMB3 clients to the CIFS server should be encrypted.
RejectUnencryptedAccess	DWORD	1	If set and if the client should encrypt his message and if he sends unencrypted message, then the server return an ACCESS_DENIED error.

Note:

◆ If RejectUnencryptedAccess=0, then the server treats encrypted and unencrypted requests with no difference.

◆ If RejectUnencryptedAccess=1, then SMB1, SMB2.0, and SMB2.1 clients are not able anymore to access to an encrypted share or to a CIFS server that requires encrypted sessions.

Planning considerations

Table 12 on page 57 summarizes the tasks that you need to perform in a Windows Server environment before you start CIFS configuration.

Table 12. Preliminary CIFS setup

Action	Procedure
Enable internationalization support	Enable internationalization support on page 23
Create network interface	Network interfaces and CIFS servers on page 21
Configure NTP server to synchronize date and time	NTP servers on page 18
Configure DNS servers	DNS servers on page 18
Join the domain	Create a domain account in Active Directory on page 64
Create, mount, and export file system for CIFS access	Mount a file system for CIFS access on page 70
Configure quotas	Quotas on page 24

BranchCache

BranchCache is a new Microsoft feature that is introduced in the Windows 7 and Windows Server 2008 R2 operating systems. When the feature is enabled, it creates a cache of the content from the file and web servers, locally within a branch office. A client from the same network can request the file and download it from the local cache, instead of downloading it from the wide area network (WAN). BranchCache optimizes the local link utilization and the responsiveness of applications and reduces the WAN bandwidth consumption.

The article explaining BranchCache in Windows 7 and Windows Server 2008 R2 Overview on the Microsoft Technet website provides detailed information about the BranchCache feature.

To be able to participate as a content server for BranchCache, the operating system must be able to provide a signature (also called SMB hash file) of the data for any file (greater than 64 KB by default) requested by the SMB2 client.

Note: The VNX File OE supports BranchCache only by using SMB2.1, as a Central Office "Content Server." Refer to the configuration steps below to configure the VNX CIFS server for BranchCache operation.

Configuring BranchCache on VNX

The VNX content server configuration is similar for the Hosted Cache mode and the Distributed Cache mode:

1. To enable BranchCache service on a per Data Mover basis, use this command syntax:

    ```
    # server_cifs <movername> -smbhash -service enable
    ```

    Where:

    <movername> = name of the Data Mover

2. To enable hash support on each CIFS Share to be used for supporting Branch Cache clients, use this command syntax:

    ```
    # server_export <movername> -name <fs_name> -option <netbios_name>
    type=hash /<fs_name>
    ```

    Where:

    <movername> = name of the Data Mover

    <fs_name> = name of the file system

    <netbios_name> = associated NETBIOS name

    Example:

    ```
    # server_export server_2 -name fs1 -option netbios=inyo1,type=hash
    /fs1
    ```

3. Configure Hash Publication using VNX File Server Registry or using GPO policies:

    *   GPO

        Run: gpedit.msc ➤ **Computer Configuration** ➤ **Administrative Templates** ➤ **Lanman Server** ➤ **Hash Publication** for BranchCache

        *   1 Disallow hash publication on all shares

        *   0 Allow hash publication only for specific shares

        *   2 Allow has publication for all shares

> Note: GPO policies take precedence over manual registry entries. VDMs can only make use of GPO policies for enabling Hash publication, not registry entries.

- Registry configuration

  Run: regedit.msc ➤ **File** ➤ **Connect Network to Registry** ➤ **CIFS_Server** ➤ **HKLM** ➤ **Software** ➤ **EMC** ➤ **SmbHash** > HashPublication: 0x00000001 (Default value 1, which is no hash publication allowed)

  > Note: Double-click to edit and set to 0 or 2, similar to the GPO values outlined above.

4. To stop and restart the VNX File CIFS service to enable the SMBHash feature (the feature is not running until this is done), use the following commands:

```
# server_setup server_2 -P cifs -o stop
```

Output:

```
server_2 : done
# server_setup server_2 -P cifs -o start
```

Output:

```
server_2 : done
```

5. Configure the Windows Clients for Branch Cache operation. Microsoft BranchCache deployment guide provides more information about this.

6. To verify the VNX File Branch Cache configuration, operation, and statistics, use the following commands:

```
$ server_cifs -smbhash -audit enable (use Event Viewer to review)

$ server_cifs server_2 -smbhash -info

$ server_stats server_2 -list |grep -i branch

$ server_export server_2
```

SMB Hash File

Format

The SMB Hash File is defined by the [MS-PCCRC] and [MS-SMB2] Microsoft documents. It is generated only on demand for files with size greater than 64 KB by default.

Storage

SMB Hash Files are stored in a dedicated directory in the file system containing the content file. The size of this directory is not constrained; it is below the limit of 1 percent of the total file system size in blocks. However, for performance reasons, if a content file is deleted or modified, the corresponding SMB Hash File is not updated or deleted. If this limit is reached then obsolete SMB Hash Files will be deleted, from time to time, to free up disk space. The selection of the SMB Hash Files to be deleted will be done as follows:

◆ Delete all SMB Hash Files corresponding to a content file that does not exist.

◆ Delete all obsolete SMB Hash Files. This includes the SMB Hash Files that have:

• The last change time of the content file stored that is different than the actual last change time of the content file.

• The size of the content file stored is different than the actual size of the content file.

GPO

Hash generation is enabled by using the GPO. The corresponding GPO is: `Computer Configuration\Policies\Administrative Templates\Network\Lanman Server\Hash Publication for BranchCache`.

This GPO is an integer with 3 possible values:

◆ 0: Allow hash publication only for shared folders with flag SHI1005_FLAGS_ENABLE_HASH set.

◆ 1: Disallow hash publication on all shared folders. No SMB Hash Files can be generated.

◆ 2: Allow hash publication for all shared folders. SHI1005_FLAGS_ENABLE_HASH flags of shares are ignored.

By default, this GPO is not set in the domain. So hash generation and publication are defined by the local registry of the DART which is disabled by default as for Windows 2008 R2 server.

Note: *Parameters Guide for VNX for File* provides more information about the parameters that are supported by this feature. *EMC VNX Command line Interface for VNX for File* provides more information on the options related to the server_export and server_cifs commands. *Managing Statistics for VNX* provides information on the statistics added to the server_stat command.

Events generated by the SMB Hash File Generation

Audit

For the BranchCache service, you can enable its usage per CIFS server or share. However, there is a single event log that is generated as there is only one BranchCache service for all the Data Movers. To view this log with the computer manager MMC tool, you must connect to the CIFS server that is on the physical Data Mover.

By default no audits are generated. Audits generation is configured by using the server_cifs –smbhash –audit CS command.

Events generated internally or by the Control Station have "user" field filled with "System" and "computer" filled with NAS version.

Events generated by the protocol have "user" field equal to the logged user name and the "computer" by the NetBIOS name on which this user is logged in.

Service

Service events monitor the start or stop of the service as well as any configuration parameters changes.

Task

This allows auditing the tasks that have been executed and the ones that are pending. For a given task, there is always the given set of events generated:

1. An event when a new task has been added. This event also describes the task itself.

2. An event when the task execution has started (Id=512).

3. An event when the task execution has ended.

Additionally in between the add task and the end task events, two additional events may be generated mentioning if an error (Id=513) or a warning (Id=514) had occurred. For instance, if a task has been cancelled, then an additional event 513 is generated mentioning that the task has been canceled and why.

A set of events relative to a given task can be linked via the "TaskId" parameter which is always present.

At last, the last events in this category which could be generated are mentioning that a task has been rejected and why, for instance if the same task already exists.

Access

Access events allow monitoring access by the SMB2 protocol to the SMB Hash Files. It can help in some circumstances to troubleshoot general BranchCache issues.

Performance of SMB hash generation

- The SMB2 clients get to read the data with less usage of the server resources.

- The performance of the protocols does not get affected. The hash files are updated with the modifications only when the SMB2 clients request for this update.

- The small size of the SMB Hash File leads to the minimal usage of the disk space. However, there is an extra usage of the disk space required to store the SMB Hash Files.

- The computation of the hash file may considerably impact the CPU usage.

Impact of SMB hash generation

The SMB hash generation service takes place at high level and does not impact other components. This includes:

- If the SMB Hash File needs to be computed for an offline file, the data needs to be recalled from the secondary storage as it is done for a standard client access enforcing the File Mover policy.

- SMB Hash Files are bad candidates as they are unique by essence.

- Files that are frequently changed, prove to be "bad candidates" for deduplication. It is recommended to enable a filter to exclude these files from SMB Hash Files generation.

- If you take a snapshot during the SMB Hash File generation, the hash file gets ignored. The status appears as "STATUS_HASH_NOT_PRESENT" and the normal SMB protocol access takes place.

- SMB Hash Files are self descriptive (no external parameter is needed to decode the file). They reside on the same file system as that of the corresponding content files. You can replicate SMB Hash Files.

- Backup is not required for SMB hash Files. When you restore the corresponding content file, the hash file becomes obsolete as with Windows.

3

Configuring

Important: Review the Planning considerations on page 57 before you begin CIFS configuration.

The tasks to configure CIFS on a Data Mover are:

- Add a CIFS server to a Windows domain on page 64
- Create a domain account in Active Directory on page 64
- Add a WINS server on page 64
- Start the CIFS service on page 65
- Create a CIFS server for Windows Server environments on page 65
- Join a CIFS server to a Windows domain on page 67
- Mount a file system for CIFS access on page 70
- Create shares for CIFS users on page 71
- Create a stand-alone CIFS server on page 75
- Create a CIFS share on MAC OS by using the GUI on page 76
- Create a CIFS share on MAC OS manually on page 77

Add a CIFS server to a Windows domain

Before adding a VNX-based CIFS server to a Windows domain, you must add a machine account to the Windows domain controller to identify the CIFS server, which you create in Create a domain account in Active Directory on page 64.

Note: This step is not necessary if you are using UNIX or SHARE user authentication.

1. On the primary domain controller, select **Start ➤ Administration Tools ➤ Server Manager**.

2. From the Computer menu, select **Add to Domain**. The **Add Computer to Domain** dialog box opens.

3. Select **Windows NT Workstation or Server** and type the NetBIOS name of the CIFS server in the **Computer Name** field. Click **Add**.

   Note: The NetBIOS name is the name used to identify the CIFS server you create in Create a domain account in Active Directory on page 64.

Create a domain account in Active Directory

The user account must belong to a domain in the same Active Directory forest as the domain the CIFS server is joining.

1. Create a new computer with the same comp_name you will use to create the CIFS server in your environment.

2. Join the CIFS server to the Windows domain as explained in Join a CIFS server to a Windows domain on page 67.

   Note: CIFS server is automatically joined to Windows domain in an NT environment.

Add a WINS server

Action
To add a WINS server to the CIFS configuration for use by all CIFS server on a Data Mover, use this command syntax:
$ **server_cifs** *<mover_name>* **-add wins=**_<ip_addr>_[,**wins=**_<ip_addr>_,...]
where:
<mover_name> = name of the Data Mover.
<ip_addr> = IPv4 address of the WINS server.
Example:

Action
To add two WINS servers to server_2, type:
`$ server_cifs server_2 -add wins=172.31.255.255,wins=172.168.255.255`
Output
`server_2: done`

Note: The system processes a list of Windows Internet Naming Service (WINS) servers in the order in which you add them in the wins= option, with the first one being the preferred WINS server. For example, if the WINS server times out after 1500 milliseconds, the system uses the next WINS server in the list. Use the wins.TimeOutMS parameter to configure WINS timeout.

Start the CIFS service

After completing the preliminary CIFS configuration, you must start the CIFS service to activate the CIFS protocol for each Data Mover.

Action
To start the CIFS service, use this command syntax:
`$` **`server_setup`** *`<mover_name>`* **`-Protocol cifs -option start`** [=*`<n>`*]
where:
`<mover_name>` = name of the Data Mover or VDM.
[=*`<n>`*] = number of threads for CIFS users (if there is 1 GB of memory on the Data Mover, the default is 96 threads; however, if there is over 1 GB of memory, the default number of threads is 256).
Example:
To start the CIFS service on server_2, type:
`$ server_setup server_2 -Protocol cifs -option start`
Output
`server_2 : done`

Note: To change the thread number after starting the CIFS service, you must stop the service and restart it with the new thread number. Stop the CIFS service on page 103 provides procedural information.

Create a CIFS server for Windows Server environments

After starting the CIFS service, create the CIFS server on a Data Mover.

⚠ **CAUTION** Do not attempt to mix the NetBIOS and compname in the same Windows domain. Doing so can result in the Data Mover losing contact with the domain.

Action
To create the CIFS server for a Windows Server environment on the Data Mover, use this command syntax:
$ **server_cifs** *<mover_name>* **-add compname**=*<comp_name>*,**domain**=*<full_domain_name>* [,**netbios**=*<netbios_name>*][,**interface**=*<if_name>*][,**dns**=*<if_suffix>*]
where:
<mover_name> = name of the Data Mover or VDM.
<comp_name> = Windows Server-compatible CIFS server.
<full_domain_name> = full domain name for the Windows environment.
<netbios_name> = (Optional) a NetBIOS name used in place of the default NetBIOS name.
Type an optional NetBIOS name if the first 15 characters of the <comp_name> do not conform to the NetBIOS naming conventions or if you want something other than the default.
Note: You can only assign one compname to a CIFS server. You may assign multiple NetBIOS names to a CIFS server by creating aliases.
<if_name>= an interface to be used by the CIFS server being configured. If you add a CIFS server and do not specify any interfaces (with the interfaces= option), this server becomes the default CIFS server and uses all interfaces not assigned to other CIFS servers on the Data Mover. You can only have one default CIFS server per Data Mover.
Note: Link local interfaces cannot be added to a CIFS server as they are not supported on VNX.
<if_suffix>= different DNS suffix for the interface for DNS updates. By default, the DNS suffix is derived from the domain. This DNS option has no impact on the DNS settings of the Data Mover.
Example:
To create CIFS server dm32-ana0 on server_2, type:
$ server_cifs server_2 -add compname=dm32-cge0,domain=universe.com,netbios=eng23b,interface=cge0,dns=nasdocs.emc.com
Output
server_2 : done

Assign a NetBIOS or computer name alias on page 91 provides procedural information.

Join a CIFS server to a Windows domain

A CIFS server has to be joined to the Windows domain in a Windows Server environment.

