EMC® VNX® Series

Release 8.1

Configuring VNX® User Mapping

P/N 300-015-120 Rev 01

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

Published March 2013

Corporate Headquarters: Hopkinton, MA 01748-9103

Contents

Preface

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

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

Special notice conventions

EMC uses the following conventions for special notices:

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

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

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

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

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

Where to get help

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

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

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

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

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

Your comments

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

Please send your opinion of this document to:

techpubcomments@EMC.com

1 Introduction

Every user of the EMC VNX, either a Microsoft Windows user or a UNIX/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, Common Internet File System (CIFS), on the VNX, you must select a method of mapping Windows SIDs to UIDs and GIDs. The method you use depends on whether you have a Windows-only or UNIX/Linux and Windows (multiprotocol) environment. These methods include:

- Usermapper
- LDAP-based directory services (including Active Directory that uses Microsoft Windows Services for UNIX [SFU] or Identity Management for UNIX [IdMU])
- Local files
- Network Information Service (NIS)
- Active Directory (by using CIFS Microsoft Management Console [MMC] snap-ins)
- ntxmap

Chapter 2 provides more information.

This document is part of the VNX documentation set and is intended for use by system administrators responsible for configuring and managing Windows user ID mapping.

Topics included are:

System requirements

Table 1 on page 10 describes the EMC® VNX® series software, hardware, network, and storage configurations required for using user mapping as described in this document.

Table 1. System requirements

Software	VNX version 8.1
Hardware	No specific hardware requirements.
Network	Windows Server or Windows NT domain. You must configure the domains with the following: ◆ Windows Server domains: ◆ Active Directory ◆ Kerberos or NT Lan Manager (NTLMSSP) ◆ DNS ◆ NTP ◆ Windows NT domains: ◆ NT Lan Manager (NTLM) ◆ WINS
Storage	Verify that sufficient space is available in the root file system. Contact your EMC Customer Support Representative for assistance with determining size requirements.

User interface choices

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

- EMC Unisphere™ software
- Microsoft Management Console (MMC) snap-ins
- Active Directory Users and Computers (ADUC) extensions

The Unisphere online help provides additional information about managing VNX.

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

The VNX release notes contain additional, late-breaking information about VNX management applications.

Using Unisphere

Unisphere can be used to configure a Data Mover to use Usermapper and NIS, as described in Table 2 on page 11. You cannot use Unisphere to configure the Identity Management for UNIX feature, or to manage the Active Directory and local files.

Table 2. User mapping configured by using Unisphere

Naming service	Unisphere procedure
NIS	To configure the Data Mover as an NIS client, select **System** ➤ **Network** and click **Interfaces**.
Usermapper	To configure Usermapper, select **Sharing** ➤ **CIFS** and click **Usermappers**.

Unisphere online help provides more information on using Unisphere to configure user mapping.

Note: You can also use the configuration wizards to set up the use of NIS or basic Usermapper.

Related information

For specific information related to the features and functionality described in this document:

- *VNX Command Line Interface Reference for File*
- *Celerra Network Server Error Messages Guide*
- *Parameters Guide for VNX*
- *Configuring Events and Notifications on VNX for File*
- *Configuring VNX Naming Services*
- *Configuring and Managing CIFS on VNX*
- *Installing Management Applications on VNX*
- *Managing a Multiprotocol Environment on VNX*
- VNX for File man pages
- *Using NTMigrate with VNX*
- *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.

2 Concepts

The concepts to understand user mapping are:

Overview

Every VNX user must be assigned a unique numeric UID and GID to indicate the ownership of directories and files. The VNX uses directory and file ownership to apply and enforce access permissions and quota limits.

Note: For connections from Windows users, file access checking is performed by using SIDs only. This is done to prevent errors due to UID mismatches and to reduce dependency on the Usermapper database.

Like the VNX, UNIX/Linux systems use UIDs and GIDs to identify users and groups. Consequently, the VNX can use the UIDs and GIDs supplied by UNIX/Linux clients without requiring any additional mappings. 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 (referred to as CIFS) on the VNX, you must select a method of mapping Windows SIDs to UIDs and GIDs. You select a mapping method based on whether you have a Windows-only or UNIX/Linux and Windows (multiprotocol) environment.

Figure 1 on page 15 identifies the factors that determine the user mapping technique best suited for the environment.

