NEXSAN

HYPER-UNIFIED STORAGE

Nexsan Unity

NFS Interoperability

NEXSAN | 325 E. Hillcrest Drive, Suite #150 | Thousand Oaks, CA 91360 USA
Printed Friday, September 27, 2019 | www.nexsan.com

Regulatory Compliance

United States Statement for FCC: Nexsan equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Electromagnetic Emissions: FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A, ICES-003

Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)

CE Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)

RoHS: RoHS2 (Global)

Other international regulatory compliance: VCC (Japan)

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

Trademarks

Nexsan® is a trademark or registered trademark of Nexsan Technologies, Inc. The Nexsan logo is a registered trademark of Nexsan Technologies, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Patents

This product is protected by one or more of the following patents, and other pending patent applications worldwide:

United States patents US8,191,841, US8,120,922;

United Kingdom patents GB2466535B, GB2467622B, GB2467404B, GB2296798B, GB2297636B

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Nexsan Technologies, Inc. is strictly prohibited.

Nexsan Technologies, Inc. reserves the right to make changes to this manual, as well as the equipment and software described in this manual, at any time without notice. This manual may contain links to Web sites that were current at the time of publication, but have since been moved or become inactive. It may also contain links to sites owned and operated by third parties. Nexsan is not responsible for the content of any such third-party site.

Contents

About this document

This guide provides procedures for configuring Unity interoperation with Network File Systems and supported environments and user authentication methods and directory services.

Audience

This guide has been prepared for the following audience:

- Any qualified NST/Unity administrator.

Conventions

Here is a list of text conventions used in this document:

Convention	Description
underlined blue	Cross-references, hyperlinks, URLs, and email addresses.
boldface	Text that refers to labels on the physical unit or interactive items in the graphical user interface (GUI).
`monospace`	Text that is displayed in the command-line interface (CLI) or text that refers to file or directory names.
`monospace bold`	Text strings that must be entered by the user in the command-line interface or in text fields in the graphical user interface (GUI).
italics	System messages and non-interactive items in the graphical user interface (GUI) References to Software User Guides

Notes, Tips, Cautions, and Warnings

Note Notes contain important information, present alternative procedures, or call attention to certain items.

Tip Tips contain handy information for end-users, such as other ways to perform an action.

CAUTION: In hardware manuals, cautions alert the user to items or situations which may cause damage to the unit or result in mild injury to the user, or both. In software manuals, cautions alert the user to situations which may cause data corruption or data loss.

WARNING: Warnings alert the user to items or situations which may result in severe injury

or death to the user.

Contacting Nexsan

For questions about Nexsan products, please visit the Nexsan support Web page, and the Nexsan Unity Documents and Downloads page. If you are unable to find the answer to your question there, please see our contact information below.

Service and support

Nexsan's Technical Services Group provides worldwide assistance with installation, configuration, software support, warranty, and repair for all Nexsan products. A variety of service and support programs are available to provide you with the level of coverage and availability your operation requires.

Nexsan Unity Documents & Downloads page:
https://helper.nexsansupport.com/unt_downloads.html

Unity Online Help page:
https://helper.nexsansupport.com/unt_onlinehelp.html

Contact Nexsan Unity support:
https://helper.nexsansupport.com/unt_support

Worldwide Web site:
www.nexsan.com

Related documentation

The following Nexsan product manuals contain related information:

- Nexsan Unity Online Help
- *Nexsan Unity Hardware Reference Guide*
- *Nexsan UnityHardware Maintenance Guide, Unity Next Generation*
- *Nexsan Unity Software User Guide*
- *Nexsan Unity nxadmin Command-line Interface Reference Guide*
- *Nexsan Unity nxcmd Command-line Interface Reference Guide*
- *Nexsan Unity Snapshots and Replication Guide*
- *Nexsan Unity Storage Expansion Reference Guide*
- *Nexsan Unity VMware Best Practices Guide*
- *Nexsan Unity NFS Interoperability*
- *Nexsan Unity Networking Best Practices Guide*
- *Nexsan Unity Performance Best Practices Guide*
- *Nexsan Unity Microsoft Best Practices Guide*

Chapter 1

Introduction

This guide provides procedures for configuring Unity interoperation with Network File Systems and supported environments and user authentication methods and directory services.

The document includes the following chapters:

Chapter	Description
Introduction	A brief overview of NFS support in Unity and links to where you'll find relevant procedures for integrating NFS with Unity for each authentication type.
Using NFS with NIS	Provides procedures for integrating Unity with NIS, and how to use NFSv4 to access an NFS share.
Using LDAP with NFS	Provides the standard LDAP procedure and how to connect LDAP in an Active Directory environment.
Using Active Directory with NFS	Provides procedures for integrating NFS with Microsoft Active Directory.