Action
To join the CIFS server to the Windows domain, use this command syntax:
$ **server_cifs** *<mover_name>* **-Join compname**=*<comp_name>*,**domain**=*<full_domain_name>*, **admin**=*<domain_administrator_name>*,**ou**=*<organizational_unit>*
where:
<mover_name> = name of the Data Mover or VDM.
<comp_name> = name for the CIFS server account in the AD.
<full_domain_name> = DNS name for the Windows domain.
<domain_administrator_name> = login name of the user with administrative rights in the domain. The user is prompted to type a password for the admin account.
<organizational_unit> = container where the CIFS server's account is being created in the AD.
Example:
To join dm112-cge0 into the AD domain nasdocs.emc.com, using the administrator account, and to add this server to Engineering\Computers organizational unit, type:
$ server_cifs server_2 -Join compname=dm112-cge0,domain=nasdocs.emc.com,admin=administrator,ou="ou=Computers:ou=Engineering"

Output	Note
| ```
server_2 : Enter Password: *******
done
``` | The user account and user password are used to create the account in the AD, and are not stored after adding the machine account. |

Note: If a CIFS server is removed from the Windows domain by using an unjoin command, you need to run the join command again to rejoin the CIFS server to the Windows domain.

Join existing computer accounts

To join existing computer accounts:

- If the Windows computer account already exists, VNX checks the servicePrincipalName attribute to see if the computer is already joined to the computer account.

- If the attribute is not set, the Data Mover joins the new CIFS server to the existing account. If the servicePrincipalName attribute is already set, the Data Mover issues an error and logs a message saying that the account already exists.

Action

If you still want to join the CIFS server to this computer account, you can reuse the account by typing:
 	
`$ server_cifs server_2 -Join`
`compname=dm32-ana0,domain=nsgprod.xyzcompany.com,admin=administrator -option reuse`

When you join a CIFS server to a domain, VNX:

- Searches for an existing account or creates an account for the CIFS server in active directory (AD) and completes its configuration.

- Sets several attributes in the computer account, including the dnsHostName and servicePrincipalName attributes.

Verify the configuration

During the CIFS server join procedure, the system configures the following attributes of the computer account in the active directory (AD):

- dNSHostName
- servicePrincipalName

Note: The attributes of the precreated computer accounts, dNSHostName and servicePrincipalName, must be empty before a join. After you perform a successful join, these attributes are assigned values.

1. To verify the configuration using ldp.exe, log in to the domain controller by using the domain administrator credentials.

2. Verify that the support tools are installed.

3. Select **Start ➤ Run** .

4. Type ldp.exe and click **OK**.

5. Connect and BIND to the AD.

6. Perform a search for the specified container (CN) with the associated attributes, including dNSHostName and servicePrincipalName.

Mount a file system for CIFS access

When a file system is mounted, it is integrated into the local directory tree. File systems are mounted permanently by default. If you unmount a file system temporarily and then restart the file server, the file system is remounted automatically.

Action
To mount a file system, use this command syntax:
$ **server_mount** *<mover_name>* [**-option** *<options>*] *<fs_name> <mount_point>*
where:
<mover_name> = name of the physical Data Mover or VDM.
<options> = file system mount type can be desginated as either read/write (rw) or read-only (ro).
<fs_name> = name of the file system being mounted.
<mount_point> = name of the mount point beginning with a forward slash (/).
Example:
To mount the file system ufs1 as read/write, type:
$ server_mount server_2 -option rw ufs1 /ufs1
Output
server_2 : done

Note: When mounting a share, if the default options such as locking behavior and access control policy are not manually typed, the options are active but not displayed in the list of mounted file systems.

By default, VNX uses the native security policy to access file systems. The native access policy means that a Windows user is granted access to a directory by using an access control list (ACL) and a UNIX user is granted access to a directory by using UNIX rights. If you are using both UNIX and Windows clients to access the same file systems, you must set the access-checking policy for the file system. *Managing a Multiprotocol Environment on VNX* explains how to set up such an environment.

Create shares for CIFS users

Use the Computer Management MMC or the Windows NT Server Manager for Domains to create shares and set access control lists (ACLs) on shares. For domain CIFS servers with local users support, you can mix local and domain users and groups in ACLs.

Note: If you create a share with Windows management tools, you cannot use any of the special CIFS export options provided by server_export. *Using Windows Administrative Tools on VNX* provides procedural informarion.

Create a local share

A local share is accessible from a single CIFS server of the Data Mover. A local share created with the netbios= option or by Windows management tools (for example, MMC) can only be managed by the CLI if you specify the NetBIOS name as part of the command. The NetBIOS name is required to locate the entry because multiple CIFS entries can have the same <sharename> when belonging to different NetBIOS names. CIFS shares on page 21 provides conceptual information.

Action
To create a local share by exporting the pathname of the share, use this command syntax:
$ **server_export** *<mover_name>* **-Protocol cifs -name** *<sharename>* [**-option** *<op tions>*] *<pathname>*
where:
<mover_name> = name of the physical Data Mover or VDM.
<sharename> = name of the CIFS share.
<options> = export options for the share. Table 2 on page 21 describes the server_export command options.
<pathname> = pathname of the directory to export. This can be a mountpoint.
Example:
To create a local share named cifs_share on server_2, type:
$ server_export server_2 -Protocol cifs -name cifs_share -option netbios=dm32-cge0 /mntpt1
Output
server_2 : done

Note: If the <sharename> you are creating exists, the parameters are modified with the new information indicated. You cannot create a NetBIOS share with the same <sharename> as a global share.

Create a global share

A global share is accessible from all CIFS servers on the Data Mover.

Action
To create a global share by exporting the pathname of the share, use this command syntax:
$ **server_export** *<mover_name>* **-Protocol cifs -name** *<sharename>*[**-option** *<options>*] *<pathname>*
where:
<mover_name> = name of the physical Data Mover or VDM.
<sharename> = name of the CIFS share.
<options> = export options for the share.
<pathname> = name of the mount point.
Example:
To create a global read-only share named cifs_share on server_2, type:
$ server_export server_2 -Protocol cifs -name cifs_share -option ro /mntpt1
Output
server_2 : done

Create global shares with MMC or Server Manager

Normally, shares created through Windows administrative tools are local shares and are only accessible from the CIFS server used by the Windows client. However, the cifs srvmgr.globalShares parameter lets you change this behavior so that shares created through Server Manager or Microsoft Management Console (MMC) are global shares.

Action
To cause all shares created through the Server Manager or MMC to be global shares, use this command syntax:
$ **server_param** *<mover_name>* **-facility cifs**   **-modify srvmgr.globalShares -value** *<new_value>*
where:
<mover_name> = name of the Data Mover.
<new_value> = 0 or 1.
0 disables global shares.
1 enables global shares.
Example:
To cause all shares created through Server Manager or MMC to be global shares, type:
$ **server_param server_2 -facility cifs -modify srvmgr.globalShares -value 1**
Output
server_2 : done

Note: Parameter and facility names are case-sensitive.

Verify shares

The shares in the export table are always listed from the Control Station database. This is a static table and contains only permanent entries. Any temporary changes to the export table are not displayed.

Action
To verify a share, use this command syntax:
$ **server_export** *<mover_name>* **-list -name** *<sharename>*[**-option** *<options>*]
where:
<mover_name> = name of the physical Data Mover or VDM.
<sharename> = name of the CIFS share.
<options> = options for listing. Currently, there is only one option, [netbios = <netbios_name>]. When the share has an associated NetBIOS name, the NetBIOS name is required to locate the entry because multiple CIFS entries can have the same <sharename> when belonging to different NetBIOS names.
Example:
To list the shares on server_2, type:
$ server_export server_2 -list -name cifs_share

Output
| ```
server_2 :
share "cifs_share" "/mntpt1" "Test Share" umask=022
maxusers=4294967295
``` |

CIFS shares on page 21 and International character support on page 22 provide conceptual information.

Provide the network password when performing management tasks

When you perform a management action that tries to retrieve user and group names, such as setting access control lists (ACLs) on a share, you might be prompted for your administrative account name and password.

If you have executed a net use command with a domain name to specify the local username for the CIFS server, you must type the <domainname>\<username> combination used in the net use command.

For example, if you run the command:

```
net use \\192.168.56.24 /user:DomainX\UserY
```

You must type the account information when prompted for the network password as:

```
DomainX\UserY
```

Note: UserY must belong to the Administrators group of the CIFS server that includes the domain administrators and the local administrator of the CIFS server, by default.

Create a stand-alone CIFS server

User authentication methods on page 28 provides conceptual information.

Note: EMC recommends to use a CIFS stand-alone server with local user support instead of Data Movers with SHARE authentication.

Action
To create a stand-alone CIFS server, use this command syntax:
$ **server_cifs** *<mover_name>* **-add standalone**=*<netbios_name>*,**workgroup**=*<work group_name>*[,**interface**=*<if_name>*][,**local_users**]
where:
<mover_name> = name of the Data Mover or VDM.
<netbios_name> = NetBIOS name for the CIFS server.
<workgroup_name> = name of the Windows workgroup. This value is used for announcements and WINS registration.
<if_name> = IP interface for the CIFS server.
Example:
To create the stand-alone CIFS server dm32-ana0 on server_2 and provide local user support, type:
$ **server_cifs server_2 -add** **standalone=dm112-cge0,workgroup=NASDOCS,interface=cge0,local_users**

Output	Notes
| ```
Enter Password:*****
Enter Password Again:*****
server_2: done
# server_cifs server_2
CIFS Server(standalone)
SERVE_ALONE[EMC] RC=2
``` | ◆ If you are using (Internet Information Service) IIS 6.0, the username and password must be the same on IIS, the Data Mover, and the client.<br><br>◆ The password is assigned to the local Administrator account on the CIFS server and can only be ASCII characters. You must change the temporary password from a Windows system before you can administer the local users or groups on the CIFS server with local user support enabled. When you change the password, the password can contain Unicode characters.<br><br>◆ The local_users option causes the server_cifs command to prompt for a password to be assigned to the local Administrator password. This option must be typed when you initially create the stand-alone server. If you do not type the local_users option, the command fails.<br><br>◆ Do not type the local_users option if you are reconfiguring the server after initial creation. To reset the Administrator password, use the local_users option. However, the password cannot be reset if it was changed through Windows.<br><br>◆ If you create the stand-alone server on a Data Mover with a VDM loaded, you must specify an IP interface. |

After you finish

Change the password for the local Administrator account on page 86 and Enable the Guest account on a stand-alone server on page 88 provide procedural information.

Create a CIFS share on MAC OS by using the GUI

Before you begin

◆ Click **Finder** and select **Go ➤ Utilities ➤ Terminal**.

◆ Login with the admin password.

Procedure

Join MAC to the Windows domain

1. Install the Administration tools disk (applicable to MAC OS Client ONLY).

2. Open the Network configuration. Click the **Apple Icon ➤ System Preferences ➤ Network**.

3. Click **Advanced** button and select the **DNS** tab.

4. Set Windows DNS IP addresses and set **Search domain** to your Windows domain.

5. From **Application Utilities** Windows, start the **Directory Utility**.

6. Click **Finder** and select **Go** ➤ **Utilities** ➤ **Terminal**.

7. To make any changes, unlock the Directory Services by clicking on the lock icon.

   Note: These changes must be made by the local MAC client administrator.

8. In **Services**, double-click on **Active Directory** to join a domain.

9. Fill the Active Directory information and click **OK**.

10. Verify that the **Search policy** includes the Active Directory with **custom path** option in the search field. Move "Active Directory" in first not grey position.

Mount a CIFS share

1. Click **Go** ➤ **Connect to Server**.

2. In the **Server Address** field, enter <servername> and <sharename> and click **Connect**.

3. A login screen appears. Enter the username and password and click **Connect**.

4. You can now browse the CIFS share on the desktop.

Unmount a CIFS share

1. Browse the CIFS share on the desktop.

2. Click the Eject icon to unmount the share.

Create a CIFS share on MAC OS manually

Before you begin

* Click **Finder** and select **Go** ➤ **Utilities** ➤ **Terminal**.

* Login with the admin password.

Action
To create a CIFS share, use this command syntax:
sudo mount-t smbfs//**Domain**\;**password:user**@ *<servername>*/*<sharename>*/*<mount point>*;::
where:
<servername> = name of the server
<sharename> = name of the CIFS share
<mount_point> = path to mount point for the server

Action
Note:
Mount_smbfs : server connection failed : No route to host - servername not found (check /etc/hosts file).
Mount_smbfs : server rejected the connection : Authentification error - verify that domain user and password are correct.
Mount_smbfs : mount error : /mountpoint : file exists - a share with same name is already mounted.
To check that share is correctly mounted, use this command syntax:
mount
Note: Verify if the smbfs option is displayed.

Managing

The tasks to manage CIFS are:

Set maximum number of passwords to retain in Kerberos authentication

Action
To indicate the maximum number of passwords to retain for Kerberos authentication, use this command syntax:
$ **server_param** *<mover_name>* **-facility** **cifs -modify srvpwd.maxHistory -value** *<new_value>*
where:
<mover_name> = name of the Data Mover or VDM.
<new_value> = value you want to set for the specified parameter, where:
◆   1 retains only the current password.
◆   2–10 retains the current password and n-1 previous passwords.
◆   The default value is 2.
Example:
To use the current password and two previous passwords for authentication, type:
$ server_param server_2 -facility cifs -modify srvpwd.maxHistory -value 3
Output
server_2 : done

Note: Parameter and facility names are case-sensitive. If you experience password reset while troubleshooting problems with authentications, reset the CIFS server password by using the server_cifs command.

The Data Mover retains a history of the new and old passwords of each CIFS server. Kerberos authentication on page 25 provides conceptual information. Computers that are a part of the Windows Active Directory typically change the password at a regular time interval. Change the CIFS server password on page 97 provides procedural information.

Change the LDAP security level

By default, when a domain controller proposes a security layer for signing or encryption to the Data Mover, it responds with signing (integrity protection without encryption).

For the following command to work, the specified Data Mover must contain a CIFS server that is a member of the domain to which LDAP is attempting communication.

LDAP signing and encryption on page 26 provides conceptual information.

Action

To indicate which level of security to use for LDAP messages, use this command syntax:
 	
`$ server_param <mover_name> -facility`
`ldap -modify SecurityLayer -value <new_value>`
 	
where:
 	
<mover_name> = name of the Data Mover or VDM.
 	
<new_value> = 0, 1, 2, or 4.
 	
0=No security layer
 	
1=Same as LDAP server
 	
2=Integrity Protection
 	
4=Privacy Protection
 	
Example:
 	
To select privacy protection for LDAP messages, type:
 	
`$ server_param server_2 -facility ldap -modify SecurityLayer -value 4`

Output	Note
`server_2 : done`	◆ Parameter and facility names are case-sensitive. ◆ Restart the CIFS service after executing the above command.

Check the current CIFS configuration

Action

To display the CIFS configuration for a Data Mover, use this command syntax:
 	
`$ server_cifs <mover_name>`
 	
where:
 	
<mover_name> = name of the Data Mover.
 	
Example:
 	
To display the CIFS configuration for server_2, type:
 	
`$ server_cifs server_2`

Output

If CIFS service is started
 	
``
server_2 :
 256 Cifs threads started
 Security mode = NT
 Max protocol = NT1
 I18N mode = ASCII
 Home Directory Shares DISABLED
 Usermapper auto broadcast enabled
 Usermapper[0] = [127.0.0.1] state:active (auto discovered)
 Enabled interfaces: (All interfaces are enabled)
 Disabled interfaces: (No interface disabled)
``
 	
If CIFS service is not started
 	
``
$ server_cifs server_2
server_2 :
Cifs NOT started
Security mode = NT
Max protocol = NT1
I18N mode = ASCII
Home Directory Shares DISABLED
Usermapper auto broadcast enabled
Usermapper[0] = [127.0.0.1] state:active (auto discovered)
Enabled interfaces: (All interfaces are enabled)
Disabled interfaces: (No interface disabled)
``

Note: The server_cifs command currently does not display the link local interfaces configured on the Data Mover.

Check a CIFS configuration and its dependencies

Action
To test a CIFS configuration and all its dependencies or a specific dependency, use this command syntax: $ **server_checkup** *<mover_name>* **-test** *<component>* **-subtest** *<dependency>* where: *<mover_name>* = name of the Data Mover or VDM. *<component>* = component to test; in this case, CIFS. *<dependency>* = specific dependency of the CIFS configuration to test, such as the Kerberos subsystem or the local groups database. Example: To check all the CIFS dependencies of server_2, type: $ **server_checkup server_2 -test CIFS**

Note: The following is an excerpt of the actual output.

```
Output
```

```
server_2 :

----------------------------------Checks-------------------------------
-------
Component CIFS :
ACL       : Checking the number of ACL per file sys-
tem.....................*Pass
Connection: Checking the load of TCP connections of CIFS...................

Pass
Credential: Checking the validity of credentials...........................

Pass
DC        : Checking the connectivity and configuration
of the DCs.........*Pass
DFS       : Checking the DFS configuration files and DFS
registry.......... Pass
DNS       : Checking the DNS configuration and connectivity
to DNS servers. Pass
EventLog  : Checking the configuration of Windows Event
Logs............... Pass
FS_Type   : Checking if all file systems are all DIR3 type.................

Pass
GPO       : Checking the GPO configuration.................................