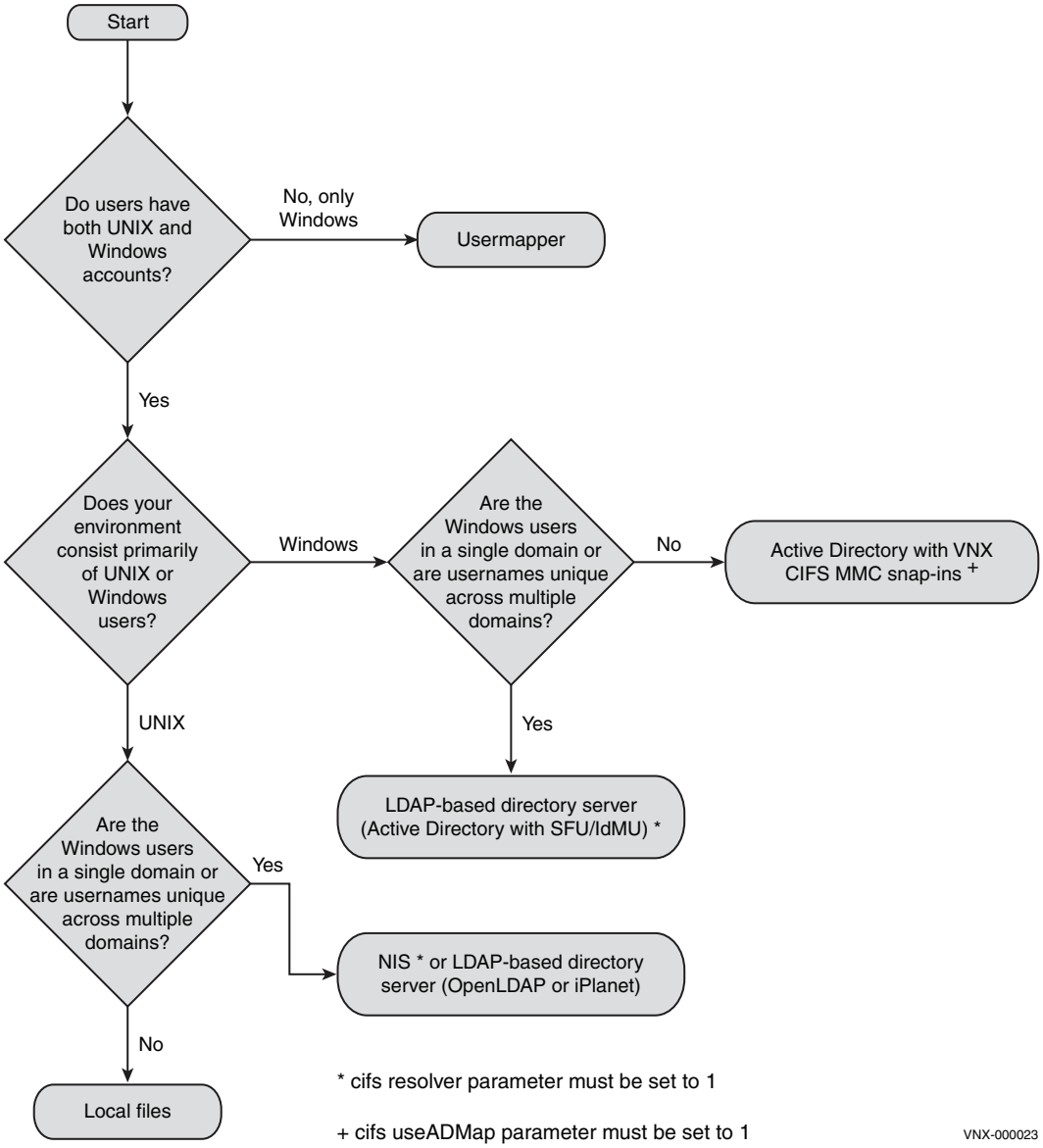

Figure 1. Flowchart of user mapping techniques

User mapping in Windows-only environments

The VNX Usermapper feature automatically assigns UIDs and GIDs to Windows users and groups. Usermapper is part of the Data Mover's software. It does not require separate installation and, in the case of a new VNX, requires no additional configuration procedures.

EMC recommends that you use Usermapper in Windows-only environments.

Note: Before you configure and run Usermapper, include only one primary Usermapper in a VNX environment.

User mapping in multiprotocol environments

In multiprotocol environments, file systems can be accessed by UNIX/Linux and Windows users. File access is determined by the permissions on the file or directory, specifically by one or both of the following:

- UNIX/Linux permissions
- Windows access control lists (ACLs)

Therefore, if a user has UNIX/Linux and Windows user accounts, you should choose a mapping method that allows you to indicate that the two accounts represent the same user. The mapping methods that enable you to control the mappings used, and ensure that specific Windows SIDs are mapped to the corresponding UIDs or GIDs and that the opposite is also true, include:

- LDAP-based directory services, such as the Active Directory (that uses Microsoft Windows Services for UNIX [SFU] or Identity Management for UNIX [IdMU])
- A Data Mover's local user and group files
- Network Information Service (NIS)
- Active Directory (by using VNX CIFS Microsoft Management Console [MMC] snap-ins)

Note: If a user in a multiprotocol environment uses only a single login (either through Windows or UNIX/Linux), then you can use Usermapper. If a user has only one account, mapping to an equivalent identity in the other environment is not necessary.

Secure mapping

Secure mapping (secmap) is a cache that contains all mappings between SIDs, and UID or GIDs used by a Data Mover or Virtual Data Mover (VDM). Secmap only caches mappings that are generated by mapping mechanisms used by VNX; secmap does not generate mappings. Normally, mappings are persistent and are never updated.

The secmap database stores two kinds of information:

- SID to UID or GID mappings
- UID or GID to SID reverse mappings

The Data Mover permanently caches all mappings it receives from any source (Usermapper, LDAP-based directory services, local files, NIS, and Active Directory) in the secmap database, making the response to subsequent mapping requests faster and less susceptible to network problems. Reverse mapping provides better quota support.

Note: Secmap caching is enabled by default and does not require any special setup. EMC recommends that you use secmap, although it can be disabled if necessary.

Chapter 6 describes the tasks to manage secmap.

Creating secmap mapping entries

To add a new mapping for a user or group to the secmap database, VNX first checks whether there is enough space to insert a new entry. VNX can only store mappings if there is more than 5 percent of inodes and blocks available on the secmap file system. This check is made only at the beginning of the operation. If the threshold is reached during the operation, VNX continues. An error is returned only if something abnormal occurs. If that occurs, VNX determines in which domain table the mapping should be put. Before adding the SID mapping, VNX first adds the corresponding reverse mapping in the required table. Then VNX adds the main mapping to the corresponding domain table. If a reverse mapping already exists for the SID, VNX appends a new SID to it.

If there is not enough space to store the new mapping or if a new domain table is needed and cannot be created, VNX returns an error. If for any reason the main mapping cannot be added, VNX rolls back the reverse mapping modifications made previously. Create secmap mapping entries on page 48 describes this task. Report secmap status on page 52 describes how to display the current secmap status, including database state, domains handled by secmap, and resource usage (number of inodes and blocks used).

Checking and updating secmap mapping entries

To check or update a mapping, VNX first looks for an existing mapping. It then resolves the mapping again by getting the SID name from the domain controller and creating the mapping through the available user mapping mechanisms. Finally, VNX compares what it gets by re-creating the mapping with what had been stored. If the values are different, VNX replaces the existing value with the new value.

An error is returned if the mapping:

- Does not exist in the secmap database
- Could not be resolved
- Could not be changed

Note: After an update is performed, an update of the ACLs of all file systems should be forced to take account of the new mappings.

Check secmap mapping entries on page 49 and Update secmap mapping entries on page 50 describe these tasks.

User mapping and ntxmap

In a multiprotocol VNX environment, when a Windows user wants to access a UNIX resource, or a UNIX user wants to access a Windows resource, the username must be mapped in the same way in each environment; otherwise, the mapping cannot occur and the user is denied access to the resource.

However, you might want to map Windows and UNIX users who are identified differently in each environment. The ntxmap feature allows you to define explicit mappings between such Windows and UNIX usernames.

Using ntxmap for CIFS User Mapping on VNX provides more information

User mapping database

Earlier versions of the VNX relied on a basic database, nameDB, to maintain Usermapper and secmap mapping information. In version 5.6, DBMS replaces the basic database. This solves the inode consumption issue and provides better consistency and recoverability with the support of database transactions. It also provides better atomicity, isolation, and durability in database management.

User mapping process

When a user logs in to a Windows domain and requests access to a Data Mover's resources:

1. When logging into a Windows NT domain, or when accessing a Data Mover that was declared as a pre-Windows 2000 computer, the user is authenticated by using NT LAN Manager (NTLM). If the Data Mover is using a computer name and is joined to a Windows Server domain, the user is authenticated through Kerberos or NT LAN Manager secure-socket provider (NTLMSSP).
2. The user's identification is forwarded to the Data Mover.
3. The Data Mover follows the default search order and searches these sources for an existing mapping of the user's SID to a UID or GID:

Note: If an nsswitch.conf file has been created on the Data Mover, the order in which the UNIX or Linux-based sources (local files, NIS, and LDAP-based directory servers) are queried is determined by that file. *Configuring VNX Naming Services* provides information on using the nsswitch.conf file.