Overview

NFS (Network File System) is the distributed file system used in many UNIX-based operating systems, such as Solaris, AIX, HP-UX, Linux, and FreeBSD. It is also available for other operating systems, such as the Mac OS, OpenVMS, Microsoft Windows, Novell NetWare, and IBM AS/400. NFS allows users on client computers to access files over a network in a manner similar to how local storage is accessed.

Nexsan Unity can be integrated with two versions of NFS: NFSv3 and NFSv4. NFSv2 is not supported.

NFSv4

NFSv4, first published in 2000 and updated in 2003, includes performance improvements, mandates strong security, and introduces a stateful protocol.

NFSv4.1 and NFSv4.2 are not supported at this time.

NFSv3

NVFv3, first published in 1995, added support for 64-bit files and offsets, thus removing the 2 GB file size limitation. It also added several other features, such as asynchronous writes, the READDIRPLUS operation (to fetch file handles and attributes along with file names when scanning a directory), and native support for TCP as a transport layer.

NFS interoperability

NFS is only one piece of the network file sharing environment. NFS must also work with the directory services of the host computers attached to the network for authentication. NFS works with UNIX services such as NIS, LDAP, and Local, and also with Microsoft services like Active Directory (AD) and Identity Management for UNIX (IDMU). Each directory service works with NFS in slightly different ways, and multiple directory services can operate with NFS at the same time. However, certain combinations require additional set up and configuration; see Finding NFS interop procedures by authentication method on the facing page.

Finding NFS interop procedures by authentication method

Use the table below to find the procedure required for the authentication method used for your UNIX directory service. Access control lists (ACLs) are supported when using Unity with NFSv3 and NSFv4.

Table 1-1: UNIX authentication scenarios

Authentication implementation	Procedure
Active Directory only	Join the Active Directory domain as described in Using Active Directory for NFS on page 24.
Active Directory and IDMU	1. Join the Active Directory domain as described in Using Active Directory for NFS on page 24. 2. Add UNIX attributes to AD users using IDMU in AD.
Active Directory with NIS implementation	1. Join the Active Directory domain as described in Using Active Directory for NFS on page 24. 2. For NFSv3 and NFSv4, use the standard NIS procedure. See Integrating with Network Information Service (NIS) on page 13. For NFSv4, configure the domain as described in Using an NFS version 4 (NFSv4) client to access an NFS share on page 14. 3. Map users using the `nstusermaps` CLI command; see nstusermaps on page 51.
Active Directory with local authentication	1. Join the Active Directory domain as described in Using Active Directory for NFS on page 24. 2. Add local users manually to AD. 3. Map users using the `nstusermaps` CLI command; see nstusermaps on page 51.
LDAP only	Use the standard LDAP connection procedure. See Connecting to an LDAP Directory Service on page 19.
LDAP with Active Directory	1. Join AD as described in Using Active Directory for NFS on page 24. 2. Login to the nxadmin CLI, and type `menu` 3. Select option 6, Configure Shares and Active Directory. 4. Select option 7, Configure the LDAP client in AD mode. See Configuring the LDAP Client in AD mode on page 21. 5. Select option 2, Initialize LDAP to Active Directory mapping. See Initializing LDAP to Active Directory mapping on page 21. 6. Select option 5, Set LDAP client configuration, and follow the steps to configure the LDAP client. See Setting the LDAP Client configuration on page 22.

Authentication implementation	Procedure
	7. Map users using the `nstusermaps` CLI command. See nstusermaps on page 51. 8. For NFSv4 only, configure the NSFv4 domain. See Using an NFS version 4 (NFSv4) client to access an NFS share on page 14.
NIS only	1. For NFSv3, use the standard NIS procedure. See Integrating with Network Information Service (NIS) on page 13 2. For NFS v4, use the standard NIS integration procedure, but do NOT modify `/etc/resolv.conf`. See Integrating with Network Information Service (NIS) on page 13. 3. For NFSv4, configure the domain as described in Using an NFS version 4 (NFSv4) client to access an NFS share on page 14. 4. Map users using the `nstusermaps` CLI command; see nstusermaps on page 51.
Local authentication (Nexsan Unity)	1. Standard Unity authentication process as described in Reverting to Unity Authentication on page 38. 2. Configure the NSFv4 domain. See Using an NFS version 4 (NFSv4) client to access an NFS share on page 14.