Pass
HomeDir   : Checking the configuration of home directory
share............ Pass
```

Manage CIFS servers with local users support

Information about the following management tasks is provided in this section:

Enable local user support on a domain CIFS server

Action
To create a Windows Server-compatible CIFS server with local user support or to add local user support to an existing CIFS server, use this command syntax: $ **server_cifs** *<mover_name>* **-add compname**=*<comp_name>* **,domain**=*<full_domain_name>*,**interface**=*<if_name>*, **wins**=*<ip_addr>*[:*<ip_addr>*][,**local_users**] where: *<mover_name>* = name of the Data Mover. *<comp_name>* = compname for the CIFS server. *<full_domain_name>* = DNS name for the Windows domain. *<if_name>* = name of the interface. *<ip_addr>* = IPv4 address of the WINS server. You are prompted to create a temporary local administrator password. Example: To create the domain CIFS server dm32-ana0 on server_2 with local users support, type: **$ server_cifs server_2 -add compname=dm112-cge0,domain=NASDOCS,interface=cge0,wins=192.168.24.18,local_users**

Output	Notes
| ```
Enter Password:*****
Enter Password Again:*****
server_2: done
# server_cifs server_2
CIFS Server CIFS_SERVER1[W2K] RC=4
(local users supported)
``` | ◆ The password is assigned to the local Administrator account on the CIFS server and must only be ASCII characters. You must change the temporary password from a Windows system before you can administer the local users or groups on the CIFS server with local user support enabled. When you change the password, the password can contain Unicode characters.<br><br>◆ The local_users option causes the server_cifs command to prompt for a password to be assigned to the local Administrator password. Do not type the local_users option if you are reconfiguring the server after initial creation. To reset the Administrator password, use the local_users option. However, the password cannot be reset if it was changed through Windows. |

Check a CIFS configuration and its dependencies on page 82 and Change the password for the local Administrator account on page 86 provide procedural information.

Note: -add netbios=<netbios_name>, domain=<domain_name> options enable local user support on a Windows NT CIFS server assigning the specified <netbios_name> and <domain_name>.

Local user and group accounts on page 31 provides conceptual information.

Enable local user support using Unisphere

Note: To enable local user support on an existing CIFS server, right-click the CIFS server, select Properties and select Local Users Enabled option.

1. Start the browser and type the IP address of the Control Station, for example, http://<IP_Address_of_the_Control_Station>.

2. Log in to Unisphere on VNX for file.

3. In the navigation pane on the left, select the system you want to set up.

4. Expand the menu and select **CIFS**. Select the **CIFS Server** tab.

5. Click **Create** to create a new CIFS server.

6. Select **Enable local users** option to enable local user support on the CIFS server. Local user support is enabled by default on a stand-alone CIFS server.

Change the password for the local Administrator account

Before you can administer local users and groups on the stand-alone CIFS server or local users enabled domain CIFS Server, you must change the password. For Windows Server clients, the password for a stand-alone server cannot be changed from a machine that is joined to a domain. Create a stand-alone CIFS server on page 75 provides procedural information.

1. To change the password of the local Administrator account, log in to a Windows client and press **Ctrl + Alt + Delete**.

2. Click **Change Password**. The **Change Password** dialog box appears.

3. Fill in the fields as follows:

   a. In the **username** field, type **Administrator**.

   b. In the **Log on to** field, type the name or IP address of the CIFS server.

   c. In the **Old Password** field, type the original Administrator account password you typed when you enabled local users support.

   d. In the **New Password** and **Confirm New Password** fields, type the new password for the local Administrator account.

Access and manage a CIFS server within the same domain

1. Open **Computer Management** on any computer within the same domain.

2. Go to **Action ➤ Connect to another computer**. The **Select Computer** dialog box appears.

3. Type the CIFS server name or the IP address.

   Note: As long as the CIFS server name or IP address is resolvable with DNS, there is no need to add the CIFS server name and IP address to the local C:\WINDOWS\system32\drivers\etc\hosts file.

Access and manage a stand-alone CIFS server within a workgroup environment

1. Type the stand-alone CIFS server name in the local Windows system Host file located at C:\WINDOWS\System32\Drivers\etc\hosts file. Add the stand-alone CIFS server name to the lmhosts file if browsing is required on a network or if the NetBIOS name resolution is required and WINS is not established on the subnet.

2. To provide the security context for the Windows logon session, use this command syntax:

```
net use \\ <standalone_server> /user: <Local_Username>
```

where:

`<standalone_server>` = IPv4 or IPv6 address; for MMC snap-in, stand-alone NetBIOS name.

`<Local_Username>` = username of an account with administrative rights on the stand-alone server.

Example:

To connect to a stand-alone server 192.168.56.24, type:

```
net use \\192.168.56.24 /user:administrator
```

Output:

```
Type the password for <IP_address>:

The command completed successfully.
```

3. Open **Computer Management**. Go to **Action ➤ Connect to another computer**. The **Select Computer** dialog box appears.

4. Type the CIFS server name. You will not be prompted for the username and password. The console will open and the local groups database will be manageable on the server. The security credentials are valid for the existing logon session only. Repeat step 2 to connect to a system from which access is desired, and each time you log in to the Windows system.

Note: If the password typed or the procedure to access the local groups database of the CIFS server from the Computer Management is incorrect, the error message `Unable to access the computer xxxxx. The error was: Access is denied` is displayed.

Enable the Guest account on a stand-alone server

To use usrmgr.exe to connect to a stand-alone server, you must first create a connection to the IPC$ share on the CIFS server as described in Access and manage a stand-alone CIFS server within a workgroup environment on page 86.

Guest accounts on page 34 provides conceptual information.

1. Open **User Manager**.

2. Connect to the stand-alone server:

   a. Select **User ➤ Select Domain**.

   b. In the Domain field, type:

      `\\<standalone_server>`

      Where:

      `<standalone_server>` = IP address; for MMC snap-in, stand-alone NetBIOS name.

   c. Click **OK.**

   d. When prompted, log in with the Administrator account.

3. Double-click the **Guest** account. The **User Properties** dialog box appears.

4. Configure the Guest account and click **OK**. To add security to the Guest account, you can also add a password to the account. Any unknown user that logs in with the Guest account password is logged as Guest.

5. In User Manager, select **Policies ➤ User Rights**. The **User Rights Policy** dialog box appears.

6. Grant the **Access this computer from network** permission to the new Guest account.

Delete a stand-alone server

Action
To delete a stand-alone CIFS server, use this command syntax:
`$ server_cifs <mover_name> -delete standalone=<netbios_name> [-remove_localgroup][,alias=<alias_name>...][,interface=<if_name>]`
where:
`<mover_name>` = name of the Data Mover or VDM.
`<netbios_name>` = NetBIOS name for the CIFS server.
Example:
To delete the stand-alone server, dm32-cge0, on server_2, type:

Action
$ server_cifs server_2 -delete standalone=dm32-cge0
Output
server_2 : done

Note: If you delete a CIFS server with local user support and then create a new one with the same name and local user support , the new server retains the original local administrative password. Hence you cannot set a new password for the new CIFS server. Set maximum number of passwords to retain in Kerberos authentication on page 80 provides procedural information.

Hint: If you add the -remove_localgroup option, the Data Mover permanently deletes the local group information of the CIFS server from the permanent storage of the Data Mover. If you add the alias and interface options, only the alias and the interface are deleted, the CIFS server exists. You can combine the alias and interface options in the same delete command.

Rename a NetBIOS name

Before renaming a NetBIOS name, add the new name to the domain using the Windows NT Server Manager or the Windows Server Users and Computers Microsoft Management Console (MMC) snap-in.

When you change a NetBIOS name, the system does the following:

- Temporarily suspends NetBIOS availability and disconnects all clients connected to it.

- Updates the local groups related to the new NetBIOS name.

- Updates all the shares corresponding to the new NetBIOS name.

- Maintains the account password between the server and the domain controller.

- Unregisters the original NetBIOS name, and then registers the new name in all the WINS servers.

- Retains all aliases associated with the original NetBIOS name.

- Resumes renamed NetBIOS availability.

- The rename command changes the NetBIOS name of the server, but not the compname of that server.

Action
To rename a NetBIOS name, use this command syntax:
$ **server_cifs** *<mover_name>* **-rename -netbios** *<old_name> <new_name>*
where:
<mover_name> = name of the Data Mover.

Action
<old_name> = name of the current NetBIOS. *<new_name>* = name of the new NetBIOS. Example: To rename the NetBIOS name of dm102-cge0 to dm112-cge0 on server_2, type: `$ server_cifs server_2 -rename -netbios dm102-cge0 dm112-cge0`
Output
`server_2 : done`

⚠ **CAUTION**   The server_cifs -Join and -Unjoin procedures generate a new computer account for the compname, as a result the original account of the computer name is lost.

Rename a compname

This procedure renames a Windows Server Data Mover while preserving local groups, shares, and file system permissions for the new name. In this example W2ktemp is renamed W2kProd.

1. To unjoin the original compname from the domain, type:

   `$ server_cifs server_2 -Unjoin compname=W2kTemp,domain=abc.com,admin=Administrator`

2. To delete the compname from the CIFS configuration of the Data Mover, type:

   `$ server_cifs server_2 -delete compname=W2kTemp`

3. To add the compname back to the CIFS configuration of the Data Mover as a NetBIOS name, type:

   `$ server_cifs server_2 -add netbios=W2kTemp,domain=abc,interface=fsn01`

4. To rename the NetBIOS server to the new name, type:

   `$ server_cifs server_2 -rename netbios W2kTemp W2kProd`

5. To delete the renamed NetBIOS name from step 4. from the CIFS configuration of the Data Mover, type:

   `$ server_cifs server_2 -delete netbios=W2kProd`

6. To add the new compname to the CIFS configuration and active directory (AD) domain, type:

   `$ server_cifs server_2 -add compname=W2kProd,domain=abc.com,interface=fsn01`

7. To join the new compname to the CIFS configuration and active directory (AD) domain, type:

   `$ server_cifs server_2 -Join compname=W2kProd,domain=abc.com,admin=Administrator`

Assign a NetBIOS or computer name alias

NetBIOS compared with DNS alias on page 32 provides conceptual information. Perform these tasks to manage aliases:

- Add a NetBIOS alias to a CIFS server on page 91
- Add a NetBIOS alias to the NetBIOS name on page 92
- Delete a CIFS server alias on page 92
- Delete a NetBIOS alias on page 93
- View aliases on page 93

Add a NetBIOS alias to a CIFS server

Action
To add an alias to a CIFS server, use this command syntax:
$ **server_cifs** *<mover_name>* **-add compname**=*<comp_name>*,**domain**=*<full_domain_name>*, **alias**= *<alias_name>* [, **alias**=*<alias_name2>*...]
where:
<mover_name> = name of the Data Mover.
<comp_name> = name of the CIFS server in the named domain.
<full_domain_name> = full domain name for the Windows environment.
<alias_name> = alias for the computer name.
Example:
To add three aliases for computer name winserver1, type:
$ server_cifs server_2 -add compname=winserver1,domain=NASDOCS.emc.com,alias=winserver1-a1,alias=winserver1-a2,alias=winserver1-a3
Output
server_2 : done

Important: The command server_cifs -add alias= creates a NetBIOS alias.

Add a NetBIOS alias to the NetBIOS name

Action
To add a NetBIOS alias to the NetBIOS name, use this command syntax:
$ **server_cifs** *<mover_name>* **-add netbios**=*<netbios_name>*,**domain**=*<domain_name>*, **alias**=*<alias_name>* [, **alias**=*<alias_name2>*...]
where:
<mover_name> = name of the Data Mover.
<netbios_name> = NetBIOS name for the CIFS server.
<domain_name> = domain name for the Windows environment.
<alias_name> = alias for the NetBIOS name.
Example:
To declare three aliases for NetBIOS dm102-cge0, type:
$ server_cifs server_2 -add netbios=dm102-cge0,domain=NASDOCS.emc.com,alias=dm102-cge0-a1,dm102-cge0-a2,dm102-cge0-a3
Output
`server_2: done`

Delete a CIFS server alias

Action
To delete a compname alias, use this command syntax:
$ **server_cifs** *<mover_name>* **-delete compname**=*<comp_name>*, **alias**=*<alias_name>*[,**alias**=*<alias_name2>*,...]
where:
<mover_name> = name of the Data Mover.
<comp_name> = name of the CIFS server.
<alias_name> = alias for the computer name.
Example:
To delete the dm102-cge0-a1 alias assigned to winserver1, type:
$ server_cifs server_2 -delete compname=winserver1,alias=dm102-cge0-a1
Output
`server_2: done`

Hint: If you specify the alias option, only the alias is deleted, the CIFS server exists. If you do not specify the alias option, the CIFS server in a Windows Server environment is removed from the CIFS configuration of the Data Mover.

Delete a NetBIOS alias

Action
To delete one or more NetBIOS aliases from a CIFS server, use this command syntax:
$ **server_cifs** *<mover_name>* **-delete netbios**=*<netbios_name>*, **alias**=*<alias_name>* [,**alias**=*<alias_name2>*,...]
where:
<mover_name> = name of the Data Mover.
<netbios_name> = NetBIOS name for the CIFS server.
<alias_name> = alias for the NetBIOS name.
Example:
To delete the dm102-cge0-a2 alias assigned to dm102-cge0, type:
$ server_cifs server_2 -delete netbios=dm102-cge0,alias=dm102-cge0-a2
Output
server_2: done

Hint: If you specify the alias option, only the alias is deleted, the CIFS server exists. If you do not specify the alias option, the CIFS server in a Windows Server environment is removed from the CIFS configuration of the Data Mover.

View aliases

Action
To list aliases on a server, use this command syntax:
$ **server_cifs** *<mover_name>*
where:
<mover_name> = name of the Data Mover.
Example:
To view the aliases for server_2, type:
$ server_cifs server_2

Output
| ```
CIFS Server (Default) dm102 -cge0 [C1T1]
Alias(es): dm102-cge0-a1,dm102-cge0-a2,dm102-cge0-a3
Full computer name=dm2-cge0.c1t1.pt1.c3lab.nasdocs.emc.com
realm=C1T1.PT1.C3LAB.NASDOCS.EMC.COM
Comment='EMC-SNAS:T5.2.7.2'
if=cge0 l=172.24.100.55 b=172.24.100.255 mac=0:6:2b:4:0:7f
FQDN=dm102-cge0.c1t1.pt1.c3lab.nasdocs.emc.com (Updated
to DNS)
``` |

Associate comments with CIFS servers

You can associate a comment with a CIFS server. Comments let you add descriptive information to a CIFS server:

◆ Restricted characters: Do not use double quotation ("), semi-colon (;), accent (`), and comma (,) characters within the body of a comment. Attempting to use these special characters results in an error message. In addition, you can only use an exclamation point (!) if it is preceded by a single quotation mark (').

◆ Default comments: If you do not explicitly add a comment, the system adds a default comment of the form EMC-SNAS:T<x.x.x.x>, where <x.x.x.x> is the version of the NAS software.

You can add comments when you initially create the CIFS server or after the CIFS server is created.

Perform these tasks to associate comments:

◆ Add comments to a CIFS server in a Windows Server environment on page 94

◆ Clear comments on page 95

◆ View comments from the CLI on page 95

◆ Comment limitations for Windows XP clients on page 96

Add comments to a CIFS server in a Windows Server environment

Action
To add comments in a Windows environment, use this command syntax:
$ **server_cifs** *<mover_name>* **-add compname**=*<compname_name>*, **domain**=*full_domain_name* **-comment** "*comment*"
where:
<mover_name> = name of the Data Mover.
<comp_name> = Windows Server-compatible CIFS server.

Action
<full_domain_name> = full domain name for the Windows environment.

<comment> = your comment.

Example:

To add the comment "EMC_VNX" to server_2 in a Windows Server environment, type:

```
$ server_cifs server_2 -add compname=dm32-ana0,domain=NASDOCS.emc.com -comment
"EMC_VNX"
```

International character support on page 22 provides conceptual information.

Note: You cannot add or change comments through the Server Management or the Computer Management MMC. You can repeat the server_cifs _add command to change a comment. You might notice a delay in the comment change when browsing the domain computers. This delay occurs when the Data Mover broadcasts its name and comment approximately every 12 minutes (except on startup, when it broadcasts five times in the first minute).

Clear comments

To clear a comment, run the server_cifs -add command with a one-space comment as in the following example.

Action
To clear a comment for server_2, type:

```
$ server_cifs server_2 -add netbios=dm32-ana0,domain=capitals -comment " "
```

View comments from the CLI

When you view a CIFS server configuration from the CLI, the comment appears with other information about the CIFS server.

Action
To view the configuration information, use this command syntax:

```
$ server_cifs <mover_name>
```

where:

<mover_name> = name of the Data Mover.

Example:

To view the configuration information for server_2, type:

```
$ server_cifs server_2
```

Output

```
server_2 :
32 Cifs threads started
Security mode = NT
.
(material deleted)
.
DOMAIN CAPITALS
SID=S-1-5-15-c6ab149b-92d87510-a3e900fb-ffffffff
>DC=BOSTON(172.16.20.10) ref=2 time=0 ms
DC=NEWYORK(172.16.20.50) ref=1 time=0 ms
CIFS Server (Default) DM32-ANA0[CAPITALS] (Hidden)
Alias(es): CFS32
Comment='EMCVNX'
if=ana0 l=172.16.21.202 b=172.16.21.255 mac=0:0:d1:1d:b7:25
if=ana1 l=172.16.21.207 b=172.16.21.255 mac=0:0:d1:1d:b7:26
```

Comment limitations for Windows XP clients

When you change a comment, the change is reflected only in certain parts of the Windows XP interface. As the computer name in a domain window, the change is immediately reflected to the Windows XP client. However, in Windows XP Explorer, the names of mapped network drives do not reflect the change.

When you first map a network drive on a Windows XP client, the client stores the comment in the local Registry and displays the comment as the name of the mapped drive. The client continues to use the stored comment as the mapped drive name until you manually change the Registry. If you manually change the name of the mapped network drive from Explorer or My Computer, the changed name is stored in another Registry entry and the client uses this name until you change it again from Explorer or in the Registry.

EMC recommends that you set the comment as part of the initial CIFS server setup.

Change the CIFS server password

Computers that are members of a Windows Active Directory (AD) typically change the password for their domain account on a regular basis (for example, every 12 hours or 7 days).

Action
To reset the CIFS password and encryption keys, use this command syntax:
$ **server_cifs** *<mover_name>* **-Join compname=**<comp_name>, **domain=**<full_domain_name>,**admin=**<admin_name> **-option resetserverpasswd**
where:
<mover_name> = name of the Data Mover.
<comp_name> = name of the CIFS server.
<full_domain_name> = full domain name for the Windows environment.
<admin_name> = login name of the user with administrative rights in the domain. The user is prompted to type a password for the admin account.
Example:
To reset the CIFS password and encryption keys for server_2, type:
$ server_cifs server_2 -Join **compname=winserver1,domain=nasdocs.emc.com,admin=compadmin -option resetserverpasswd**

Output
| ```
server_2: Enter Password: ******
done
``` |

Configure automatic computer password changes on page 132 explains how to set the time interval at which the Data Mover changes passwords with the domain controller.

Note: When a Windows NT-mode CIFS server is created, a default password is assigned. The Data Mover tries to change the password when it communicates with the domain controller. If the password change fails, the CIFS server continues to use the default password. Because the default password is the name of the server you should reset the password. Restart the CIFS service to force the Data Mover to update the password on its domain controller. Start the CIFS service on page 65 provides procedural information.

Display the SMB2 dialect release

Action
To display the current SMB2 dialect release, use this command syntax: $ **server_cifs** *<movername>* where: *<movername>* = name of the Data Mover. Example: To display the current SMB 2 dialect release on server_2, type: **$ server_cifs server_2**

Output
| ```
server_2 :
256 Cifs threads started
Security mode = NT
Max protocol = SMB3.0      <<<< dialect here
I18N mode = UNICODE
Home Directory Shares DISABLED
Usermapper auto broadcast enabled

Usermapper[0] = [127.0.0.1] state:active (auto discovered)

Enabled interfaces: (All interfaces are enabled)

Disabled interfaces: (No interface disabled)
...
``` |

Verify the effective SMB dialect for the connected clients

Perform this task to verify the protocol that is in use on the various clients that are connected to the CIFS server:

Action
To display the effective SMB dialect, use this command syntax: # **server_cifs** *<movername>* **-option audit** where: *<movername>* = name of the Data Mover. Example: To display the effective SMB dialect on server_2, type: # server_cifs server_2 -option audit

Important: The audit output might be extensive as all the client connections are listed if no option is specified with the audit command. It is recommended to specify the filtering options for server_cifs –o audit command. The EMC VNX Command Line Interface Reference for File provides more information related to this command.

Output
| ```
SMB2 session Id=0x50a6933200000003, 1 channel(s)
Uid=0x3 NTcred(0x0338a72408 RC=6 KERBEROS Capa=0x200002) 'W2012\tmatta'
AUDIT Ctx=0x0009a50c08, ref=2,  Client(10.241.168.71) Port=59131/445
SMB30[W2012] on if=cge-2-0
CurrentDC 0x00099fa008=VM200W2012
Proto=SMB3.00, MaxReadWriteSz=0x100000, MaxTransactSz=0x100000, popupMsg=1
SrvCapa=0x7f, CltCapa=0x7f  ---abridged---
``` |

Display the number and names of open files

Action
To display the number and names of open files, use this command syntax:
$ **server_cifs** *<mover_name>* **-option audit** [,**user**=*<user_name>*] [,**client**=*<client_name>*][,**full**]
where:
<mover_name> = name of the Data Mover.
<user_name> = the user name can be simply <user_name> or Domain\<user_name> or <user_name@emc.com>.
<client_name> = the machine name, which can be a string or an IP address.
Example:
To display the number and names of open files on server_2, type:
$ server_cifs server_2 -option audit,full

Output
| ```
AUDIT Ctx=0xdffcc404, ref=2,  Client(fm-main07B60004)
Port=36654/139
NS40_1[BRCSLAB] on if=cge0_new
CurrentDC 0xceeab604=W2K3PHYAD
Proto=NT1, Arch=UNKNOWN, RemBufsz=0xfefb, LocBufsz=0xffff,
popupMsg=1
0 FNN in FNNlist NbUsr=1 NbCnx=0
Uid=0x3f NTcred(0xcf156a04 RC=1 NTLM Capa=0x401) 'BRCSLAB\gustavo'
CHECKER
AUDIT Ctx=0xde05cc04, ref=2, XP Client(BRCSBARREGL1C) Port=1329/445
NS40_1[BRCSLAB] on if=cge0_new
CurrentDC 0xceeab604=W2K3PHYAD
Proto=NT1, Arch=Win2K, RemBufsz=0xffff, LocBufsz=0xffff,
popupMsg=1
0 FNN in FNNlist NbUsr=1 NbCnx=2
Uid=0x3f NTcred(0xceeabc04 RC=3 NTLMSSP Capa=0x11001) 'BRCSLAB\gustavo'
CHECKER
Cnxp(0xceeaae04), Name=IPC$, cUid=0x3f Tid=0x3f, Ref=1,
Aborted=0
readOnly=0, umask=22, opened files/dirs=0
Cnxp(0xde4e3204), Name=gustavo, cUid=0x3f Tid=0x41, Ref=1,
Aborted=0
readOnly=0, umask=22, opened files/dirs=2
Fid=64, FNN=0x1b0648f0(FREE,0x0,0), FOF=0x0  DIR=\
Notify commands received:
Event=0x17, wt=0, curSize=0x0, maxSize=0x20, buffer=0x0
Tid=0x41, Pid=0xb84, Mid=0xec0, Uid=0x3f, size=0x20
Fid=73, FNN=0x1b019ed0(FREE,0x0,0), FOF=0xdf2ae504 (CHECK)
FILE=\New Wordpad Document.doc
``` |

Using Windows Administrative Tools on VNX provides more information on viewing open files by using Microsoft Management Console (MMC).

Hint: In the case of a Microsoft Windows 7 SMB2 client, the suboption **full** displays the current caching lease information on the Data Mover.

Delegate join authority

When you delegate join authority, the CIFS server can be joined to its domain by any user to whom you give authority. The user does not need specific Windows permissions, but must be in the same AD forest as the CIFS server.

To delegate join authority, set the following parameters:

* cifs djUsekpassword

* cifs djAddAdminToLg

* cifs djEnforceDhn

Note: Use djEnforceDhn as a temporary measure for access rights because the Data Mover authenticates Windows clients by using NTLMSSP mode instead of Kerberos.

The *Parameters Guide for VNX for File* provides additional information. Delegating joins on page 40 provides conceptual information.

Manage file systems

Perform these tasks to manage file systems:

- Ensure synchronous writes on page 101
- Turn oplocks off on page 101
- Configure file change notification on page 102

Ensure synchronous writes

The cifssyncwrite option ensures that any write to the file server is done synchronously. It is important that you ensure synchronous writes if VNX is used to store certain database files. EMC recommends that you use this mount option to avoid chances of data loss or file corruption across various failure scenarios, for example, loss of power.

Action
To mount a file system to ensure synchronous writes, use this command syntax:
$ **server_mount** *<mover_name>* **-option cifssyncwrite** *<fs_name> <mount_point>*
where:
<mover_name> = name of the Data Mover or VDM.
<fs_name> = name of the file system being mounted.
<mount_point> = name of the mount point.
Example:
To mount the file system ufs1 with ensured synchronous writes, type:
$ server_mount server_2 -option cifssyncwrite ufs1 /ufs1
Output
server_2 : done

Turn oplocks off

Opportunistic file locking on page 48 provides conceptual information.

> ⚠️ **CAUTION** — EMC recommends that you leave oplock on unless you are using a database application that suggests oplock be turned off, or if you are handling critical data and cannot afford any data loss. When oplock is enabled, data loss can occur in a Microsoft network if the Windows Server crashes or network problems occur.

Action
To turn oplocks off for a specific file system, use this command syntax:
$ **server_mount** *<mover_name>* **-option nooplock** *<fs_name> <mount_point>*
where:
<mover_name> = name of the Data Mover or VDM.
<fs_name> = name of the file system being mounted.
<mount_point> = name of the mount point.
Example:
To mount the file system ufs1 with oplocks turned off, type:
$ server_mount server_2 -option nooplock ufs1 /ufs1
Output
server_2 : done

Note: You might notice performance degradation if oplocks are disabled.

Configure file change notification

A directory file must be opened before this command is used. File change notification on page 49 provides conceptual information.

Note: File change notification is enabled by default. Consider disabling the option if you experience performance issues.

Action
To disable the notify feature for a file system, use this command syntax:
$ **server_mount** *<mover_name>* **-option nonotify** *<fs_name> <mount_point>*
where:
<mover_name> = name of the Data Mover or VDM.
<fs_name> = name of the file system being mounted.
<mount_point> = name of the mount point.
Example:
To disable the notify feature for file system ufs1 on server_2, type:

Action
`$ server_mount server_2 -option nonotify ufs1 /ufs1`
Output
`server_2 : done`

Table 13 on page 103 provides information about file change notification options.

Table 13. File change notification options

Option	Description	Range	Example
triggerlevel=<value>	Specifies how many directory levels beneath the monitored directory are monitored for changes.	<value> must be in hexadecimal format. Default value: 512 levels (0x00000200)	The following example shows a configuration for up to 15 directory levels: `$ server_mount server_2 -option "triggerlevel= 0x0000000f" ufs1 /ufs1`
notifyonwrite	Provides a notification of write access to a file system. This option is useful when an application needs to be notified of file writes before closing the file.	Default value: disabled	The following example enables notifyonwrite: `$ server_mount server_2 -option notifyonwrite ufs1 /ufs1`
notifyonaccess	Provides a notification of the access time of a modification.	Default value: disabled	The following example enables notifyonaccess and notifyonwrite: `$ server_mount server_2 -option notifyonaccess, notifyonwrite ufs1 /ufs1`

Note: For performance reasons, the notifyonwrite and notifyonaccess options are disabled by default.

Stop the CIFS service

Action
To stop CIFS service for a Data Mover, use this command syntax:
`$ server_setup <mover_name> -Protocol cifs -option stop`
where:

Action
<mover_name> = name of the Data Mover.
Example:
To stop the CIFS service on server_2, type:
`$ server_setup server_2 -Protocol cifs -option stop`
Output
`server_2: done`

⚠ **CAUTION** Stopping the CIFS service on a Data Mover prohibits users from accessing all CIFS servers on that Data Mover.

Delete a CIFS server

Before you begin

Use Microsoft Management Console (MMC) or Server Manager to close all active sessions before deleting a CIFS server.

⚠ **CAUTION** Data loss can occur if you stop or delete a CIFS server (Windows Server or Windows NT) when writes are in process. Before you perform this procedure, notify all users in advance that the CIFS server will no longer be available.

Delete a CIFS server in a Windows Server environment

1. To unjoin the computer from the domain, use this command syntax:

   `$ server_cifs <mover_name> -Unjoin compname=<comp_name>,domain=<full_do main_name>`

   Where:

   <mover_name> = name of the Data Mover.

   <comp_name> = computer name of the CIFS server.

   <full_domain_name> = full domain name for the Windows environment.

   Example:

   To unjoin the computer from the domain universe.com, type:

   `$ server_cifs server_2 -Unjoin compname=dm32-cge0,domain=universe.com`

2. To remove the CIFS server, use this command syntax:

   `$ server_cifs <mover_name> -delete compname=<comp_name> [-remove_localgroup][,alias=<alias_name>...][,interface=<if_name>]`

   Where:

<mover_name> = name of the Data Mover.

<comp_name> = computer name of the CIFS server.

Example:

To remove a CIFS server, type:

```
$  server_cifs server_2 -delete compname=dm32-cge0
```

Hint: If you add the -remove_localgroup option, the Data Mover permanently deletes the local group information of the CIFS server from the permanent storage of the Data Mover. If you add the alias and interface options, only the alias and the interface are deleted, the CIFS server exists. You can combine the alias and interface options in the same delete command.

Note: The -delete command does not delete the NetBIOS entry from the primary domain controller (PDC).

Delete CIFS shares

When you delete a share, users no longer have access to that share. All unexports on CIFS shares are permanent—when a CIFS share is unexported, the entry is deleted from the export table. To provide user access to the file system, you must reexport the file system.

Before you delete shares, ensure that all users have disconnected from the share before you unexport the share. If you export a directory or file system from a Data Mover before unmounting it, you will be unable to connect to the share the next time you try to access the file system.

Note: By default, shares created by Windows management tools are local shares. Create shares for CIFS users on page 71 provides procedural information. To delete a local share through the CLI, you must specify the NetBIOS name when you run the server_export command.

Delete a specific share

Action
To delete a CIFS share, use this command syntax:
$ **server_export** *<mover_name>* **-unexport -name** *<sharename>* [**-option** *<options>*]
where:
<mover_name> = name of the physical Data Mover or VDM.
<sharename> = name of the CIFS share.

Action
<options> = options for listing. Currently, there is only one option. netbios=<netbios_name>. When the share has an associated NetBIOS name, the NetBIOS name is required to locate the entry because multiple CIFS entries can have the same <sharename> when belonging to different NetBIOS names.
Example:
To delete share cifs_share on server_2, type:
`$ server_export server_2 -unexport -name cifs_share`
Output
`server_2: done`

Delete all shares

> **⚠ CAUTION** Use this option carefully. After deleting all shares, you must rebuild the export table by reexporting each path on each Data Mover to restore user connectivity to all mounted file systems.

Action
To delete all CIFS shares, use this command syntax:
$ **server_export** *<mover_name>* **-Protocol cifs -unexport -all**
where:
<mover_name> = name of the physical Data Mover or VDM.
Example:
To delete all shares on server_2, type:
$ server_export server_2 -Protocol cifs -unexport -all
Output
server_2: done

Note: Deleting the shares does not delete the underlying file system.

Manage domain migration

The server_cifs -Migrate command updates all SIDs from a source domain to the SIDs of a target domain by matching the user and group account names in the source domain to the user and group account names in the target domain. The interface specified in this option queries the local server and then its corresponding source and target domain controllers to search each object's SID.

Review the following before using the server_cifs -Migrate command option:

* The migrate option does not require running any type of domain migration tool beforehand.

* For the migrate option:

  · The source and target domain controllers must exist.

  · As long as a trusted relationship is established between the source and target domains, you can specify the same interface or NetBIOS name in the server_cifs command.

  · To use different interfaces or NetBIOS names, you must configure two separate CIFS servers on the Data Mover for the source and target domains.

Action

To migrate all SIDs in the ACL database for file system, ufs1, from eng.emc.com:nb=dm112-cge1:if=cge1 to nas-docs.emc.com:nb=dm112-cge0:if=cge0, type:
 	
`$ server_cifs server_2 -Migrate ufs1 -acl eng.emc.com:nb=dm112-cge1:if=cge1`
`nasdocs.emc.com:nb=dm112-cge0:if=cge0`

Output
`server_2: done`

The server_cifs -Replace command replaces the history SIDs from the old domain with the new SIDS in the new domain. The interface that you specify in this option queries the local server and then its corresponding target domain controller to search each object's SID and history SID.

Review the following before using the server_cifs -Replace command option:

- The replace option requires that you first perform account migration by using a domain migration tool.

- The replace option provides one quota per user or group.

Action
To replace the SIDs for ufs1, type: `$ server_cifs server_2 -Replace ufs1 -acl:nb=dm112-cge0:if=cge0`
Output
`server_2: done`

Domain migration on page 19 provides conceptual information.

Note: After running a local group update, stop and start the CIFS service on the Data Mover to ensure that all changes are made to the target domain. Stop the CIFS service on page 103 and Start the CIFS service on page 65 provide procedural information.

Change the user authentication method

By default, VNX uses the NT user authentication method. Use NT user authentication with both domain CIFS servers and a stand-alone CIFS server with local user support. For security reasons, it is strongly recommended that you do not use UNIX or SHARE user authentication. User authentication methods on page 28 provides more information.

Action
To change the user authentication method for the Data Mover, use this command syntax:
$ **server_cifs** *<mover_name>* **-add security=***<security_mode>*
where:
<mover_name> = name of the Data Mover or VDM.
<security_mode> = NT, UNIX, or SHARE.
Example:
To set the user authentication method to UNIX for server_2, type:
$ server_cifs server_2 -add security=UNIX
Output
server_2 : done

Check the user authentication method

Action
To check the user authentication method set on the Data Mover, use this command syntax:
$ **server_cifs** *<mover_name>*
where:
<mover_name> = name of the Data Mover or VDM.
Example:
To check the user authentication method for server_2, type:
$ server_cifs server_2

Output
| ```
server_2 :
256 Cifs threads started
Security mode = NT
Max protocol = NT1
I18N mode = UNICODE
Home Directory Shares DISABLED
usermapper auto broadcast enabled
usermapper[0] = [128.221.253.2] state:active (auto discovered)
usermapper[1] = [128.221.252.2] state:active (auto discovered)
Default WINS servers = 172.24.101.108
Enabled interfaces: (All interfaces are enabled)
Disabled interfaces: (No interface disabled)
Unused Interface(s):
if=cge1 l=172.24.100.61 b=172.24.100.255 mac=0:60:16:4:43:ec
if=cge2 l=172.24.100.62 b=172.24.100.255 mac=0:60:16:4:43:e9
if=cge3 l=172.24.100.71 b=172.24.100.255 mac=0:60:16:4:43:e8
DOMAIN W2KPAGCHILD1NBN FQDN=child1.win2kpag.ad.root SITE=NET-100
RC=5
SID=S-1-5-15-f7d03a54-f0a67e26-297741d6-ffffffff
>DC=LNSGC046(172.24.101.46) ref=2 time=9 ms (Closest
Site)
>DC=LNSGC108(172.24.101.108) ref=3 time=1 ms (Closest
Site)
CIFS Server CS80-DM4-CGE0[W2KPAGCHILD1NBN] RC=40
Alias(es): CS80DM4-ALIAS1,CS80DM4-ALIAS2,CS80DM4-ALIAS3,CS80DM4-
ALIAS4,CS80DM4-
ALIAS5,CS80DM4-ALIAS6,CS80DM4-ALIAS7,CS80DM4-ALIAS8,CS80DM4-ALIAS9,CS80DM4-
ALIAS10
Full computer name=cs80-dm4-cge0.child1.win2kpag.ad.root
realm=CHILD1.WIN2KPAG.AD.ROOT
Comment='EMC-SNAS:T5.5.15.0'
if=cge0 l=172.24.100.47 b=172.24.100.255 mac=0:60:16:4:43:ed
wins=172.24.101.108
FQDN=cs80-dm4-cge0.pag.emc.com (Updated to DNS)
Password change interval: 30 minutes
Last password change: Thu Dec  20 14:09:07 2005 GMT
Password versions: 1088, 1087
``` |

Note: If there are CIFS servers on the Data Mover, you cannot reset the user authentication method because this method is in use by the existing CIFS servers.

Leveraging Advanced Functionality

Advanced CIFS functionalities are:

Enable and manage home directories

The home directory feature is disabled by default. Create the CIFS server and start the CIFS service before you enable the home directory as discussed in the Unisphere online help. Home directories on page 41 provides conceptual information.

Perform these tasks to manage the home directory feature:

1. Create the database on page 112
2. Create the home directory file on page 112
3. Add home directories to user profiles on page 113
4. Disable home directories on the Data Mover on page 115

Create the database

1. To use the home directory feature, create a database file named homedir. The database file maps each domain or username combination to the home directory location of the user.

2. Use the home directory snap-in to create a new database on the Data Mover during the creation of the initial entry.

Create the home directory file

Action
To enable home directories on the Data Mover, use this command syntax:
$ **server_cifs** *<mover_name>* **-option homedir**
where:
<mover_name> = name of the Data Mover.
Example:
To enable home directories on server_2, type:
$ server_cifs server_2 -option homedir
Output
server_2 : done

Appendix A provides more information about the home directory database file.

Note: EMC recommends that for creating home directories you use the Home Directory management MMC snap-in to create and edit user home directory entries. The MMC snap-in validates the entries as you type them. If you create or edit the homedir file and type an incorrect entry, the home directory environment might become unusable. The VNX management MMC snap-in online help provides more information about creating directories automatically.

Add home directories to user profiles

Action
To allow user access to individual home directories, you must map the home directory in each user profile with the following path: *<cifs_server>***HOME**   where: *<cifs_server>* = IP address, computer name, or NetBIOS name of the CIFS server.   HOME = special share name reserved for the home directory feature.   Example: To map the home directory in each user profile on dm32-cge0, type: **\\\\dm32-cge0\\HOME**

Perform these tasks to add home directories for user profiles:

Add home directories from Windows Server

1. Log in to a Windows Server from a domain administrator account.

2. Click **Start** and select **Programs ➤ Administrative Tools ➤ Active Directory Users and Computers**.

3. Click **Users** to display the users in the right pane.

4. Right-click a user and select **Properties**. The **Sample User Properties** window appears.

5. Click the **Profile** tab and in the **Home folder** section:

   a. Select **Connect**.

   b. Select the drive letter you want to map to the home directory.

   c. In the **To** field, type:

   \\\\<cifs_server>\\HOME

   Where:

$<cifs\_server>$ = IP address, computer name, or NetBIOS name of the CIFS server.

6. Click **OK**.

Add home directories with regular expressions

1. Log in to a Windows Server from a domain administrator account.

2. Click and select **Start ➤ Programs ➤ Administrative ToolsCelerra Management**.

3. Right-click the Homedir folder icon and select **New ➤ home directory entry**. The home directory property window appears.

4. In the home directory properties window:

   a. In **Domain**, type a regular expression. In this example, the expression matches any domain name that begins with DOC.

   b. In **User**, type a regular expression. In this example, an asterisk matches any username.

   c. In the Path, type \homedirs\<u>. In this example, homedirs is the share where home directories are stored. <u> is the login name of the user. A directory with the same name as the login name of the user will be created, if it does not already exist.

5. Click **OK**.

Regular expressions on page 156 provides more information.

Disable home directories on the Data Mover

Action
To disable home directories on a Data Mover, use this command syntax:
$ **server_cifs** *<mover_name>* **-option homedir=no**
where:
<mover_name> = name of the Data Mover.
Example:
To disable home directories on server_2, type:
$ server_cifs server_2 -option homedir=no

Manage group policy objects

Perform these tasks to manage group policy object (GPO) support:

- Display GPO settings on page 116
- Update GPO settings on page 117
- Disable GPO support on page 119
- Disable GPO caching on page 119

Group policy objects on page 35 provides conceptual information.

Display GPO settings

Note: You can display group policy object (GPO) settings for each CIFS server joined to a Windows Server domain.

Action
To display the current GPO settings for the Data Mover, use this command syntax:
$ **server_security** *<mover_name>* **-info -policy gpo**
where:
<mover_name> = name of the Data Mover.
Example:
To display the current GPO settings for server_2, type:
$ server_security server_2 -info -policy gpo

Output
``
server_2:
Server compname: k10eqa19s2
Server NetBIOS: K10EQA19S2
.
.
.
by days
Retention Method for application log server list: k10eqa19s2
Disable background refresh of Group Policy: Not defined
Group Policy Refresh interval (minutes): 60
Refresh interval offset (minutes): 5
GPO Last Update time (local): Wed Sep 10 14:47:42 EDT
2007
GPO Next Update time (local): Wed Sep 10 15:50:42 EDT
2007
``

Note: To display the GPO settings for all the CIFS servers on all the Data Movers, use the ALL option of the server_security command.

Update GPO settings

While the CIFS service is running or after restarting the CIFS service, the Data Mover updates its group policy object (GPO) settings based on one of the following refresh intervals:

◆ If defined in the domain, the refresh interval can be set from zero (updates every 10 seconds) up to 64800 minutes (updates every 45 days).

◆ If not defined in the domain, the Data Mover uses its default refresh value of 90 minutes.

Perform these tasks for GPO updates:

Disable automatic GPO updates

Action
To disable the automatic GPO updates, enable the Disable background refresh of Group Policy GPO setting.

Output

```
Disable background refresh of Group Policy: Enabled
Group Policy Refresh interval (minutes): 90
Refresh interval offset (minutes): Not defined
GPO Last Update time (local): Wed Sep 10 14:47:42 EDT 2007
GPO Background Update disabled, must be updated manually
```

Update GPO settings manually for all Data Movers

If you change group policies through Microsoft Management Console (MMC) or the Server Manager, you can force an update of the GPO settings on the VNX.

Action
To force an update of GPO settings for the Data Mover, use this command syntax:
$ **server_security** *<mover_name>* **-update -policy gpo**
where:
<mover_name> = all Data Movers.
Example:
To force an update of GPO settings for server_2, type:
$ server_security server_2 -update -policy gpo
Output
server_2 : done

Note: To update the GPO settings for all the CIFS servers on all the Data Movers, use the ALL option of the server_security command.

Update GPO settings manually for the specified domain

Action
To force an update of GPO settings for the Data Mover in a specified domain, use this command syntax:
$ **server_security** *<mover_name>* **-update -policy gpo domain=***<domain_name>*
where:
<mover_name> = name of the Data Mover.
<domain_name> = domain name of the CIFS server.
Example:
To update the GPO settings for server_2 in domain NASDOCS, type:
$ server_security server_2 -update -policy gpo domain=NASDOCS
Output
server_2 : done

Note: To update the GPO settings for all CIFS servers in domain NASDOCS, use the ALL option of the server_security command.

Disable GPO support

Group policy object (GPO) support is enabled per Data Mover and is enabled by default. When GPO support is disabled, VNX cannot access the Windows domain controller, and the related VNX functions automatically use their own default settings.

The *Parameters Guide for VNX for File* provides additional information about the cifs gpo parameter.

Action
To disable GPO support, use this command syntax:
$ **server_param** *<mover_name>* **-facility cifs -modify gpo -value 0**
where:
<mover_name> = name of the Data Mover.
Example:
To disable GPO support on server_2, type:
$ server_param server_2 -facility cifs -modify gpo -value 0
Output
server_2 : done

Note: Parameter and facility names are case-sensitive.

Disable GPO caching

The Data Mover caches the group policy object (GPO) settings retrieved from the Windows domain controller. The GPO cache allows a Data Mover to quickly retrieve GPO settings even when the domain controller is inaccessible.

You can disable GPO caching if you do not want the Data Mover to use cached settings. If GPO caching is disabled, the Data Mover must retrieve the settings from the Windows domain controller.

The *Parameters Guide for VNX for File* provides additional information about the cifs gpocache parameter.

Note: If you disable GPO caching and VNX cannot access the Windows domain controller, the related VNX functions use their own default settings.

Action
To disable GPO caching, use this command syntax:
$ **server_param** *<mover_name>* **-facility cifs -modify gpocache -value 0**
where:
<mover_name> = name of the Data Mover.
Example:
To disable GPO caching on server_2, type:
$ server_param server_2 -facility cifs -modify gpocache -value 0
Output
server_2 : done

Note: Parameter and facility names are case-sensitive.

Disable alternate data streams

Alternate Data Stream (ADS) support is controlled by the shadow stream parameter and is enabled by default. Although there are rare cases when you might want to disable ADS support, EMC generally recommends that alternate data stream support be enabled. Alternate data stream support on page 44 provides more information.

The *Parameters Guide for VNX for File* provides additional information about the shadow stream parameter.

Action
To disable ADS support, use this command syntax:
$ **server_param** *<mover_name>* **-facility shadow -modify stream -value 0**
where:
<mover_name> = name of the Data Mover.
Example:
To disable ADS support on server_2, type:
$ server_param server_2 -facility shadow -modify stream -value 0
Output
server_2 : done

Configure SMB signing

Perform these tasks to configure server message block (SMB) signing:

- Configure SMB signing with the smbsigning parameter on page 121
- Disable SMB signing on a Data Mover on page 121
- Configure SMB signing with GPOs on page 121
- Configure SMB signing with the Windows Registry on page 122

SMB protocol support on page 45 provides conceptual information.

Configure SMB signing with the smbsigning parameter

The cifs.smbsigning parameter controls server message block (SMB) signing on the Data Mover and affects all CIFS servers on the Data Mover. This parameter is configured on the individual Data Mover or VNX, and controls the client-side and server-side signing.

Refer the *Parameters Guide for VNX for File* for additional information on using the cifs.smbsigning parameter.

Disable SMB signing on a Data Mover

Action
To disable SMB signing, use this command syntax:
$ **server_param** *<mover_name>* **-facility cifs -modify smbsigning -value 0**
where:
<mover_name> = name of the Data Mover.
Example:
To disable SMB signing support on server_2, type:
$ server_param server_2 -facility cifs -modify smbsigning -value 0
Output
server_2: done

Configure SMB signing with GPOs

If you want independent control of server-side and client-side server message block (SMB) signing, you can configure the GPOs shown in Figure 5 on page 122. These group policy

objects (GPOs) are found under the **Default Domain Security Settings** and can be configured from any domain controller.

To access **Default Domain Security Settings** go to **Start ➤ Control Panel ➤ Administrative Tools ➤ Domain Security Policy**.

Figure 5. SMB signing GPOs in default domain security settings

Note: Configuring SMB signing through GPOs affects all clients and servers within the domain and overrides individual Registry settings.

Configure SMB signing with the Windows Registry

Table 14 on page 122 explains the group policy objects available for SMB signing.

Table 14. SMB signing GPOs

GPO name	What it controls	Default setting for Data Mover
Microsoft network server: Digitally sign communications (always)	Whether the server-side SMB component requires signing	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Whether the server-side SMB component has signing enabled	Disabled

Table 14. SMB signing GPOs *(continued)*

GPO name	What it controls	Default setting for Data Mover
Microsoft network client: Digitally sign communications (always)	Whether the client-side SMB component requires signing	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Whether the client-side SMB component has signing enabled	Enabled

You can also configure server message block (SMB) signing through the Windows Registry. If there is no group policy object (GPO) service available, such as in a Windows NT environment, the Registry settings are used.