---

   a. The Data Mover first checks its secmap database for an existing SID to UID or GID mapping.
   b. If no mapping is found, the Windows domain controller is queried for the user or group name associated with the SID, and then the Data Mover checks its local passwd and group files for a UID or GID to associate with the name.
   c. If no mapping is found, and NIS is configured, the Data Mover queries NIS for a UID or GID to associate with the name.
   d. If no mapping is found, and LDAP-based directory services are configured (including Active Directory with SFU or IdMU), the Data Mover queries the LDAP-based directory services for a UID or GID to associate with the name.
   e. If no mapping is found, and queries to the Active Directory (by using VNX CIFS MMC snap-ins) are configured, the Data Mover queries the Active Directory for an SID to UID or GID mapping.
   f. If no mapping is found, the Data Mover queries Usermapper for an SID to UID or GID mapping.
   g. The primary Usermapper service checks its database to determine if this user or group has already been assigned a UID or GID. If not, the primary Usermapper generates a new UID or GID and adds the new user or group and the mapping to its database. It then returns the mapping to the Data Mover.
   h. The Data Mover permanently caches all mappings it receives from any source (Usermapper, LDAP-based directory services including Active Directory with SFU or IdMU, local files, NIS, and Active Directory by using MMC snap-ins) in the secmap database, making the response to subsequent SID to UID or GID mapping requests faster and less susceptible to network problems.
   i. The user is then authenticated and given access to the CIFS share (network drive).

j. If a user ID mapping cannot be resolved through one of these methods, an error is logged in the server log and the user is unable to access the CIFS share (network drive).

Usermapper

Usermapper is a VNX service that automatically generates and maintains a database that maps SIDs to UIDs and GIDs for users or groups accessing file systems from a Windows domain. Usermapper performs these functions:

- One instance of the Usermapper service serves as the primary Usermapper, meaning that it assigns UIDs and GIDs to Windows users and groups. By default, this instance is configured on the Data Mover in slot 2 (server_2).
- The other Data Movers in a single VNX environment are configured as clients of the primary Usermapper service, meaning that they send mapping requests to the primary service when they do not find a mapping for a user or group in their local cache. By default, all the client Data Movers automatically relay a broadcast over the VNX system's internal interfaces to discover the location of the primary Usermapper service. Using the default single-VNX Usermapper configuration on page 22 provides information on Usermapper services in a single VNX environment.
- In a multi-VNX environment, only a single primary Usermapper service is configured on one of the VNX platforms, and all the Data Movers on that platform will use the primary Usermapper service. Each additional VNX platform will have its own secondary Usermapper service, and all their respective Data Movers would point to its secondary Usermapper. Like a primary Usermapper service, a secondary Usermapper service checks its database to determine if a user or group has already been assigned a UID or GID. If not, it forwards the mapping request to the primary Usermapper service. The primary Usermapper service checks its database and, if necessary, generates a new UID or GID, and returns the mapping to the secondary Usermapper service.

The secondary Usermapper service then adds the new user or group and the mapping to its database, and returns the mapping to the Data Mover. If the secondary Usermapper service is unavailable, new users cannot access files. Existing users can access files only if a user has used the Data Mover before and the Data Mover's local cache contains the previous mapping.

Configure a multi-VNX Usermapper environment on page 28 provides information on configuring Usermapper services in an environment with more than one VNX sharing the same domain space.

Restrictions

Before you configure and run Usermapper, note these restrictions:

- Designate only one primary Usermapper service in a given VNX environment, and only on one of the VNX platforms, in case of a multi-VNX environment. Otherwise, the same

user can be assigned different mappings. Additional VNX platforms should run a secondary Usermapper service and point to the primary Usermapper service to obtain their mappings. A primary Usermapper service and a secondary Usermapper service should not be run on the same VNX cabinet.

- In a single VNX, ensure that there is only one instance of the Usermapper service, either primary or secondary. All the other Data Movers in that VNX are clients of the primary or secondary service.
- In a multi-VNX environment, ensure that the primary Usermapper service is enabled before you configure any secondary Usermapper services.
- By default, Usermapper runs on the Data Mover in slot 2 (server_2). This is the preferred location from which to run the primary or secondary Usermapper service.
- You cannot configure a primary or secondary Usermapper service on a Virtual Data Mover (VDM).

Planning considerations

Before you begin using Usermapper, consider these situations:

- Usermapper stops mapping new UIDs and GIDs when the root file system of the Data Mover on which the Usermapper database is stored becomes full. In this situation, new users will not be allowed access to system objects. The size of the root file system that is required is based on the number of users in the Windows environment. Contact your EMC Customer Support Representative for assistance with determining size requirements.
- If you are replicating a Windows environment that uses Usermapper or if you are using the EMC Symmetrix® Remote Data Facility (SRDF®), special Usermapper restrictions might apply. Contact your EMC Customer Support Representative for more information.
- In Usermapper, the UID and GID ranges are fixed in the Usermapper database, and Usermapper automatically assigns new UIDs and GIDs based on the next available value. Therefore, it does not need to use a Usermapper configuration file to define UID and GID ranges. However, it is possible to import an existing usrmap.cfg and use this file to define UID and GID ranges. This is referred to as the manual mapping method. After the ranges defined in the usrmap.cfg file are enabled, Usermapper's automatic mapping method maintains this information and prevents duplicate mappings.

  Note: If there is no special reason to use particular UID and GID ranges for the environment's domains, EMC encourages you to use the automatic mapping method and let Usermapper automatically assign new UIDs and GIDs based on the next available values. If a future revision to the usrmap.cfg file cannot be avoided, contact your EMC Customer Support Representative for assistance.

- Usermapper supports the SID History functionality introduced in Windows 2000. This aids the migration of users from Windows NT domains to Windows 2000 native mode domains. To use the SID History, it must be enabled in Windows 2000 and on the VNX system. Windows 2000 documentation provides the correct procedure for enabling SID

History on the Windows 2000 systems. With SID History enabled, when you migrate users from a Windows NT domain or a Windows 2000 domain in mixed mode to a Windows 2000 domain in native mode, the Security Access Token contains the SID History from the Windows NT domain and a new SID from the Windows 2000 domain. Usermapper automatically assigns UID and GID mappings, including SID History, by default.

Using the default single-VNX Usermapper configuration

Note: When a new system running software version 5.3 or later is started for the first time, it is automatically configured with the default single VNX Usermapper configuration. In this situation, Usermapper is automatically enabled as a VNX for file service and no additional installation or configuration procedures are required.

The default Usermapper configuration consists of a single VNX in which the Data Mover in slot 2 (server_2) is configured with the primary Usermapper service. Each of the remaining Data Movers in the VNX system cache all the SID to UID or GID mappings it has used. However, if one of these Data Movers is accessed by a user for whom it does not have a mapping, it queries the primary Usermapper service. These Data Movers are clients of the primary Usermapper service. By default, all the Data Movers in the VNX system automatically relay a broadcast over the VNX internal interfaces to discover the location of the primary Usermapper service.

Certain UID and GID values are reserved and cannot be mapped to SIDs. For example, 0 is reserved for the UNIX root account. Additional numbers are reserved for maintenance. UID and GID values can start at 32 KB. The maximum possible value for UIDs and GIDs is imposed by the underlying file system. All domain users and groups accessing this file system are assigned UIDs and GIDs based on these definitions.

Note: As in a standard VNX configuration, you can configure another Data Mover to serve as a failover Data Mover, providing a backup for the primary Usermapper service.

Display Usermapper status on page 38 describes how to verify the Usermapper configuration and display its current status. In case the primary Usermapper service is not automatically enabled, Chapter 7 provides information that can help resolve the issue. Chapter 5 provides information on managing the Usermapper environment.