Chapter 2

Using NFS with NIS

Use the following procedures when integrating NFS with the NIS directory service.

Integrating with Network Information Service (NIS)

In UNIX environments (for connectivity to NFS file systems), the Unity Storage System supports three UNIX directory services: LDAP (Lightweight Directory Access Protocol), NIS (Network Information Service), and Unity authentication.

If you have UNIX users that authenticate through NIS—regardless of the authentication set up for the Unity Storage System—you must run some nxadmin CLI commands in a specific order to fully integrate the Unity Storage System with NIS.

► **To integrate the Unity Storage System with NIS:**

1. Create the name of the domain. Type this command:

   ```
   domainname <domain>
   ```

   Where **<*domain*>** is the name of the NIS domain used; for further details, see domainname on page 41.

2. Define the domain as the default NIS domain used; for further details, see setdefaultdomain on page 41.

   ```
   setdefaultdomain <domain>
   ```

3. Reconfigure the `etc/nsswitch.conf` file after changing the authentication mode so that the NIS authentication settings are added to password and group files. Type this command:

   ```
   changenameservices -c add -s nis
   ```

   For further details, see changenameservices on page 42.

4. To initialize the NIS server, type this command on the active controller:

   ```
   ypinit -c
   ```

   For further details, see ypinit on page 42.

   a. You will be prompted to enter the NIS server name:

   ```
   "In order for NIS to operate successfully, we have to construct a list
   of the NIS servers.  Please continue to add the names for YP servers in
   order of preference, one per line.  When you are done with the list,
   type a <control D> or a return on a line by itself."

   next host to add:  nis.nisdomain2.lan

   next host to add:
   ```

   b. When prompted to confirm the NIS server name, type **y** and press Enter:

   ```
   The current list of yp servers looks like this: nis.nisdomain2.lan
   Is this correct?  [y/n: y]  y
   ```

   If you see `svcadm` messages about services missing, similar to this:

   ```
   svcadm: Pattern 'network/nis/server:default' doesn't match any
   instances
   ```

   you may ignore these messages.

5. Add the NIS server host to `/etc/hosts` on both controllers.

   a. Open the `hosts` configuration file, type: **`edit /etc/hosts`**

   b. Add the NIS server to the list, in this format:

   ```
   <server IP address> nis-p-<server name> <domain name>
   ```

6. To start active services for the NIS client, type this command on both controllers:

   ```
   svc enable nis/client
   ```

   For further details, see svc on page 43.

7. To display the list of NIS users, type:

   ```
   ypcat -k passwd
   ```

   For further details, see ypcat on page 45.

8. To display the list of NIS groups, type:

   ```
   ypcat -k group
   ```

▶ **What's Next:**

1. Give the NIS users access to the file using the `chmod` command. For information, see chmod on page 45.
2. Map users using the `nstusermaps` command. For information, see nstusermaps on page 51.

Using an NFS version 4 (NFSv4) client to access an NFS share

To access or mount an NFS share from an NFS version 4 (NFSv4) client, you must perform some additional configuration steps, both on Unity where the NFS share exists and on the NFSv4 client computers where you intend to mount the NFS share.

Note NSFv4 uses name-based permissions mapping. This means users must have the same name on both the client and Unity. It also requires an NFSv4 domain to be set. This must be identical on both Unity and the client.

▶ **On Unity where the NFS share exists, you must:**

1. Use the nxadmin CLI to specify a domain name to enable user/group mapping between Unity and your NFSv4 clients.
   For example, `nfs domain set nst.domain`
2. Add user and/or group accounts, respectively, on Unity with account names that correspond to user and/or group accounts on the NFSv4 client computers where you intend to mount the NFS share.

▶ **On the NFSv4 client computers where you intend to mount the NFS share (for example, Linux/CentOS), you must:**