Registry settings affect only the individual server or client that you configure. Registry settings are configured on individual Windows workstations and servers and affects individual Windows workstations and servers. There are four Registry settings—two for server-side and two for client-side signing, and they function the same as the SMB signing GPOs.

Note: The following Registry settings pertain to Windows NT with SP 4 or later. These Registry entries exist in Windows Server, but should be set through GPOs.

Server-side signing

The server-side settings are located in:

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\`

shows the server-side SMB signing Registry entries.

Table 15. Server side SMB signing Registry entries

Registry entries	Values	Purpose
enablesecuritysignature	0 disabled (default) 1 enabled	Determines if SMB signing is enabled
requiresecuritysignature	0 disabled (default) 1 enabled	Determines if SMB signing is required

Client-side signing

The client-side settings are located in:

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\`

shows the client-side SMB signing Registry entries.

Table 16. Client side SMB signing Registry entries

Registry entries	Values	Purpose
enablesecuritysignature	0 disabled 1 enabled (default)	Determines if SMB signing is enabled
requiresecuritysignature	0 disabled (default) 1 enabled	Determines if SMB signing is required

Manage SMB2 and SMB3 protocols

The tasks to manage SMB2 and SMB3 protocols are:

- Enable the SMB2 protocol on page 124
- Enable the SMB3 protocol on page 125
- Configure the Continuous Availability functionality on the Data Mover on page 125
- Disable the SMB2 and SMB3 protocols on page 127
- Create a symbolic link to a file with a relative path on page 127

SMB protocol support on page 45 provides conceptual information.

Enable the SMB2 protocol

Action
To enable the SMB2 protocol, use this command syntax: $ **server_cifs** *<mover_name>* **-add security=NT,dialect=SMB2** where: *<mover_name>* = name of the Data Mover. Example: To enable the SMB2 protocol on server_2, type: **$ server_cifs server_2 -add security=NT,dialect=SMB2**
Output
done

Enable the SMB3 protocol

SMB3 is enabled by default with the for a fresh install. In case of an upgrade, if you have modified the MAX protocol dialect using the server_cifs command then the MAX protocol will not be default one. Perform this task to enable the SMB3 protocol:

Action
To enable the SMB3 protocol, use this command syntax:
$ **server_cifs** *<mover_name>* **-add security=***<security_mode>* **dialect=***SMB3*
where:
<mover_name> = name of the Data Mover
<security_mode> = NT
Example:
To configure the max SMB dialect on server_2, type:
$ server_cifs server_2 -add security=NT dialect=SMB3
Output
server_2: done

Note:

◆ The keyword that is used for the dialect option in the server_cifs command indicates the maximum supported dialect. For example, when you enable SMB3, all protocol dialects up to SMB 3.0 are enabled, including NT1, SMB2.0, and SMB 2.1.

◆ To switch to SMB1, use NT1 dialect.

◆ SMB2 indicates the max dialect in SMB2=> SMB2.1. SMB2.0 or SMB2.1 can be specified explicitly.

◆ SMB3 indicates max dialect in SMB3 => SMB3.0. SMB 3.0 can be specified explicitly.

Configure the Continuous Availability functionality on the Data Mover

You must start by setting 'smbca' capability on the file system (required for multiprotocol environment):

1. To mount the smbca ount option on the file system, use this command syntax:

   $ **server_mount** *<movername>***-o smbca fs1**

   where:

<movername>= name of the Data Mover

Example:

```
$server_mount server_2 -o smbca fs1
```

Output:
```
server_2: done
```

2. To create a CIFS share, type:

```
$ server_export server_2 -Protocol cifs -name ufs/fs1
```

Output:
```
server_2: done
```

3. To display the details of the CIFS share ufs, type:

```
$server_export server_2 -Protocol cifs -list -name usf
```

Output:

```
server_2 :

share "ufs" "/fs1" umask=022 maxusr=4294967295 type=Global  >>>> share
created as a global share
```

4. To display the specific share ufs, type:

```
$server_export server_2 -Protocol cifs -name ufs -option type=Global:CA
/fs1 >>> Bit CA added
```

Output:
```
server_2: done
```

5. To list the CIFS entries, type:

```
$server_export server_2 -Protocol cifs -name ufs -list
```

Output:

```
server_2 :

share "ufs" "/fs1" umask=022 maxusr=4294967295 type=Global  >>>> share
created as a global share
```

Disable the SMB2 and SMB3 protocols

Action
To disable both SMB3 and SMB2 protocols, enabling the SMB1 protocol, use this command syntax: $ **server_cifs** *<mover_name>* **-add security=NT,dialect=NT1** where: *<mover_name>* = name of the Data Mover. Example: To disable both SMB3 and SMB2 protocols, enabling the SMB1 protocol on server_2, type: $ **server_cifs server_2 -add security=NT,dialect=NT1**
Output
done

Note: To disable any one of the protocols (SMB2 or SMB3), mention the dialect as NT1 in the server_cifs command.

Create a symbolic link to a file with a relative path

SMB2 support for symbolic links on page 48 provides conceptual information.

Action
To create a symbolic link from a MS DOS console on the SMB2 client, use this command syntax: **mklink** *<symlink> <target>* where: *<symlink>* = name of the symbolic link. *<target>* = location and name of the target. Example: To create a symbolic link target1 that points to a file with an absolute pathname from a MS DOS console on the SMB2 client, type: **mklink target1 myData\applicationData\file1.txt**
Output
``` d:\temp>mklink link0.txt report.txt symbolic link created for link0.txt <<===>> report.txt d:\temp> ```

Note: The creation of symbolic link with an absolute path or an UNC path works the same way. When creating a symbolic link to a directory, use mklink /d to indicate a directory.

Change the default symbolic link behavior

To modify the default behavior of symbolic links:

- ◆ Enable symbolic links with absolute paths on page 129
- ◆ Enable symbolic links with target paths to parent directories on page 128

Enable symbolic links with target paths to parent directories

By default, the Data Mover does not resolve symbolic links that have a pathname that refers upward using the ".." component.

⚠ CAUTION   Enabling the shadow followdotdot parameter so that the Data Mover follows symbolic links upwards on behalf of Windows clients might create infinite loops in the namespace presented to Windows clients. Applications that perform a search of the namespace have the risk of getting stuck in an infinite loop.

Action
To enable the Data Mover to follow symbolic links with the '..' component in the target pathnames, use this command syntax:
$ **server_param** *<movername>* **-facility shadow -modify followdotdot -value 1**
where:
<movername> = name of the Data Mover
Example:
To enable symbolic links with target paths to parent directories on server_2, type:
$ **server_param server_2 -facility shadow -modify followdotdot -value 1**
Output
server_2 : done

Enable symbolic links with absolute paths

By default, the Data Mover will not follow symbolic links that contain absolute paths (full pathnames).

Note: When the shadow followabsolutpath parameter is enabled to follow absolute paths, the target is interpreted by the Data Mover. The Data Mover can only resolve paths that are relative to the root file system on the Data Mover. If this is a Virtual Data Mover, this path must be the root of the VDM (for example, /mountpoint/directory); otherwise, a Windows client is unable to access the target.

Note: With NFS, clients read a symbolic link target path and try to access the target by doing a local lookup on the client. NFS clients must have the same mount point as the Data Mover to access targets with absolute paths.

Action

To enable the Data Mover to follow symbolic links when the target is an absolute path, use this command syntax:
 	
$ **server_param** *<movername>* **-facility shadow -modify followabsolutpath -value** *<new_value>*
 	
where:
 	
<movername> = name of the Data Mover or VDM
 	
<new_value> = Bit list
 	
◆ Bit 0:
 	
    0 = does not allow symbolic links that contain an absolute path
 	
    1= allows symbolic links that contain an absolute path to be followed
 	
◆ Bit 1:
 	
    0 = allows only absolute symbolic links owned by root (UID 0) to be followed
 	
    1= allows any absolute symbolic links to be followed
 	
Note: Setting Bit 1 creates a potential security issue for NFS access because the NFS client can create an absolute symbolic link to any location in the Data Mover. If Bit 1 is not set, only links owned by the root (uid 0) are followed.
 	
Example:
 	
To enable symbolic links when the target is an absolute path, type:
 	
$ **server_param server_2 -facility shadow -modify followabsolutpath -value 1**

Output
server_2 : done

Access symbolic links through CIFS clients

You must have root privileges to create a symbolic link.

Perform the following steps using the Control Station and an NFS client.

1. Set the shadow followabsolutpath parameter to enable symbolic links with absolute paths.

   Example:

   To enable server_2 to follow symbolic links when the target is an absolute path, type:

   ```
   $ server_param server_2 -facility shadow -modify followabsolutpath -value 1
   ```

2. Mount the file systems.

   Example:

   To mount ufs1 and ufs2, type:

   ```
   $ server_mount server_2

   server_2 :
   root_fs_2 on / uxfs,perm,rw
   root_fs_common on /.etc_common uxfs,perm,ro
   ufs1 on /ufs1 uxfs,perm,rw
   ufs2 on /ufs2 uxfs,perm,rw
   ```

3. Create a share to the top-level file system.

   Example:

   To create a share to ufs1, type:

   ```
   $ server_export server_2
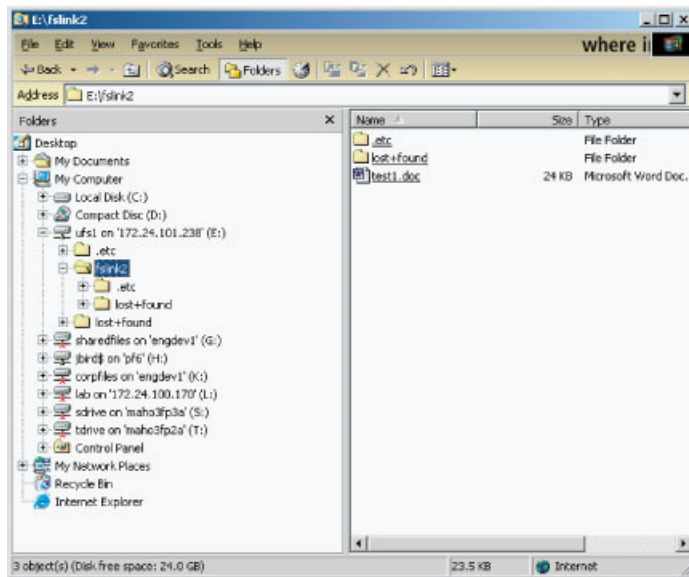
   server_2 :
   export "/ufs1"
   share "ufs1" "/ufs1" netbios=NS700-JB1 maxusr=4294967295 umask=22
   ```

4. Mount the top-level file system on an NFS client.

   Example:

   To mount ufs1 on an NFS client, type:

   ```
   # mount 192.168.101.238:/ufs1 /ufs1 # mount 192.168.101.238:/ufs1 on /ufs1 type
   nfs (rw,addr=192.168.101.238)
   ```

5. Create a symbolic link to the second file system.

   Example:

   To create a symbolic link from ufs1 to ufs1, type:

   ```
   # ln -s /ufs2 fslink2 # ls -l
   ```

```
total 8
lrwxrwxrwx    1 root      root           5 Jun 10  2004 fslink2 -> /ufs2
drwxr-xr-x    2 root      root        8192 Jun  9 12:14 lost+found
```

Note: Checkpoints of a linked file system do not appear under the top-level file system. You must be in the linked file system directory to view these checkpoints.

The command ln -s /ufs2 fslink2 links fslink2 to the path /ufs2 as it applies to the Data Mover. CIFS clients accessing the ufs1 share can view fslink2 as one of its directories, as shown in the following illustration.

Note: NFS clients cannot access fslink2 because the client has no knowledge of its path on the Data Mover.

Configure automatic computer password changes

You can activate computer password changes by doing one of the following:

- Setting a group policy object (GPO) to a password change interval. The Data Mover retrieves this policy and applies it to all CIFS servers within the domain.

- Setting the cifs srvpwd.updtMinutes parameter that is overridden by the GPO policy.

- Changing the password change interval for a particular CIFS server by using the srvpwd interface that is overridden by any GPO policy.

The system parameter cifs srvpwd.updtMinutes lets you configure the time interval at which the Data Mover changes passwords with the domain controller.

The *Parameters Guide for VNX for File* provides additional information about the cifs srvpwd.updtMinutes parameter.

Change time interval for password changes

Action
To change the password change time interval, use this command syntax:
$ **server_param** *<mover_name>* **-facility cifs** **-modify srvpwd.updtMinutes -value** *<new_value>*
where:
<mover_name> = name of the Data Mover.
<new_value> = minimum time interval between CIFS server password changes. Value 0 allows server password change after 7 days minus 1 hour. Value 720 allows server password change after 12 hours. Value 1440 allows server password change after 24 hours.
Example:
To set the password interval to one day (1440 minutes), type:
$ server_param server_2 -facility cifs -modify srvpwd.updtMinutes -value 1440
Output
server_2: done

Note: When configured for automatic computer account password updates, the CIFS server initiates an attempt to change the password at 80 percent of the configured time limit. This is done to provide time for a retry. It also gives the administrator an advanced warning in case of any problem in the environment before the password expires, to prevent any access issues.

Change the location of the Windows security log

By default, each Data Mover stores its Windows security log at C:\security.evt, which has a size limit of 512 KB. You can access this security log through the C$ share of each Data Mover:

```
\\<netbiosnameofdatamover>\C$\security.evt
```

On a Windows Server, the security log is located at:
C:\WINNT\System32\config\security.evt. If an application tries to access the Windows security log of a Data Mover at this location, it fails. However, you can change the location and the size limit of the Data Mover's Windows security log.

⚠ CAUTION Incorrectly modifying the Registry might cause serious system-wide problems that require you to reinstall the system. Use this tool at your own risk.

You can access the Windows security log for a Data Mover in one of the following two ways:

1. Create a file system to store the security log in its new location.

2. Mount the file system on the Data Mover on a mount point called /WINNT and share it.

3. From a CIFS client, connect to the new WINNT share on the Data Mover and create the folder structure System32\config under the WINNT directory. This enables you to access the path \\<netbiosnameofdatamover>\C$\WINNT\System32\config.

4. As the domain administrator, perform the following steps using the Windows Registry Editor:

    a. Run the Registry Editor (regedt32.exe).

    b. From the **Registry** menu, select the **Select Computer**, and select the Data Mover NetBIOS name.

    c. From the **Window** menu, select the **Hkey Local Machine on Local Machine** subtree, and go to the key System\CurrentControlSet\Services\Eventlog\Security.

    d. Select the string [File: REG_EXPAND_SZ:c:\security.evt].

    e. From the **Edit** menu, select **String**.

    f. Edit the string that has information c:\WINNT\System32\config\security.evt.

    g. Click **OK** and quit the Registry Editor. All Windows security events on the Data Mover are now logged to the new security event log location.

Join a CIFS server to a Windows domain—Advanced Procedures

Before you begin

The configuration prerequisites are based on Microsoft Knowledge Base article 258503: DNS Registration Errors 5788 and 5789 when DNS Domain and AD Domain Name Differ. This article explains how to set domain-level permissions.

The configuration prerequisites explained in Microsoft Knowledge Base article 258503 are required only if the DNS domain name on the CIFS client has changed and if the new DNS domain name does not match the active directory (AD) domain name for the CIFS client.

Perform these tasks for add and join procedures:

* Create a CIFS server for Windows Server environments on page 65
* Join a CIFS server to a Windows domain for a disjoint namespace and a delegated join on page 134
* Join a CIFS server to a Windows domain for the same namespace and a delegated join on page 135
* Add the user performing the join to the local administrators group on page 136

Procedure

The procedure for creating and joining a CIFS server to a Windows domain differs when:

* DNS domain name is disjoint with the Windows domain name of the computer.
* User account is delegated.

Note: Delegating joins on page 40 provides conceptual information. The article explaining Disjoint Namespace at Microsoft Technet website provides detailed information.

Join a CIFS server to a Windows domain for a disjoint namespace and a delegated join

Action
To join the CIFS server to the Windows domain, use this command syntax:
$ **server_cifs** *<mover_name>* **-Join compname**=*<comp_name.FQDN>*, **domain**=*<full_domain_name>*,**admin**=*<user_name>*@**realm**
where:
<mover_name> = name of the Data Mover or VDM.
<comp_name> = name for the CIFS server's account in the Active Directory. For disjoint namespaces, you must type compname.FQDN; otherwise, the AD attributes are not updated. For example: compname=dm32-cge0.nasdocs.emc.com.
<full_domain_name> = full domain name for the Windows environment.
<user_name>@realm = delegated user login name and domain name of the Active Directory.
Example:
To join the CIFS server dm32-ana0 to the universe.com domain, type:
$ **server_cifs server_2 -Join compname=dm32-cge0.nasdocs.emc.com,domain=universe.com,admin=user@universe.com**

Output	Note
| ```
CIFS Server SERVER1[WIN] RC=2
Full computer name=server1.win.com
realm=WIN.COM
Comment='EMC-SNAS:T5.6.43.0'
if=cge0 l=172.24.100.47
b=172.24.100.255 mac=0:60:16:4:43:ed
FQDN=server1.abc.net (Updated to DNS)
Password change interval: 720 minutes
Last password change: Thu Feb 26
10:28:23 2009 GMT
Password versions: 53, 52
``` | The user account and user password are used to create the account in the Active Directory, and are not stored after adding the machine account. |

Note: The <comp_name> value must match the fully qualified domain name (FQDN) of the interface of the CIFS server. For example, if the Windows domain is win.com, the DNS primary suffix is abc.net, and the CIFS server is server1, the command would be server_cifs <mover_name> -Join c ompname=server1.abc.net,domain=win.com.