Using a multi-VNX Usermapper environment

If you have a VNX environment in which there is more than one VNX that shares the same Windows domain space, the default Usermapper configuration is not suitable. In this situation, you must modify the default Usermapper configuration on all the additional VNX systems to use one primary Usermapper service. In this situation, use a configuration in which the Data Mover located in slot 2 (server_2) of each of the additional VNX servers is configured as a secondary Usermapper service. The remaining Data Movers in each VNX server then

send mapping requests to their local secondary Usermapper service, and each secondary Usermapper service then forwards these requests to the single primary Usermapper service.

The secondary Usermapper service sends mapping requests to the primary Usermapper service one at a time and only when needed. Therefore, all the secondary Usermapper services in an environment might not have the same entries in their databases.

Note: If there is any possibility of file systems ever being replicated, then the VNX servers involved should share a single primary Usermapper service.

Configure a multi-VNX Usermapper environment on page 28 describes this task. Chapter 5 provides information on managing the Usermapper environment.

LDAP-based directory services

If the multiprotocol environment consists primarily of UNIX users and has only one Windows domain, or usernames that are unique across multiple Windows domains, you can use LDAP-based directory services, including Active Directory with SFU or IdMU, to manage user and group mapping.

Note: EMC recommends that you use the Active Directory with SFU or IdMU for user mapping in multiprotocol environments.

Configuring VNX Naming Services provides information on configuring a Data Mover as a client of an LDAP-based directory server.

After you have configured LDAP-based directory services, the Data Mover automatically checks the LDAP-based directory server for a user and group name. By default, it checks for a username in the form username.domain and a group name in the form groupname.domain. If you have added usernames and group names to the LDAP-based directories without a domain association, you can set the cifs resolver parameter so that the Data Mover looks for the names without appending the domain. Retrieve user and group names without a domain association on page 32 provides a description of using the cifs resolver parameter.

Note: User account migration tools on page 26 provides information about migrating user information from one environment to another.

Local files

If the multiprotocol environment consists primarily of UNIX users and has more than one Windows domain, or usernames that are not unique across the Windows domains, you can manually edit the Data Mover's local passwd and group files. Copy local files from the Data Mover on page 33 describes how to manually add Windows users and groups to the passwd and group files on the Data Mover.

By default, the Data Mover checks for a username in the form username.domain and a groupname in the form groupname.domain. If the usernames and group names do not have a domain association, you must add the Windows domain name and verify that the Windows user is assigned the UID and GID of the existing UNIX account.

If you have added usernames and group names to the local files without a domain association, you can set the cifs resolver parameter so the Data Mover looks for the names without appending the domain. Retrieve user and group names without a domain association on page 32 provides a description of using the cifs resolver parameter.

Note: User account migration tools on page 26 provides information about migrating user information from one environment to another.

NIS

If the multiprotocol environment consists primarily of UNIX users and has only one Windows domain, or usernames that are unique across multiple Windows domains, you can use NIS to manage user and group mapping.

Configuring VNX Naming Services provides information on configuring a Data Mover to access a NIS server. NIS server documentation provides information about manually updating the NIS passwd and group maps.

Note: All of the entries (Windows names, usernames, domain names, and global group names) in the passwd and group maps must be typed in lowercase ASCII only.

After you have configured NIS, the Data Mover automatically checks NIS for a user and group name. By default, it checks for a username in the form username.domain and a group name in the form groupname.domain. If you have added usernames and group names to NIS without a domain association (which reflects the use of NIS files without any modifications), you can set the cifs resolver parameter so the Data Mover looks for the names without appending the domain. Retrieve user and group names without a domain association on page 32 provides a description of using the cifs resolver parameter.

Note: User account migration tools on page 26 provides information about migrating user information from one environment to another.

Active Directory

Before the introduction of Microsoft software that provides a UNIX environment on Windows (Active Directory with SFU or IdMU), Active Directory was primarily used in Windows Server environments to provide authentication and authorization for Windows users.

Note: EMC recommends that you use Active Directory with SFU or IdMU instead of Active Directory with Celerra CIFS MMC snap-ins. Do not use the ADmap parameter. LDAP-based directory services on page 23 provides more information on using Active Directory with SFU or IdMU.

However, if the Active Directory schema was extended with an EMC proprietary schema to include UNIX attributes for Windows users and groups, you could configure a Data Mover to query the Active Directory to determine if a user and the group of which the user is a member have UNIX attributes assigned. If so, information stored in these attributes could be used for file access authorization.

To configure a Data Mover to query the Active Directory for UNIX attributes, you must install the UNIX user management component of the Celerra CIFS management MMC snap-ins. You must also set the cifs useADMap parameter. Configure a Data Mover to query the Active Directory on page 36 describes this task.

Installing Management Applications on VNX for File and the Celerra UNIX User Management and Celerra UNIX Attribute Migration online help systems provide more information. User account migration tools on page 26 provides information about migrating user information from one environment to another.

UNIX user management snap-in

UNIX User Management is an MMC snap-in to the VNX Management view that you can use to assign, remove, or modify the UNIX UID or GIDs for a single Windows user or group on the local domain and on remote domains.

You also use this snap-in to select the location of the attribute database. This location can either be in a local or a remote domain. You would choose to store the attribute database in the Active Directory of a local domain when:

- You have only one domain.
- Trusts are not allowed.
- You do not need to centralize the UNIX user management information.

You would choose a remote domain when:

- You have multiple domains.
- Bidirectional trusts between domains that need to access the attribute database already exist.
- You want to centralize the UNIX user management information.

VNX UNIX users and groups property page extension

VNX UNIX Users and Groups property pages are extensions to Active Directory Users and Computers view. You can use these property pages to assign, remove, or modify UNIX UIDs or GIDs for a single Windows user or group on the local domain.

Note: You cannot use this extension to manage users or groups on a remote domain.

User account migration tools

If you currently have a single protocol environment (either pure CIFS or pure NFS), and you want to convert to a multiprotocol environment (supporting Windows and UNIX clients), you can use these tools to migrate the user accounts from one environment to the other:

- VNX UNIX Attributes Migration Tool
- NTMigrate

VNX UNIX Attributes Migration tool

VNX UNIX Attributes Migration is a tool that enables you to migrate existing UNIX users from the VNX (local files) or NIS to the Active Directory. You can select the UNIX attributes (UIDs and GIDs) to add to the Active Directory. However, you cannot add new users or groups, nor can you modify existing UNIX UIDs or GIDs. To add new users or groups, or to modify existing UNIX attributes, see Active Directory on page 24 for information on using the Active Directory for user mapping.

Note: Using this tool extends the Active Directory schema. After the schema is extended, you cannot revert to the original Active Directory schema.

Installing Management Applications on VNX provides more information on installing this tool. The VNX UNIX Attributes Migration Tool online help provides more information on using this tool.

NTMigrate

NTMigrate is a tool that migrates Windows users to an existing UNIX UID or GID database (local passwd file or NIS). NTMigrate collects user information from the Windows domain and merges it with UNIX passwd and group files.

NTMigrate is best suited for mapping large Windows domains into UNIX UIDs and GIDs. *Using NTMigrate with VNX* provides more information.

3

Configuring in Windows Environments

EMC recommends that you use Usermapper in Windows-only environments. User mapping in Windows-only environments on page 16 provides general information.