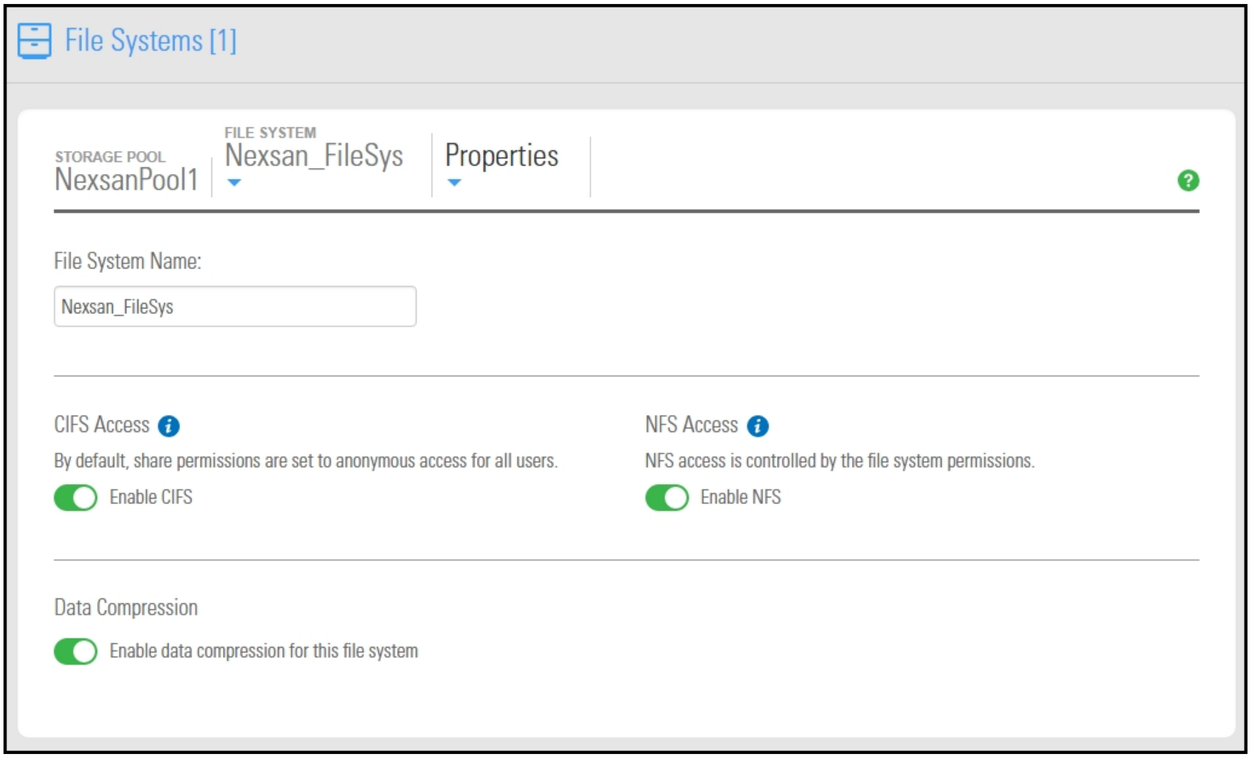
1. Add the NFSv4 domain name you specified on Unity to the `/etc/idmapd.conf` file.
2. Stop and then restart the `idmap` (Identity Mapping) service.
3. Make sure this service starts on system boot up: `chkconfig rpcidmapd on`
4. Mount the NFS share.

▶ **To configure NFSv4 support:**

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you need to access.
3. Select **Summary > Properties**.

4. Click the **Enable NFS** button

Figure 2-1: File System Properties panel



File Systems [1]

STORAGE POOL NexsanPool1 | FILE SYSTEM Nexsan_FileSys | Properties

File System Name: Nexsan_FileSys

CIFS Access

By default, share permissions are set to anonymous access for all users.

● Enable CIFS

NFS Access

NFS access is controlled by the file system permissions.

● Enable NFS

Data Compression

● Enable data compression for this file system

5. Click the **Apply** button to save your settings.

6. Use the nxadmin CLI to add user and/or group accounts to Unity with account names that correspond to user and/or group accounts on the NFSv4 client computers where you intend to mount the NFS share:
   a. Access the nxadmin CLI on Unity.
   b. Log on as **`nxadmin`**.
   c. Enter `menu`.
   d. In the NestOS Admin Menu, enter **`4`** (**`Run a Command`**).
   e. At the `command:` prompt, enter the **`useradd`** command using this syntax to add a user:

      ```
      useradd -u <uid> <user name>
      ```

      You cannot use these UID numbers because they are reserved:

      - 0 to 101
      - 60001
      - 60002
      - 65534
      - 90000 to 90050

      If one of these IDs is already assigned to a user on your network, please contact Nexsan Technical Support to request that they free up the reserved ID.
   f. At the `command:` prompt, enter the **`groupadd`** command using this syntax to add a group:

      ```
      groupadd -u <gid> <group name>
      ```

      You cannot use these GID numbers because they are reserved:

      - 0 to 101
      - 60001
      - 60002
      - 65534
      - 90000 to 90050
      - 99999

      If one of these IDs is already assigned to a user on your network, please contact Nexsan Technical Support to request that they free up the reserved ID.
7. Mount the NFS share.