Join a CIFS server to a Windows domain for the same namespace and a delegated join

Action
To join the CIFS server to the Windows domain, use this command syntax:
$ **server_cifs** *<mover_name>* **-Join compname**=*<comp_name>*, **domain=***<full_domain_name>*,**admin=***<user_name>*@**realm**
where:
<mover_name> = name of the Data Mover or VDM.
<comp_name> = name for the CIFS server account in the Active Directory.
<full_domain_name> = full domain name for the Windows environment.
<user_name>@realm = delegated user login name and domain name of the Active Directory.
Example:
To join the CIFS server dm32-ana0 to the universe.com domain, type:
$ server_cifs server_2 -Join compname=dm32-cge0,domain=universe.com,admin=user@universe.com

Output	Note
| ```
server_2 : Enter Password: *******
done
``` | The user account and user password are used to create the account in the Active Directory, and are not stored after adding the machine account. |

Add the user performing the join to the local administrators group

Each CIFS server contains a set of built-in user groups: Administrators, Users, Guests, Power Names, Account Operators, Backup Operations, and Replicator. The Administrators group contains the users and groups authorized to manage the CIFS server. By default, the Administrators group contains one entry for the Domain Admins group, which gives each member of the Domain Admins group the authority to manage the CIFS server.

To add the user to the local administrative group for the user to be able to manage the CIFS server, set the cifs djAddAdminToLg parameter to 1. The *Parameters Guide for VNX for File* provides additional information.

Customize file filtering pop-up messages

Following are the error codes that can be used with the cifsmsg.txt file:

- FileDeletedByVC
- FileRenamedByVC
- FileModifiedByVC
- File_ReservedName
- Remote
- NoSpace
- QuotaExceeded
- GroupQuotaExceeded
- TreeQuotaExceeded

1. Log in to the Control Station as root.

2. Copy the cifsmsg.txt file from the Data Mover to the Control Station by using this command syntax:

   ```
   # server_file server_<x> -get cifsmsg.txt cifsmsg.txt
   ```

   Where:

   <x> = Data Mover that has the cifsmsg.txt file that you want to copy to the Control Station and edit.

   Example:

   To copy the file from server_2, type:

   ```
   # server_file server_2 -get cifsmsg.txt cifsmsg.txt
   ```

Note: If this file does not exist, you must create it and specify the information shown in the next steps. If you do not create this file, VNX uses default messages in the pop-up windows.

3. Open the cifsmsg.txt file with a text editor. To change an error message, use this syntax:

   $ **error.***<error.condition.code>*=

   <popup message line 1>

   .

   .

   .

   <pop-up message line n>

   .

   Where:

   <error.condition.code> = condition upon which you want the message to be sent.

   <pop-up message line> = message that you want to send (such as the nature of the condition, contact information, and suggested action).

   Important: The last line must be a period (.).

   All pop-up messages also contain the share name and filename.

   Hint: To avoid repeating the same text for different messages, use the following syntax:

   $ **error.***<error.condition.code3>*=$ **error.***<error.condition.code2>*

4. Save and close the file, and then type:

   ```
   $  server_file server_2 -put cifsmsg.txt cifsmsg.txt
   ```

5. To implement the changes that you made to the cifsmsg.txt file, restart (stop and start) the CIFS service on the Data Mover (<x>) by using this command syntax:

   ```
   $ server_setup server_<x> -P cifs -o stop
   ```

   ```
   $ server_setup server_<x> -P cifs -o start
   ```

6

Troubleshooting

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

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

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

Topics included in this chapter are:

EMC E-Lab Interoperability Navigator

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

VNX user customized documentation

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

Known problems and limitations

Table 17 on page 141 describes known problems that might occur when managing VNX for Windows environment and presents workarounds.

Table 17. Windows environment known problems and workarounds

Known problem	Symptom	Workaround
With NT user authentication, certain Windows 95 clients might not be able to map drives from the Data Mover.	The domain name sent to the Data Mover by the client was incorrectly specified, or the username.domain is not mapped in the passwd file on the Data Mover.	Verify that the client is sending the correct domain name to the passwd file on the Data Mover. To verify that the client is sending the correct domain: 1. In the Network option in the Control Panel, double-click the network client (Client for Microsoft Networks). 2. Under General properties, verify that the correct domain name is shown.
With NT user authentication, the error message `Incorrect password or unknown username` appears after attempts to connect to the server, and the username and password window appears.	The Windows NT user account might be missing from the PDC domain, or the Data Mover was unable to determine a UID to use for this user.	Add the Windows NT user to the PDC of the domain and map the user to a UNIX username and UID.
Unable to create files or directories in a share that is mapped to a client.	UNIX permission bits are not set to grant permission for the user to write to the shared directory. Note: This situation occurs if the access policy is set incorrectly. *Managing a Multiprotocol Environment on VNX* provides more information.	Change the access policy or mount the directory over NFS on the Control Station or any other UNIX client, and use chmod to set the appropriate UNIX permission to allow the user to be able to write to it.

Table 17. Windows environment known problems and workarounds *(continued)*

Known problem	Symptom	Workaround

Windows clients cannot connect to a server by using clear text passwords. (For example, this might occur when VNX is in UNIX mode.)
 	
The following error message might appear:
 	
`The Account is not authorized to login from this station`
	The SMB redirector handles unencrypted passwords differently than previous version of Windows NT. The SMB redirector does not send an unencrypted password unless you add a Registry entry to enable unencrypted passwords.	You must modify the Registry to enable unencrypted passwords:
		
		⚠️ **CAUTION** Incorrectly modifying the Registry might cause serious system-wide problems that might require you to reinstall the system. Use this tool at your own risk.
		
		1. Run Registry Editor (Regedt32.exe).
		
		2. From the HKEY_LOCAL_MACHINE subtree, go to the following key:
		System\CurrentControlSet\Services\rdr\parameters
		  a. Under this key, create a new DWORD Registry key named EnablePlainTextPassword.
		  b. Set its value to 1.
		  c. Restart the computer.
		
		3. Select **Add Value** on the **Edit** menu.
		
		4. Add the following:
		Value Name: EnablePlainTextPassword
		Data Type: REG_DWORD
		Data: 1
		
		5. Click **OK** and quit Registry Editor.
		
		6. Shut down and restart Windows NT.

Table 17. Windows environment known problems and workarounds *(continued)*

Known problem	Symptom	Workaround
		Note: Use GPOs for Windows Server clients. This procedure was adapted from Article ID: Q166730 of the Microsoft Knowledge Base.
With NT user authentication, clients are unable to connect to the server, and the window to prompt for username and password does not appear on the client side.	No domain controller found for the domain.	Check if PDC or BDC is up. Check if Data Mover can access a WINS server that knows about the PDC domain, or have the PDC or BDC in the same local subnet as the Data Mover.

	The server's NetBIOS name is not registered as a computer account on the PDC domain or a trust relationship has not been established between the client and server domains.
	
	The following message might appear in the server_log:
	
	`The SAM database on the`
	`  Windows NT server does`
	
	`not have a complete`
	`account for this`
	`workstation trust`
	`relationship.`
		Add a computer account to the PDC. If the computer account does exist, remove it and add it again before retrying the command. Microsoft NT server 4.0 documentation provides information on how to set up a trust relationship between domains.

Table 17. Windows environment known problems and workarounds *(continued)*

Known problem	Symptom	Workaround

After joining a CIFS server to a domain, the following error appears in the server_cifs output, indicating the system cannot update the DNS record:
 	
`FQDN=dm4-`
 	
`a140-ana0.`
 	
`c1t1.pt1.c3lab.`
 	
`nsgprod.emc.com`
 	
`(Update`
`of "A" record failed`
`during update: Operation`
` refused for policy or`
`security reasons)`
	The DNS Server zone might include the same fully qualified domain name (FQDN) for another computer account.	◆ Check whether the DNS server accepts the dynamic updates for the zone (property of the zone).
		
		◆ Verify that the DNS Server zone does not have the same FQDN with a different IP address for another computer account.
		
		◆ If the zone accepts only secured dynamic updates, verify the content of the security tab for the record and check if the access control list includes an entry with "S-1-5..." as owner name. Such a security entry indicates that the record belongs to a deleted computer account. The DNS record must be removed manually.

Table 17. Windows environment known problems and workarounds *(continued)*

Known problem	Symptom	Workaround

When attempting to join a CIFS server to a domain, the following error message appears:
 	
`Error 4020: server_2 :`
 	
`failed to complete command`
 	
`Possible server_log error`
 	
`messages:`
 	
`2004-03-11`
 	
`13:42:29: SMB: 3:`
 	
`DomainJoin::`
 	
`getAdminCreds:`
 	
`gss_acquire_cred_ext failed: Miscellaneous`
 	
`failure. Clients credentials`
`have been revoked.`
 	
`2004-03-11 13:42:29: ADMIN: 3:`
 	
`Command failed: domjoin`
 	
`compname=dm3-A121-`
 	
`ana0 domain=c1t1.pt1.`
 	
`c3lab.nsgprod.emc.com`
 	
`admin=c1t1admin`
 	
`password=6173399`
 	
`D179D3999673D init`
	Domain administrator account was locked out. Typically, this happens when another user is logged in with the same administrator account on another system.	Clear the Account is locked out checkbox on the Account tab of the User Account Properties window.

Table 17. Windows environment known problems and workarounds *(continued)*

Known problem	Symptom	Workaround

If you create the computer without enabling Allow pre-Windows 2000 computers to use this account option, the following error message appears:
 	
`0xC0000022 2004-04-26`
 	
`10:49:40: SMB: 3:`
 	
`Srv=<Celerra_`
 	
`netbios_name>`
 	
`buildSecureChanel`
 	
`=Authenticate2`
 	
`InvalidReply E=0xc`
	Access is denied because the computer was created on the domain controller without enabling the Allow pre-Windows 2000 computers to use this account option on the Windows New Object - Computer dialog box.	Delete the computer and then recreate it with the Allow pre-Windows 2000 computers to use this account option enabled.

After upgrading from a Windows NT domain to Windows 2000, unable to change the original domain suffix during Windows 2000 setup.	Unable to change domain suffix because it was hardcoded in DDNS.	Before upgrading, change the domain suffix.

Access is denied to Internet Information Services (IIS) 6.0 when attempting to connect to the web directory on a VNX share.
 	
In the IIS web log, the error:
 	
`bad user name`
`or password`
 	
appears even though the username and password are in the local user database.
	For a stand-alone CIFS server with local user support enabled, the username and password must be the same on IIS 6.0, the Data Mover, and the client.	Specify the same username and password on IIS 6.0, the Data Mover, and the client.

Symbolic link limitations

The limitations of file linking are:

◆ When a user follows a link from the top-level file system to a subordinate file system, the access-checking policy on the top-level file system is applied to the subordinate file system.

◆ The file system size of the top-level file system (from where the user is connecting) does not reflect the size of the subordinate file systems.

◆ Quotas are always reported per file system. If there are users or groups or trees on subordinate file systems, each file system is reported individually.

◆ If notification requests are set on the top-level file system with the WatchTree bit, changes to subordinate file systems do not trigger notification.

◆ Some requests return the full pathname of open files. If an open file is on a file system accessed through a symbolic link, the path returned might not be the path expected.

◆ When traversing file systems through symbolic links, invoking the command cd .. might not return the directory containing the symbolic link (this is not an issue using Microsoft Windows Explorer).

◆ When restoring files from backups into linked file systems, always restore symbolic links first; otherwise, the entire restore is done to the top-level file system.

◆ If a subordinate file system is not mounted on a Data Mover, the symbolic link appears as a directory to CIFS clients. This directory is the root file system of the Data Mover.

Error messages

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

To view message details, use any of these methods:

◆ Unisphere software:

• Right-click an event, alert, or status message and select to view Event Details, Alert Details, or Status Details.

◆ CLI:

• Type nas_message -info <MessageID>, where <MessageID> is the message identification number.

◆ *Celerra Error Messages Guide*:

• Use this guide to locate information about messages that are in the earlier-release message format.

◆ EMC Online Support:

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

EMC Training and Professional Services

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

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

GPO conflict resolution

Audit policies are resolved by combining settings from the multiple servers on the Data Mover and using the most secure setting. The CIFS servers are processed in the order in which they were joined to the domain. Event log policies are resolved by using the most secure setting of all the related settings on the CIFS server. For example, for the maximum application log size setting, the system looks at the log size setting of each server on the Data Mover, and then uses the largest size. Table 18 on page 148 lists the GPO settings requiring conflict resolution.

Table 18. GPO settings requiring conflict resolution

Setting name	Shared across CIFS server (Yes/No)	Requires conflict resolution (Yes/No)	Possible values
Audit:			
Audit account logon events	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit account management	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit directory service access	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"

Table 18. GPO settings requiring conflict resolution *(continued)*

Setting name	Shared across CIFS server (Yes/No)	Requires conflict resolution (Yes/No)	Possible values
Audit logon events	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit object access	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit policy change	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit privilege use	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit process tracking	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Audit system events	Yes	Yes	"No Audit", "Success", "Failure", "Success, Failure"
Event logs:			
Maximum application log size	Yes	Yes	64 - 4194240
Maximum security log size	Yes	Yes	64 - 4194240
Maximum system log size	Yes	Yes	64 - 4194240
Restrict guest access to application log	Yes	Yes	"Enabled", "Disabled"
Restrict guest access to security log	Yes	Yes	"Enabled", "Disabled"
Restrict guest access to system log	Yes	Yes	"Enabled", "Disabled"
Retain application log	Yes	Yes	"Overwrite events by days", "Overwrite events as needed", "Do not overwrite events"
Retain security log	Yes	Yes	"Overwrite events by days", "Overwrite events as needed", "Do not overwrite events"

Table 18. GPO settings requiring conflict resolution *(continued)*

Setting name	Shared across CIFS server (Yes/No)	Requires conflict resolution (Yes/No)	Possible values
Retain system log	Yes	Yes	"Overwrite events by days", "Overwrite events as needed", "Do not overwrite events"
Retention method for application log	Yes	Yes	0 - 365
Retention method for security log	Yes	Yes	0 - 365
Retention method for system log	Yes	Yes	0 - 365

LDAP signing and encryption

The domain controller requires LDAP message signing. The following error message is logged if this does not occur:

```
00002028: LdapErr: DSID-0C090169, comment: The server requires binds to
turn on integrity checking if SSL\TLS are not already active on the
connection.
```

If you experience any problems with LDAP signing or encryption, do the following:

1. On the domain controller, set either the LDAP security policy (Windows Server 2003) or the LDAP Registry setting (Windows 2000) to **no signing**.

2. Set the ldap SecurityLayer parameter to 0.

3. Reboot the Data Mover.

SMB signing resolution

In Windows domains, you can separately configure server-side and client-side SMB signing settings:

◆ Required — Client or server requires that SMB signing is used in all transactions.

◆ Enabled — Client or server supports SMB signing but does not require it for transactions.

◆ Disabled — Client or server does not support any SMB signing.

The SMB signature is activated on a CIFS connection as per the criteria on the Data Mover and the CIFS client. The criteria are an addition of the two bits; enabled and required. The criteria are computed according to the following three values on the Data Mover:

1. cifs.smbSigning parameter

2. GPO settings

3. Registry values

The CIFS client executes its own algorithm to define its own bits: enabled and required. The matrix explained in Table 19 on page 151 and Table 20 on page 151 is applied to determine if the signature is activated for that connection or not.

Table 19. Resolution matrix for SMB1 signing

	Client			
	SMB1	Required	Enabled	Disabled
Server	Required	Signed	Signed	Fail
	Enabled	Signed	Signed	Not signed
	Disabled	Fail	Not signed	Not signed

Table 20. Resolution matrix for SMB2 signing

	Client		
	SMB2	Required	Enabled
Server	Required	Signed	Signed
	Enabled	Signed	Not signed

Note: The default value of the cifs.smbSigning parameter should not be changed.

DNS issues

You might encounter the following DNS issues while configuring VNX:

◆ With the Windows Server environment, the domain controller does not register itself into DNS when the domain is a top-level domain, for example, .com or .org. You can change this rule from the Windows Registry or by enabling the group policy Update Top Level Domain Zones option.

> Note: The Data Mover does not have an equivalent of this Registry entry and does not use the group policy because the Data Mover only updates the DNS zone for host entries and not for service entries.

◆ When two Windows-based DNS servers are working in the same DNS zone, their content might vary for several minutes. In DNS environments that have AD integrated zones, replication of the resource records is dependent on the AD replication, which occurs periodically. Replication might not occur immediately when changes are made; this is a Microsoft limitation.

MS Event Viewer snap-in

VNX CIFS servers support the MS Event Viewer snap-in for viewing logs on a VNX CIFS server. *Using Windows Administrative Tools on VNX* provides steps to connect the MMC to a CIFS server.

When you connect an Event Viewer to a CIFS server from a Windows Vista or Windows Server 2008, and experience problems with the Event Viewer help, perform the following:

1. Download and install the old executable for .hlp files from the Microsoft support website Windows Help program (WinHlp32.exe) is no longer included with Windows.

2. Retrieve the C:\Windows\Help\els.hlp file from a Windows Server 2003 or Windows XP machine and install it on the Windows Vista or Windows Server 2008 machine.

Appendix A

Additional Home Directory Information

This section provides additional information regarding the optional home directory feature described in Enable and manage home directories on page 112. The information in this section is intended for users who are creating or maintaining home directory configurations:

- Home directory database format on page 154
- Wildcards on page 155
- Regular expressions on page 156
- Parsing order on page 157
- Guest accounts on page 157

Home directory database format

This section outlines the format of the entries in the home directory database.

EMC recommends that you use the home directory Microsoft Management Console (MMC) snap-in to create and maintain the home directory. The snap-in validates entries and helps to ensure that the entries are correct and complete.

The following table contains the basic home directory database format.

Format
The database contains an entry for each user and uses the following format:
<domain>:*<username>*:*</path>* [:**regex**][:**create**][:**ro**][:*<umask>*]
where:
<domain> = Windows domain name (must be the NetBIOS name not the FQDN).
<username> = user's Windows username.
</path> = UNIX path of the parent home directory.
create = target directory will be created if it does not already exist.
regex = domain and username are regular expressions.
ro = read-only file access (the default is read/write).
<umask> = user file-creation <mask> for the umask allowing NFS permissions to be determined for the share.
The database might contain comments. Comments start with a # on a new line.
Example:
The following is an example of a database:
``` # Comment - These entries specify users in the galaxy domain. galaxy:glenn:/mnt1/usr1 galaxy:grissom:/mnt2/usr2 galaxy:armstrong:/mnt2/usr3 ```
where:
# = character that precedes comment text
galaxy = Windows domain
glenn, grissom, and armstrong = usernames
/mnt1/usr1,/mnt/usr2, and /mnt/usr3 = individual home directories for glenn, grissom, and armstrong, respectively.

Format
Wildcards

Format
Map files can contain wildcard entries. provides more information.

Example:

The following example is a database with wildcard entries:

```
*:*:/mnt3/guest
galaxy:*:/mnt3/CIFS
galaxy:glenn:/mnt1/usr1
galaxy:grissom:/mnt2/usr2
galaxy:armstrong:/mnt2/usr3
```

Create

Map files can indicate that directories should be created automatically. The parent directory must exist. In following example, the directory sales must exist before the directory usr1 can be created.

Example:

The following is an example of a database with a directory entry that will be created automatically:

```
galaxy:glenn:/mnt1/sales/usr1:create
```

Regular expressions

Map file entries can contain regular expressions. The VNX Management MMC plug-in online help provides a complete discussion on regular expressions.

Example:

The following is an example of a database with regular expression entries:

```
nasdocs:*:/ufs/user4/<d>/<u>:regex:create
 nasdocs:^[a-g]:/ufs/user1/<d>/<u>:regex:create
 nasdocs:^[h-p]:/ufs/user2/<d>/<u>:regex:create
 nasdocs:^[q-z]:/ufs/user3/<u>/<u>:regex:create
```

Umask

Map files can contain an NFS permissions mask that sets the permissions on newly created directories and files. This mask does not affect the CIFS ACL.

Note
Each field in the database must be separated by the ":" delimiter.

Wildcards

Map files can contain wildcards (*) for the domain and username fields. Wildcards let you assign home directories to multiple users without making individual entries for each user in the database.

For example, if the username field contains a wildcard, all users from the specified domain match the wildcard entry. In this situation, a directory with the user's Windows username in its path becomes the user's home directory.

Therefore, if the database contains galaxy:*:/mnt3/CIFS/, all users in the galaxy domain can access home directories under /mnt3/CIFS/ that match their usernames. For example, user1 in the galaxy domain can access the home directory /mnt3/CIFS/user1, and user2 can access the home directory /mnt3/CIFS/user2. Wildcard entries should be put at the beginning of the database, with specific entries following. Parsing order on page 157 provides more information.

Regular expressions

When defining Home Directory database entries using only alphanumeric characters and the two supported wild cards ('*' and '.') it can sometimes be very difficult to encode the patterns you need. This often results in the use of an excessive number of home directory database entries to achieve something that should have been relatively simple. Home Directory solves this problem by giving you the enormous flexibility of using regular expressions when specifying the domain name and username of a database entry. Table 21 on page 156 shows examples of how regular expressions can be used in the Home Directory database to simplify Home Directory management.

Table 21. Examples of regular expression use in the Home Directory database

Domain Name	Username	Matches	Does not match
[ENGINEERING|FINANCE]	.*	All users in the domains ENGINEERING and FINANCE	Users in any other domain
.*	[wdc|moc].*	All users in all domains whose names are prefixed with the contractor designations 'wdc' (Widget Development Corp) or 'moc' (Manufacturing Operations Consultants)	Users whose names are not prefixed with one of the two designations
.*	.* [2] [0-9] {3}.*	All users in all domains that have four sequential numeric characters in the username where the first digit is 2; for example, joe2006	Users whose names do not have the required sequence of digits

Regular expressions should be used to simplify your Home Directory management. However, care must be taken to consider whether a given regular expression may unintentionally match users other than those you designed it for.

Note: EMC recommends using the VNX Management MMC plug-in to create and edit usernames and directories when you are using regular expressions. The MMC plug-in validates the regular expressions as you type them. If you create or edit the .homedir file and type incorrect regular expressions, the home directory environment might become unusable.

The VNX Management MMC plug-in online help provides additional information about the implementation of regular expressions on VNX.

Parsing order

The Data Mover parses the database from top to bottom. If you use wildcards, there might be multiple matches for a domain:user pair. When the Data Mover finds a match for a domain:user pair, it then searches the path for the user's directory. If there is a user directory under the path, that directory is mapped as the home directory of the user. If there is no matching directory, the Data Mover continues parsing the database looking for the user's home directory.

For example, you have a database that contains the following wildcard entries:

galaxy:*:/homes1/

galaxy:*:/homes2/

galaxy:*:/homes3/

You are trying to map a HOME directory for user1 and you have the following directory structures:

/homes1/user1 – does not exist

/homes2/user1 – does exist

/homes3/user1 – does not exist

If the Data Mover looked only for a galaxy:user1 match, it would stop parsing at the first map entry. However, the Data Mover, after finding a galaxy:user1 match, searches the path for a user1 directory—if it does not find a user1 directory, the Data Mover continues parsing the database. In the example above, the Data Mover would find the match under the second entry, and then map that directory as the home directory for user1.

Guest accounts

For occasional or guest users, you can specify a guest directory in the database. Users who log in from domains not listed in the database are directed to the guest directory. A guest directory entry contains wildcards for the domain and the username as shown in the following example:

```
*:*:/mnt3/guest
```

VNX supports a set of Microsoft Management Console (MMC) snap-ins and programs for managing VNX users and Data Mover security settings from a Windows Server or Windows XP computer.

EMC recommends you to use Microsoft Services for UNIX (SFU) or Identity Management for UNIX (IMU):

Data Mover Management snap-in

The Data Mover management comprises several MMC snap-ins. You can use these snap-ins to manage virus-checking, home directories, and security settings on Data Movers from a Windows Server or Windows XP computer.

AntiVirus Management

You can use the AntiVirus Management snap-in to manage the virus-checking parameters (viruschecker.conf file) used with Common AntiVirus Agent (CAVA) and third-party antivirus programs. CAVA and a third-party antivirus program must be installed on the Windows Server. *Using VNX Event Enabler* provides more details about CAVA.

Home Directory Management snap-in

You can use the home directory management snap-in to associate a username with a directory that then acts as the home directory of the user. The home directory feature simplifies the administration of personal shares and the process of connecting to them.

Data Mover Security Settings snap-in

The Data Mover Security Settings comprises the Audit Policy node and the User Rights Assignment node.

Audit Policy

You can use the Audit Policy node to determine which Data Mover security events are logged in the Security log. You can then view the Security log by using the Windows Event Viewer. You can log successful attempts, failed attempts, both, or neither. The audit policies that appear in the Audit Policy node are a subset of the policies available as GPOs in active directory users and computers (ADUC). Audit policies are local policies and apply to the selected Data Mover. You cannot use the Audit Policy node to manage GPO audit policies.

User Rights Assignment

You can use the User Rights Assignment node to manage which users and groups have login and task privileges to a Data Mover. The user rights assignments that appear in the User Rights Assignment node are a subset of the user rights assignments available as group policy objects (GPOs) in active directory users and computers (ADUC). User rights assignments are local policies and apply to the selected Data Mover. You cannot use the User Rights Assignment node to manage GPO policies.

The online help for a snap-in or program provides more information.

A

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

Active Directory (AD)
Advanced directory service included with Windows operating systems. It stores information about objects on a network and makes this information available to users and network administrators through a protocol such as Lightweight Directory Access Protocol (LDAP).

Active Directory Users and Computers (ADUC)
Administrative tool designed to perform day-to-day Active Directory administration tasks. These tasks include creating, deleting, modifying, moving, and setting permissions on objects stored in the directory. These objects include organizational units, users, contacts, groups, computers, printers, and shared file objects.

Alternate data stream (ADS)
Alternate data stream allows files to be associated with more than one data stream. For example, a file such as text.txt can have an ADS with the name of text.txt:secret (of form filename:streamname) that can only be accessed by knowing the ADS name or by specialized directory browsing programs.

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

C

CIFS server
Logical server that uses the CIFS protocol to transfer files. A Data Mover can host many instances of a CIFS server. Each instance is referred to as a CIFS server.

CIFS service
CIFS server process that is running on the Data Mover and presents shares on a network as well as on Microsoft Windows-based computers.

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

D

Data Mover
In VNX for file, a cabinet component that is running its own operating system that retrieves data from a storage device and makes it available to a network client. This is also referred to as a blade.

default CIFS server
CIFS server created when you add a CIFS server and do not specify any interfaces (with the interfaces= option of the server_cifs -add command). The default CIFS server uses all interfaces not assigned to other CIFS servers on the Data Mover.

domain
Logical grouping of Microsoft Windows Servers and other computers that share common security and user account information. All resources such as computers and users are domain members and have an account in the domain that uniquely identifies them. The domain administrator creates one user account for each user in the domain, and the users log in to the domain once. Users do not log in to each individual server.

Domain Name System (DNS)
Name resolution software that allows users to locate computers on a UNIX network or TCP/IP network by domain name. The DNS server maintains a database of domain names, hostnames, and their corresponding IP addresses, and services provided by the application servers.

See also *ntxmap*.

F

File Allocation Table (FAT)
File system used by MS-DOS and other Windows-based operating systems to organize and manage files. The file allocation table (FAT) is a data structure that Windows creates when you format a volume by using the FAT or FAT32 file systems. Windows stores information about each file in the FAT so that it can retrieve the file later.

file system
Method of cataloging and managing the files and directories on a system.

G

Group Policy Objects (GPO)
In Windows operating systems, administrators can use Group Policy to define configuration options for groups of users and computers. Windows Group Policy Objects can control elements such as local, domain, and network security settings.

L

Lightweight Directory Access Protocol (LDAP)

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.

N

NetBIOS name

Name recognized by WINS, which maps the name to an IP address.

network basic input/output system (NetBIOS)

Network programming interface and protocol developed for IBM personal computers.

network file system (NFS)

Network file system (NFS) is a network file system protocol that allows a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks.

NTFS

NTFS is the standard file system of Windows NT, including its later versions. NTFS supersedes the FAT file system as the preferred file system for Microsoft Windows. NTFS has several improvements over FAT such as improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization, plus additional extensions such as security access control lists (ACLs) and file system journaling.

S

Security Access Manager or Security Accounts Manager (SAM)

Microsoft Windows service that authenticates users to use resources on the network. The SAM database is the location for all security and user account information for a Windows NT domain.

Server Message Block (SMB)

Underlying protocol used by the CIFS protocol enhanced for use on the Internet to request file, print, and communication services from a server over the network. The CIFS protocol uses SMB to provide secure file access and transfer to many types of hosts such as LANs, intranets, and the Internet.

share name

Name given to a file system, or resource on a file system available from a particular CIFS server to CIFS users. There may be multiple shares with the same name, shared from different CIFS servers.

V

Virtual Data Mover (VDM)

VNX for file software feature that enables users to administratively separate CIFS servers, replicate CIFS environments, and move CIFS servers from one Data Mover to another.

W

Windows domain
Microsoft Windows domain controlled and managed by a Microsoft Windows Server by using the Active Directory to manage all system resources and by using the DNS for name resolution.

Windows Internet Naming Service (WINS)
Software service that dynamically maps IP addresses to computer names (NetBIOS names). This allows users to access resources by name instead of requiring them to use IP addresses that are difficult to recognize and remember. WINS servers support clients by running Windows NT 4.0 and earlier versions of Microsoft operating systems.

Windows NT domain
Microsoft Windows domain controlled and managed by a Microsoft Windows NT server by using a SAM database to manage user and group accounts and a NetBIOS namespace. In a Windows NT domain, there is one primary domain controller (PDC) with a read/write copy of the SAM, and possibly several backup domain controllers (BDCs) with read-only copies of the SAM.

See also *domain* and *domain controller*.