A new VNX is automatically configured with the default single VNX Usermapper configuration. Using the default single-VNX Usermapper configuration on page 22 provides general information on single-VNX Usermapper environments.

If you have a VNX environment in which there is more than one VNX that shares the same Windows domain space, you must modify the default Usermapper configuration on all the additional VNX systems to use one primary Usermapper service. Configure a multi-VNX Usermapper environment on page 28 describes this task.

The task to configure user mapping in Windows-only environments is:

- Configure a multi-VNX Usermapper environment on page 28

Configure a multi-VNX Usermapper environment

To configure a multi-VNX Usermapper environment:

1. Verify the status of the primary Usermapper service on page 28
2. Disable the primary Usermapper service on page 29
3. Configure the secondary Usermapper service on page 29
4. Verify the status of the secondary Usermapper service on page 30

Using a multi-VNX Usermapper environment on page 22 provides general information on multi-VNX Usermapper environments.

Note: In this procedure, the VNX that supports the primary Usermapper service is referred to as VNX_A and the VNX that runs the secondary Usermapper service is referred to as VNX_B.

Verify the status of the primary Usermapper service

On VNX_A, verify that the primary Usermapper service is enabled on server_2, which is the default configuration.

Action
To verify that the primary Usermapper service is enabled, use this command syntax: $ **server_usermapper** *<movername>* where: *<movername>* = name of the Data Mover Example: To verify that the primary Usermapper service is enabled on server_2 of VNX_A, type: **$ server_usermapper server_2**
Output
server_2 : Usrmapper service: Enabled Service Class: Primary

Disable the primary Usermapper service

The default Usermapper configuration always designates the Data Mover in slot 2 (server_2) as supporting the primary Usermapper service. You must explicitly configure a Data Mover on VNX_B to support a secondary Usermapper service. On VNX_B, disable the primary Usermapper service that is enabled by default.

No user mapping requests should be sent to the primary Usermapper service on VNX_B before you have reconfigured it. Consequently, you should not configure CIFS on the VNX_B Data Movers until the Usermapper service is reconfigured as a secondary service.

Action
To disable the primary Usermapper service, use this command syntax: `$ server_usermapper <movername> -disable` where: `<movername>`= name of the Data Mover Example: To disable the primary Usermapper service on server_2 of VNX_B, type: `$ server_usermapper server_2 -disable`
Output
`server_2 : done`

Configure the secondary Usermapper service

After you have disabled the primary Usermapper service on VNX_B, you can configure server_2 to run as a secondary Usermapper service.

When you enable a secondary Usermapper service, you also indicate the location of the primary Usermapper service to which the secondary service will send mapping requests. To do this, specify the IP address of the Data Mover on which the primary service is located.

Note: The primary Usermapper service must be enabled before you configure a secondary service.

Action
To enable a secondary Usermapper service, use this command syntax: `$ server_usermapper <movername> -enable primary=<ip addr>` where: `<movername>` = name of the Data Mover

Action
<ip addr> = network IP address of the Data Mover on which the primary Usermapper service is running Example: To enable a secondary Usermapper service on server_2 of VNX_B, type: **$ server_usermapper server_2 -enable primary=192.168.21.1**
Output
server_2 : done

Verify the status of the secondary Usermapper service

Verify that the secondary Usermapper service has been enabled on server_2 of VNX_B.

Action
To verify that the secondary Usermapper service is enabled, use this command syntax: $ **server_usermapper** *<movername>* where: *movername* = name of the Data Mover Example: To verify that the secondary Usermapper service is enabled on server_2 of VNX_B, type: **$ server_usermapper server_2**
Output
server_2 : Usrmapper service: Enabled Service Class: Secondary Primary = 192.168.21.1(c)

4 Configuring in Multiprotocol Environments

In multiprotocol environments, file systems can be accessed by UNIX/Linux and Windows users. If a user has both UNIX/Linux and Windows user accounts, you should choose a mapping method that allows you to indicate that the two accounts represent the same user. User mapping in multiprotocol environments on page 16 provides conceptual information:

The tasks to configure user mapping in a multiprotocol environment are:

Retrieve user and group names without a domain association

By default, VNX checks for a username in the form username.domain and a group name in the form groupname.domain. If you have added usernames and group names without a domain association to local files, NIS, or Active Directory (that uses Microsoft Windows Services for UNIX [SFU] or Identity Management for UNIX [IdMU]), you can set the cifs resolver parameter so the Data Mover looks for names without appending the domain extension.

Note: Active Directory with SFU or IdMU requires that cifs resolver be set so that user and group names are retrieved with a domain extension.

Action
To change the default format of username and group name so that they can be retrieved without a domain extension, use this command syntax: `$ server_param <movername> -facility cifs -modify resolver -value 1` where: *<movername>* = name of the Data Mover Example: To change the default format of username and group name so they can be retrieved without a domain extension, type: `$ server_param server_2 -facility cifs -modify resolver -value 1`
Output
`server_2 : done`

Configure a Data Mover to query local files

Before you begin

When editing the passwd and group files:

- All the entries (Windows names, usernames, domain names, and global group names) in the passwd and group files must be typed in lowercase ASCII only.
- Any spaces in Windows domain or group names should be replaced with =20 so that they become legal in a UNIX-style passwd or group file.
- If UNIX user authentication is used, run the server_user command to generate an encrypted password in the password field, but do not include the domain as part of the username.

Note: *Configuring VNX Naming Services* provides additional information on using local files for naming services.

Procedure

To manually add Windows users and groups to the passwd and group files on the Data Mover:

1. Copy local files from the Data Mover on page 33
2. Add the Windows domain name as a group name on page 34
3. Add Windows usernames on page 35
4. Copy edited local files to the Data Mover on page 36

Local files on page 23 provides conceptual information.

Copy local files from the Data Mover

Before editing the local files, you must copy them from the Data Mover.

Copy the passwd and group files from the Data Mover to the Control Station for editing. If the local files do not exist, create them with an ASCII editor such as vi or Emacs.

CAUTION This command overwrites existing files of the same name without notification. Be careful when copying files.

Action
To copy the passwd or group file, use this command syntax for each file: `$ server_file <movername> -get <src_file> <dst_file>` where: *<movername>* = name of the Data Mover *<src_file>* = name of the source file *<dst_file>* = name of the destination file Example: To copy the passwd file to /home/nasadmin/passwd, type: `$ server_file server_2 -get passwd /home/nasadmin/passwd`
Output
`server_2 : done`

Add the Windows domain name as a group name

Use this procedure to add the Windows domain name to the copy of the UNIX group file on the Data Mover.

Use the UNIX text editors vi, Emacs, or Windows Notepad to manually modify the configuration file.

Action
Using a text editor, add the Windows domain name as a group name in the group file. Assign a GID for the newly created group name. The group file entries are in the following format: *<groupname.domain>*:*:*<GID>*: where: *<groupname.domain>* = group name and Windows domain name ***** = UNIX password for the group; this field should contain an asterisk (*) because the password is not used on the VNX. *<GID>* = unique numeric group ID that you assign to the group name Example 1: To add the Windows domain galaxy to the group file, add the following line: **galaxy:*:100** The Windows domain galaxy is the group name. The GID is 100. Example 2: Here is an example of a group file, including the galaxy example and the default Windows global groups: .(numerous UNIX groups skipped) **galaxy:*:100:** **domain=20admins.galaxy:*:101: domain=20users.galaxy:*:102:** **domain=20guests.galaxy:*:103:**

Add Windows usernames

Use this procedure to add usernames to the copy of the UNIX passwd file on the Data Mover.