Chapter 3

Using LDAP with NFS

Use the following procedures when integrating NFS with the LDAP directory service:

- If you are using a standard LDAP environment, follow the steps under Connecting to an LDAP Directory Service on the next page.
- If you are using LDAP in an Active Directory environment, follow the steps under Configuring the LDAP Client in AD mode on page 21.

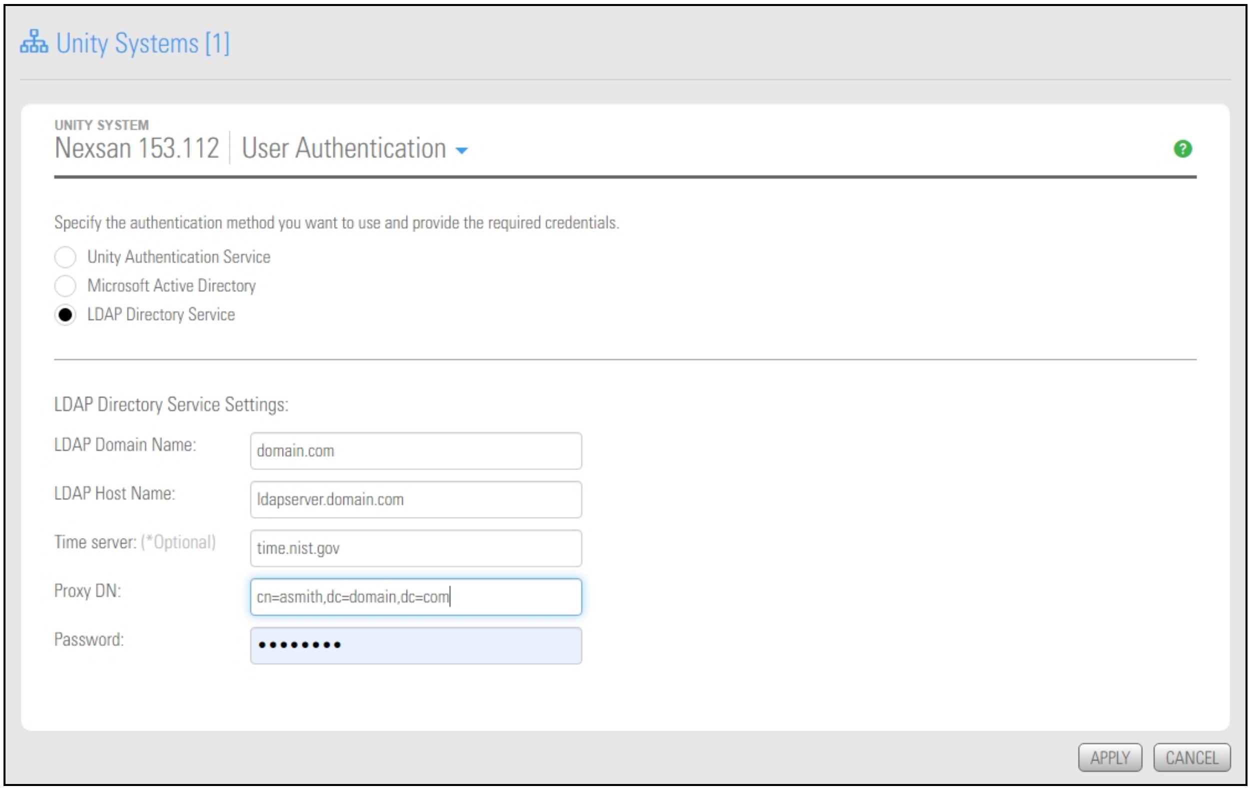
Connecting to an LDAP Directory Service

The Unity Authentication service is preconfigured by default during initial system setup. Use this procedure if you want to instead connect to an LDAP Directory Service.

► **To connect to an LDAP Directory Service:**

1. From the **System** menu, select **Unity Systems**.
2. Click the link to the Unity System you want to connect to LDAP.
3. Click **Summary** > **User Authentication**.

Figure 3-1: Connecting to an LDAP Directory Service



Unity Systems [1]

UNITY SYSTEM

Nexsan 153.112 | User Authentication

Specify the authentication method you want to use and provide the required credentials.

○ Unity Authentication Service

○ Microsoft Active Directory

● LDAP Directory Service

LDAP Directory Service Settings:

LDAP Domain Name: domain.com

LDAP Host Name: ldapserver.domain.com

Time server: (*Optional) time.nist.gov

Proxy DN: cn=asmith,dc=domain,dc=com

Password: •••••••••

4. Select **LDAP Directory Service**. The settings display for connecting to an LDAP Directory service on the network.
5. In the **LDAP Domain Name** field, type the name of the LDAP domain and extension for the domain that you want Unity to connect to. For example, `domain.com`.

6. (Optionally) In the **LDAP Host Name** field, type the host name of the LDAP Directory server that you want Unity to connect to. For example, `ldapserver.domain.com`.

   This step is only required if:

   - the domain name you specify in the **LDAP Domain Name** field does not resolve to the IP address of the LDAP Directory server, or
   - the LDAP domain name you specify is an identification label for multiple resources in your LDAP implementation.

   If you do not specify an LDAP host name, Unity automatically connects to the LDAP Directory server that you specify in the **LDAP Domain Name** field.

7. Optionally, in the **Time Server** field, type the IP address or the fully qualified domain name of the time server that you want Unity to synchronize its date and time with. A time server is required to ensure that the date and time settings on Unity are synchronized with the LDAP Directory server that the system connects to. By default, a time server is already defined.

   Note Unity supports multiple time servers: if you specify a time server in the **Time Server** field, as opposed to using the LDAP Directory server for date and time synchronization for Unity, we highly recommend that you specify at least two time servers; this ensures that date and time synchronization on Unity continues in the event that one of the time servers you specify is no longer available.

   Note To specify multiple time servers, use a comma to separate each entry, for example: `tick.utoronto.ca,time.nrc.ca`.

8. In the **Proxy DN** field, type the Proxy identity's distinguished name (DN) configured on your LDAP Directory server. For example, `cn=asmith,dc=domain,dc=com`, where `cn` denotes common name, and `dc` denotes domain component. The Proxy identity is a user on the LDAP Directory server that has restricted authority to required information on the server. Nexsan Unity binds to the LDAP Directory server using the Proxy user's DN.

   Note The LDAP Directory server must have a Proxy identity configured before you connect Unity to the server.

9. Type the Proxy identity's password in the **Password** field.

10. Click the **Apply** button.

11. When the **Confirm DNS Settings** prompt appears, do one of the following:

    a. If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and click the **Apply** button, or

    b. If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to keep the current DNS settings.

12. The wizard applies your settings and if all are successful, prompts you to click **OK**.

Configuring the LDAP Client in AD mode

A UNIX environment can use either a Local directory service or the NIS or LDAP protocol to access the directory service and the data stored on any UNIX server on the network. If the UNIX environment also communicates with a Windows environment, other directory services must be taken into account for proper access to directory services. For example, if Active Directory is used as the main directory service in your environment, you must join the Active Directory domain in addition to using your current UNIX directory service.

This section covers these topics:

- Initializing LDAP to Active Directory mapping below
- Setting the LDAP Client configuration on the facing page

Initializing LDAP to Active Directory mapping

► **To initialize LDAP:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **2** (**Initialize LDAP to Active Directory mapping**) and press Enter.

Figure 3-2: NestOS LDAP Client in AD Mode menu

```
1 - Show current information
2 - Initialize LDAP to Active Directory mapping
3 - Upload a CA Certificate
4 - Remove a CA Certificate
5 - Set LDAP Client configuration
6 - Configure file systems group lookup
7 - Reset the LDAP Client configuration
8 - Clear the nstusermaps cache
9 - View instructions on using nstusermaps for LDAP to AD mapping
10 - Show ACLs on file systems
11 - Set ACLs on file systems
12 - Restart the LDAP Client Service

q - Exit

Select an option:
```

The Unity Storage System initializes the mapping on both the current cluster node and the other cluster node.

Setting the LDAP Client configuration

► **To configure the LDAP client:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **5** (**Set LDAP Client configuration**) and press Enter.
4. Select one of the two options:

   `1 - anonymous`:

   a. Type **1** and press Enter to set the LDAP Client configuration to `anonymous`.

   b. Select one of the two credential options (`tls` or `none`) by typing its number and pressing Enter.

   `2 - simple bind`:

   a. Type **2** and press Enter to set the LDAP Client configuration to `simple bind`.

   b. Enter the proxy DN and press Enter .

Chapter 4

Using Active Directory for NFS

Use the following procedures when integrating Microsoft Active Directory and NFS:

To integrate NFS with Microsoft Active Directory:

1. Join an Active Directory Domain.
   - To join an Active Directory domain through Unity, see Joining a Microsoft Active Directory domain on page 33.
   - To join an Active Directory domain using the CLI, see Joining a domain using the CLI on page 35.
2. Map users using the `nstusermaps` CLI command. See nstusermaps on page 51.

Microsoft Active Directory domain requirements

This section describes the Microsoft Active Directory support requirements for Unity. Carefully review this table before joining Unity to a Microsoft Active Directory domain.