Action
Add the Windows usernames from the Windows domain to the passwd file and assign each user a unique UID and the GID specified for the Windows domain in Add the Windows domain name as a group name on page 34. Password file entries are in the following format: *<user.domain>*:*:*<UID>*:*<GID>* :*<name>*:*<path>*:*<shell>* where: *<user.domain>* = Windows username and domain name, which is appended to preclude accidental mapping to existing UNIX or Windows clients of the same name ***** = UNIX password for the user; if the user authentication mode on the Data Mover is set to NT or SHARE, this field should contain an asterisk (*); if the Data Mover uses UNIX user authentication, the field should contain the encrypted password for the user *<UID>* = unique user ID that you assign *<GID>* = GID assigned to the domain *<name>*, *<path>*, and *<shell>* are optional informational fields and are ignored during processing Example: The following is an example of a password file entry of user, glenn, in the domain galaxy. This requires an entry in passwd as: **glenn.galaxy:*:530:100:J.GLENN:/usr/home/jdir:/bin/csh**

Copy edited local files to the Data Mover

Use this procedure to copy the edited local files (passwd or group file) back to the Data Mover.

CAUTION This command overwrites existing files of the same name without notification. Be careful when copying files.

Action
To copy the edited local files back to the Data Mover, use this command for each file: `$ server_file <movername> -put <src_file> <dst_file>` where: *<movername>* = name of the Data Mover *<src_file>* = name of the source file *<dst_file>* = name of the destination file Examples: `$ server_file server_2 -put passwd passwd` `$ server_file server_2 -put group group`
Output
server_2 : done

Configure a Data Mover to query the Active Directory

Active Directory on page 24 provides conceptual information.

1. Install the UNIX user management component of the CIFS Microsoft Management Console (MMC) snap-ins for managing VNX users from a Windows computer. These snap-ins provide a manual mapping method that enables you to assign specific UIDs and GIDs to Windows users. The CIFS MMC snap-ins are not required if you are using SFU/IdMU with the Active Directory.

2. Set the cifs useADMap parameter to 1 to enable the snap-ins to interact with the Data Mover. *Installing Management Applications on VNX for File* describes how to enable the CIFS management snap-ins and tools.

5 Managing Usermapper

The tasks to manage Usermapper are:

- Display Usermapper status on page 38
- Import and export database information on page 40
- Maintain the Usermapper database on page 41
- Back up Usermapper on page 42
- Change Usermapper default configuration settings on page 43

Display Usermapper status

You can display Usermapper status on the VNX by using two commands:

- The server_usermapper command displays the status of Usermapper services running on a Data Mover.
- The server_cifs command displays a Data Mover's CIFS configuration, including the Usermapper service it is using.

Display Usermapper service information

The server_usermapper command displays the status of Usermapper services running on a Data Mover, including:

- Whether Usermapper is configured as a primary or secondary service
- The IP address of the primary Usermapper service used by the secondary service
- The operational status of the service

Action	
To display the status of the Usermapper service, use this command syntax: `$ server_usermapper <movername>` where: *<movername>* = name of the Data Mover Example: To display the status of the Usermapper service on server_2, type: `$ server_usermapper server_2`	
Output	**Note**
`server_2 : Usrmapper service: Enabled Service Class: Secondary Primary = 192.168.21.1(c)`	Usermapper has three operational states: ◆ Uninitialized — When Usermapper is not available on the Data Mover ◆ Initialized — When Usermapper has been created on the Data Mover, but has been disabled for some reason ◆ Enabled — When Usermapper is running You should have only one instance of the Usermapper service, either primary or secondary, in a single VNX server. All the other Data Movers in that environment are clients of the primary or secondary service.

Display the Data Mover's Usermapper service

The server_cifs command displays a Data Mover's CIFS configuration, including the Usermapper service it is using.

If you run the server_cifs command for the Data Mover on which the Usermapper service is running (typically server_2), the Usermapper service listed displays the Data Mover's loopback address (127.0.0.1) as the IP address of its Usermapper service.

Action

To display the Usermapper service used by a Data Mover, use this command syntax:

$ **server_cifs** *<movername>*

where:

<movername> = name of the Data Mover

Example:

To display the Usermapper service used by server_3, type:

$ server_cifs server_3

Output

```
server_3 :
96 Cifs threads started
Security mode = NT
Max protocol = NT1
I18N mode = UNICODE
Home Directory Shares DISABLED
Usermapper auto broadcast enabled

Usermapper[0]=[128.221.252.2] state:active (auto discovered)
Usermapper[1]=[128.221.253.2] state:active (auto discovered)

Default WINS servers = 192.168.4.230
Enabled interfaces: (All interfaces are enabled)

Disabled interfaces: (No interface disabled)
```

Note

This example shows that server_3 is using the Usermapper service located on server_2 at internal IP addresses 128.221.252.2 and 128.221.253.2; the service is available, and the service was located using the autodiscovery broadcast.

Import and export database information

You can import and export user and group information to and from the Usermapper database.

Import database information

Typically, you import information into the Usermapper database from a user and group file to reimport an edited Usermapper database, migrate the primary Usermapper service from one Data Mover to another, or upgrade or migrate the Usermapper configuration. Contact your EMC Customer Support Representative for assistance if you are migrating the primary Usermapper service from one Data Mover to another.

Use the import option of the server_usermapper command to import a user or group file. Usermapper can import files in either of two formats: a standard UNIX format that corresponds to the passwd and group file formats, or a format that includes the SID in the first field.

Example of a user file entry in standard UNIX format (Format 1):

```
rob.hilder.dir:*:26831:903:rob.hilder.dir:/usr/rob.hilder.dir:/bin/sh
```

Example of a user file entry in SID-based format (Format 3):

```
S-1-5-15-139d2e78-56b177fd-5475b975-3323d:*:26831:903:user rob.hilder
from domain
dir:/usr/S-1-5-15-139d2e78-56b177fd-5475b975-3323d:/bin/sh
```

Example of a group file entry in standard UNIX format (Format 1):

```
people.mass.subscribers.db.dir:*:58362:people.mass.subscribers.db.dir:
```

Example of a group file entry in SID-based format (Format 3):

```
S-1-5-15-139d2e78-56b177fd-5475b975-2c3d6:*:58362:people.mass.subscribers.db.dir:
```

Action
To import user and group information into the Usermapper database, use this command syntax: `$ server_usermapper <movername> -Import {-user | -group} <pathname>` where: *<movername>* = name of the Data Mover *<pathname>* = name and location of the user file to be imported Examples: To import user information into the Usermapper database on server_2, type: `$ server_usermapper server_2 -Import -user /nas/cifs/usrmapperV3/linux/usrmap.passwd` To import group information into the Usermapper database on server_2, type: `$ server_usermapper server_2 -Import -group /nas/cifs/usrmapperV3/linux/usrmap.group`

Output
server_2 : done

Export database information

Typically, you would export user and group information from the Usermapper database to migrate the primary Usermapper service, back up the Usermapper database, or collect information for troubleshooting.