Requirement	Description
Operating Systems	Any of the following: ● Windows Server 2016 ● Windows Server 2012 ● Windows Server 2008 R2 ● Windows Server 2008 x86 or x64, including: ● Windows Server 2008 with Service Pack 1 ● Windows Server 2008 with Service Pack 2 ● Window Server 2003 R2 x86 or x64
Reverse DNS	The Microsoft Active Directory implementation must be configured with a reverse DNS lookup zone.
Global catalog and LDAP catalog ports	The primary domain controller that Unity connects to must have both the global catalog port (3268) and the LDAP catalog port (389) open. In a Microsoft Active Directory forest implementation, all domain controllers must have these ports open.
Time server	The primary domain controller that Unity connects to must be configured as a reliable time source (time server capability) for the domain. In a Microsoft Active Directory forest implementation, all domain controllers must have this capability. If the Microsoft Active Directory implementation does not provide, or is not configured for, time server capability, you must specify a valid Network Time Protocol (NTP) source for Unity to synchronize its date and time with.
Domain administrator privileges	You will need to provide domain credentials for a domain administrator, or of a user who has full domain administrative privileges. If the user account does not have domain administrator privileges, you must create computer objects for Unity in the Active directory domain, and give the corresponding user account management access to the objects before joining the domain.

Requirement	Description
DNS alias for non-standard domain names	Use a DNS alias if the domain controller name starts with a digit, or contains nonstandard characters. If the name of the primary domain controller that you configure Unity to connect to starts with a digit, or contains nonstandard characters, you must set up an alias—made up of only standard characters—for the domain controller on the DNS server; standard characters include: (A-Z, a-z), digits (0-9), and hyphens (-). You must also add a resource record for the alias in the reverse DNS lookup zone. Later, when you configure the Unity Storage System to join the Microsoft Active Directory domain, you must specify the domain controller's alias, including its fully qualified domain name (FQDN), in the Domain Controller (optional) field. As an example, if the domain controller uses this name: **1MYDC_001.mydomain.lan**, 1. Create this alias for the domain controller on the DNS server: **MYDC-001** 2. Add a resource record for the alias in the reverse DNS lookup zone. 3. When configuring Unity to join the Microsoft Active Directory domain, specify the domain controller's alias, including its fully qualified domain name (FQDN), in the Domain Controller (optional) field: **MYDC-001.mydomain.lan**
Creation of machine accounts	The Microsoft Active Directory implementation must support the creation of machine accounts in the default Organizational Unit (OU).

Creating computer objects on the Active Directory server

In a typical deployment, Unity requires Domain Administrator privileges to join a Microsoft Active Directory domain. This process allows Unity to automatically create and configure computer objects for Unity on the Microsoft Active Directory server, without any manual intervention from a network administrator.

In some environments, specifying Domain Administrator credentials to integrate Unity with the Microsoft Active Directory Domain is not desirable, or possible. For these deployments, a network administrator can join Unity to a Microsoft Active Directory Domain using a user account with limited domain administrative privileges.

To allow this, you must manually perform configuration steps for creating and configuring computer objects for Unity on the Microsoft Active Directory server:

- Create a computer object(s) for Unity on the corresponding Active Directory Server for each controller node, as described in this procedure.
- Configure the attributes for the computer object(s) according to the settings described in this procedure.

⚠ **CAUTION: RISK OF OUTAGE**

Do not join Unity with Active Directory to Domain Controllers hosted on VMware. Domain Controllers used with Unity and Active Directory must either be a physical device or hosted externally to Unity.

▶ To create a computer object for a non-Administrator user account:

1. On the relevant Active Directory Server, add a new computer object for Unity, using each controller node's host name.

   CAUTION: When creating the computer object, make sure to enter the host name exactly as it is configured on Unity, or on each of its controller nodes.

   #### ▶ To obtain the host name for Unity controller nodes:

   a. Access the nxadmin CLI on Unity via SSH or remote console. Download and install an SSH client of your choice on a client machine that has network connectivity to Unity. You can use Putty, which is a (free) open source telnet and SSH client, available for download at this URL:

      http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

   b. Once you download and install an SSH client, launch it, and enter the IP address of a controller node.

   c. When the login prompt displays, type **nxadmin**, and press Enter.

   d. When you are prompted for the password, type the nxadmin (Nexsan Unity Administrator) password configured on Unity, and then press Enter. If you are connecting to a system that has not yet been configured using the Nexsan Unity System Configuration wizard—that is, an uninitialized Unity—you must type the default password for the nxadmin (Nexsan Unity Administrator) account: PASSWORD (all upper-case).