Use the export option of the server_usermapper command to export a user or group file. Usermapper exports files in a format that includes the SID in the first field.

Example of a user file entry in SID-based format (Format 3):

```
S-1-5-15-139d2e78-56b177fd-5475b975-3323d:*:26831:903:user rob.hilder
from domain
dir:/usr/S-1-5-15-139d2e78-56b177fd-5475b975-3323d:/bin/sh
```

Example of a group file entry in SID-based format (Format 3):

```
S-1-5-15-139d2e78-56b177fd-5475b975-2c3d6:*:58362:people.mass.subscribers.db.dir:
```

Action
To export user and group information from the Usermapper database, use this command syntax: $ **server_usermapper** *<movername>* **-Export {-user | -group}** *<pathname>* where: *<movername>* = name of the Data Mover *<pathname>* = name and location of the file to which information is to be exported Examples: To export user information from the Usermapper database on server_2, type: **$ server_usermapper server_2 -Export -user /home/nasadmin/backup.passwd** To export group information from the Usermapper database on server_2, type: **$ server_usermapper server_2 -Export -group /home/nasadmin/backup.group**
Output
server_2 : done

Maintain the Usermapper database

Do not modify the Usermapper database files. Windows users might have problems accessing files if you modify the Usermapper database files.

If an issue seems to require a change to a Usermapper mapping entry, consult your EMC Customer Support Representative to determine the best course of action.

Note: Changes made to the Usermapper database are not reflected by a client Data Mover, if the client Data Mover has already cached the existing Usermapper information in its local cache. If the files and folders have already been created by using the existing UIDs and GIDs, just changing the UID or GID map will make file objects inaccessible.

Back up Usermapper

1. As root, dump the password and group files to a specified directory by typing:

   $ **server_usermapper server_2 -Export -user /home/nasadmin/backup.passwd**

   $ **server_usermapper server_2 -Export -group /home/nasadmin/backup.group**

2. Make a backup copy of the current usrmap.cfg file (if one is in use) by typing:

   $ **cp /nas/rootfs/slot_2/.etc/usrmapper/usrmap.cfg /home/nasadmin/usrmap.cfg**

3. Make a backup copy of the usrmap.settings file by typing:

   $ **cp /nas/rootfs/slot_2/.etc/usrmapper/usrmap.settings /home/nasadmin/usrmap.settings**

Change Usermapper default configuration settings

Usermapper has default configuration settings, but you can change them by modifying these parameters:

- usrmap minuid
- usrmap maxuid
- usrmap mingid
- usrmap maxgid

If you have imported an existing configuration file, these UID and GID range limits only apply when a new Usermapper database entry is created.

Note: Parameter and facility names are case-sensitive.

Action
To change the default Usermapper UID or GID values, use this command syntax: $ **server_param** *<movername>* **-facility usrmap -modify** *<param_name>* **-value** *<new_value>* where: *<movername>* = name of the Data Mover *<param_name>* = name of the parameter *<new_value>* = value you want to set for the specified parameter Example: To change the minimum UID value, type: $ **server_param server_2 -facility usrmap -modify minuid -value 32** To change the maximum UID value, type: $ **server_param server_2 -facility usrmap -modify maxuid -value 2147483647**
Output
server_2 : done

6 Managing secmap

Secure mapping on page 17 provides conceptual information. The tasks to manage secmap are:

Disable secmap

Secmap caching is enabled by default when CIFS service starts. It is automatically disabled when CIFS service stops. It can also be disabled by using the parameter cifs secmap.enable. This parameter is only taken into account at CIFS startup.

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

Display secmap mapping entries

Action
To display secmap mapping entries for a user, group, domain, or SID, or for all existing entries, use this command syntax: `$ server_cifssupport <movername> -secmap -list [ -name <name> -domain <domain_name> | -domain <domain_name> | -sid <SID> | -uid <user_id> | -gid <group_id>]` where: *<movername>* = name of the Data Mover *<name>* = name of the user or group *<domain_name>* = the fully qualified domain name *<SID>* = SID *<user_id>* = UID *<group_id>* = GID Example: To display all the secmap mapping entries on server_2, type: `$ server_cifssupport server_2 -secmap -list` To display the secmap mapping entry on server_2 for the user user1 in domain NASDOCS, type: `$ server_cifssupport server_2 -secmap -list -name user1 -domain NASDOCS`

Output	Note
`server_2 : done`	The output includes the SID, type (user or group), ID (UID or GID according to type), origin, domain, and account names (optional). If a mapping is not found, the message, mapping not found, is returned.

Display secmap reverse mapping entries

Action
To display secmap reverse mapping entries (SIDs) for a UID or GID, use this command syntax: `$ server_cifssupport <movername> -secmap -list -uid <user_id> | -gid <group_id>` where: *<movername>* = name of the Data Mover *<user_id>* = UID *<group_id>* = GID Example: To display the secmap reverse mapping entry on server_2 for UID 32771, type: `$ server_cifssupport server_2 -secmap -list -uid 32771`

Output	Note
`server_2 : done`	The output might include multiple SIDs if more than one SID has been mapped to the specified ID. The output displays all information associated with the SID.

Create secmap mapping entries

Creating secmap mapping entries on page 17 provides conceptual information.

Action
To create secmap mapping entries, use this command syntax: `$ server_cifssupport <movername> -secmap -create{ -name <name> -domain <domain_name> | -sid <SID> }` where: *<movername>* = name of the Data Mover *<name>* = name of the user or group *<domain_name>* = the fully qualified domain name *<SID>* = SID Example: To create a secmap mapping entry on server_2 for the user user3 in domain NASDOCS, type: `$ server_cifssupport server_2 -secmap -create -name user3 -domain NASDOCS`

Output	Note
`server_2 : done`	The output displays all mappings that have changed after they were introduced to the database.

Check secmap mapping entries

Checking and updating secmap mapping entries on page 18 provides conceptual information.

Action
To check all the secmap mapping entries, use this command syntax: `$ server_cifssupport <movername> -secmap -verify {-name <name> -domain <domain_name> | -sid <SID>}` where: *<movername>* = name of the Data Mover *<name>* = name of the user or group *<domain_name>* = fully qualified domain name *<SID>* = SID Example: To check all the secmap mapping entries on server_2, type: `$ server_cifssupport server_2 -secmap -verify -user user3 -domain NASDOCS`

Output	Note
`server_2 : done`	The output displays all mappings that have changed after they were introduced to the database.

Update secmap mapping entries

Checking and updating secmap mapping entries on page 18 provides conceptual information.

Action	
To update all the secmap mapping entries, use this command syntax: `$ server_cifssupport <movername> -secmap -update { -name <name> -domain <domain_name> | -sid <SID>}` where: *<movername>* = name of the Data Mover *<name>* = name of the user or group *<domain_name>* = the fully qualified domain name *<SID>* = SID Example: To update all the secmap mapping entries on server_2, type: `$ server_cifssupport server_2 -secmap -update -user user3 -domain NASDOCS`	
Output	**Note**
`server_2 : done`	The output displays all mappings that have been updated.

Remove secmap mapping entries

To remove a mapping, VNX first removes the corresponding reverse mapping and then removes the main mapping. If the reverse mapping contains several SIDs, VNX removes the specified SID.

Action
To remove secmap mapping entries, use this command syntax: `$ server_cifssupport <movername> -secmap -delete { -name <name> -domain <domain_name> | -sid <SID>}` where: *<movername>* = name of the Data Mover *<name>* = name of the user or group *<domain_name>* = fully qualified domain name *<SID>* = SID Example: To remove a secmap mapping entry on server_2 for the user user3 in domain NASDOCS, type: `$ server_cifssupport server_2 -secmap -delete -name user3 -domain NASDOCS`
Output
`server_2 : done`

Export secmap mapping entries

Action	
To export secmap mapping entries, use this command syntax: `$ server_cifssupport <movername> -secmap -export [ -file <filename> ]` where: *<movername>* = name of the Data Mover *<filename>* = name of the file where the mappings should be saved Example: To export secmap mapping entries on server_2, type: `$ server_secmap server_2 -secmap -export -file exportfile.txt`	
Output	**Note**
`server_2 : done`	If you do not specify a filename, the secmap database is displayed on the screen.

Import secmap mapping entries from a file

Action	
To import secmap mapping entries, use this command syntax: `$ server_cifssupport <movername> -secmap - import -file <filename>` where: *<movername>* = name of the Data Mover *<filename>* = name of the file that contains the mappings to be imported Example: To import secmap mapping entries on server_2, type: `$ server_cifssupport server_2 -secmap -import -file importfile.txt`	
Output	**Note**
`server_2 :`	If imported mappings conflict with existing mappings, they are rejected and an error is returned.

Report secmap status

Action
To display current secmap status, including database state, domains handled by secmap, and resource usage (number of inodes and blocks used), use this command syntax: `$ server_cifssupport <movername> -secmap -report` where: *<movername>* = name of the Data Mover Example: To display current secmap status on server_2, type: `$ server_cifssupport server_2 -secmap -report`

Output

```
server_2 : done

SECMAP GENERAL INFORMATIONS

Name         :server_2
State        :Enabled
Fs           : /
Used nodes   : 27
Used blocks  : 0

SECMAP MAPPED DOMAIN

Name           SID
INTGW2K3       S-1-5-15-56db7d78-9b661160-9e19279b-ffffffff
```

7

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.

Topics included 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**.

Known problems and limitations

Table 3 on page 56 describes known problems that might occur when using Usermapper and presents workarounds.

Table 3. Usermapper known problems and workarounds

Known problem	Symptom	Workaround
The primary Usermapper service must be enabled before secondary services can be configured.	When you run the server_usermapper <movername> -enable primary= command, you receive the following error: Error 4020: <movername>:failed to complete command	Check the operational state of the primary service and enable it by using the server_usermapper <movername> -enable command.
Usermapper stops mapping new UIDs and GIDs after the root file system of the Data Mover (where the Usermapper database is stored) becomes full. New users will be denied access to system objects.	The following errors are entered repeatedly in the server log for any additional mapping requests after the root file system reaches capacity: error: -20 for user uid request error: -20 for group gid request	Determine the required size of the root file system based on the number of users in the Windows environment. Contact your EMC Customer Support Representative for assistance in determining size requirements.

Known problems and limitations in using secmap

Table 4 on page 57 describes known problems that might occur when using secmap and presents workarounds.

Table 4. Secmap known problems and workarounds

Known problem	Symptom	Workaround
No new mappings created	If the secmap file system is nearly full, the secmap database might reach a point where it cannot store new mappings although it can continue to return existing mappings.	Secmap will work in a degraded mode until the file system where it resides is cleaned or extended.
Synchronization required with mapping services	By default, secmap is a write-once, read-many cache to avoid accidental mapping modifications. However, when mappings are purposely changed, the new mapping is not automatically made in secmap. The new mapping has to be enforced manually in secmap before resetting the ACL. Consequently, secmap can be out of sync if mappings are changed in mapping services.	Use the secmap commands to check database consistency and possibly fix mapping inconsistencies. **⚠ CAUTION** After modifying mappings,you must update the ACLs to ensure that they use the new mappings. Otherwise, access rights issues might arise due to inconsistencies between secmap mappings and mappings stored in ACLs.

Usermapper events and notifications

Table 5 on page 58 lists the Usermapper events. *Configuring Events and Notifications on VNX for File* provides a description of how to configure the Celerra Network Server to record and display these events.

Table 5. USRMAP events

Facility name	Facility ID	Facility description	Event ID	Event description
USRMAP	93	Monitors Usermapper events	0	Usermapper OK
			1	Usermapper database created
			2	Usermapper service enabled
			3	Usermapper service stopped
			4	Usermapper database destroyed
			5	Usermapper available
			6	Usermapper unreachable
			7	Usermapper file system quota exceeded

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.

Glossary

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).

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.

Control Station
Hardware and software component of VNX for file that manages the system and provides the user interface to all VNX for file components.

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.

database management system (DBMS)
Software designed to manage databases. Data Movers use DBMS to create and manage Usermapper and secmap mapping information.

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 controller
Server that authenticates user logins and maintains the security policy and the security account's master database for a Windows domain. Domain controllers manage user access to a network, which includes logging in, authentication, and access to the directory and shared resources.

See also *Windows domain*.

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*.

G

group identifier (GID)
Numeric identifier assigned to a particular group of users.

I

Identity Management for UNIX (IdMU)
Microsoft software that provides a UNIX environment on Windows, specifically UNIX identity and security services.

K

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

L

LDAP-based directory
Directory servers that support LDAP, including Active Directory with IdMU, or SFU, OpenLDAP, or iPlanet (also known as Sun Java System Directory Server and Sun ONE Directory Server).

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.

M

Microsoft Windows Services for UNIX (SFU)
Microsoft software that provides a UNIX environment on Windows.

N

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.

Network Information Service (NIS)
Distributed data lookup service that shares user and system information across a network, including usernames, passwords, home directories, groups, hostnames, IP addresses, and netgroup definitions.

Network Time Protocol (NTP)
Protocol used to synchronize the realtime clock in a computer with a network time source.

ntxmap
Customized software used to support mapping requirements in a multiprotocol environment.

P

primary Usermapper service
Instance of the Usermapper service that assigns user IDs (UIDs) and GIDs to Windows users and groups by asking for access to system objects.

Q

quota
Limit on the amount of allocated disk space and the number of files (inodes) that a user or group of users can create in a Production File System. Quotas control the amount of disk space or the number of files that a user or group of users can consume or both.

S

secondary Usermapper service
In a multi- environment, an instance of the Usermapper service that forwards requests for user mappings to the primary Usermapper service and returns those mappings to the Data Movers in addition to storing the mappings it processes.

security identifier (SID)
Unique identifier that defines a user or group in a Microsoft Windows environment. Each user or group has its own SID.

SFU

See Microsoft Windows Services for UNIX.

U

user file
Refers to the passwd file that resides on each Data Mover.

User ID (UID)
Numeric identifier that corresponds to a particular user.

Usermapper
Service that automatically maps distinct Windows users and groups to distinct UNIX-style UIDs and GIDs.

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*.

Index

U