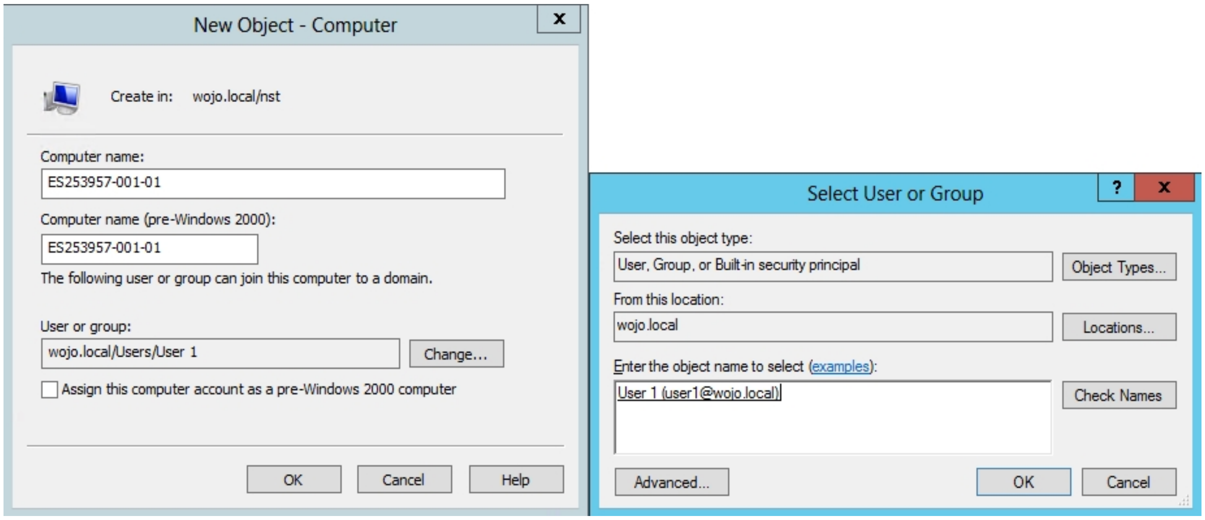
   e. On each controller node, run the `hostname` command.

   f. Take note of Unity host name; for example, `ES253957-001-01`.

2. Give the non-Administrator domain user account the ability to perform the operation for integrating Unity with the Active Directory Domain. You must give the non-Administrator domain user account the ability to join each controller node to the Active Directory Domain.

   It is important that you perform this step, since, by default, the privileges for joining a new computer object to the Active Directory Domain are automatically assigned to the Domain Administrator user/group account.

   Here is an example:



New Object - Computer

Create in: wojo.local/nst

Computer name: ES253957-001-01

Computer name (pre-Windows 2000): ES253957-001-01

The following user or group can join this computer to a domain.

User or group: wojo.local/Users/User 1

☐ Assign this computer account as a pre-Windows 2000 computer

Select User or Group

Select this object type: User, Group, or Built-in security principal

From this location: wojo.local

Enter the object name to select (examples): User 1 (user1@wojo.local)

3. Set the following attributes for the computer object that you added for Unity to the Active Directory Server. You must set these attributes separately for each controller node.

   CAUTION: Use the Active Directory Service Interfaces Editor (ADSI Edit) to set the attributes for the computer object(s). For each attribute, make sure to specify the value using the exact letter case, as shown.

Table 4-1: Computer object attributes

Attribute	Value to set...

dNSHostName	`<NESTHOSTNAME>.<domain name>`
	For example:
	`ES777666-001-01.qadomain.net`

msDS-SupportedEncryptionTypes	31
servicePrincipalName	● `cifs/<NESTHOSTNAME>.<domain name>` For example: `cifs/ES777666-001-01.qadomain.net` ● `host/<NESTHOSTNAME>.<domain name>` For example: `host/ES777666-001-01.qadomain.net` ● `HTTP/<NESTHOSTNAME>.<domain name>` For example: `HTTP/ES777666-001-01.qadomain.net` ● `nfs/<NESTHOSTNAME>.<domain name>` For example: `nfs/ES777666-001-01.qadomain.net` ● `root/<NESTHOSTNAME>.<domain name>` For example: `root/ES777666-001-01.qadomain.net` ● `host/<NESTHOSTNAME>` For example: `host/ES777666-001-01`

userPrincipalName	`host/<NESTHOSTNAME>.<domain name>@<DOMAINNAME>`
	For example:
	`host/ES777666-001-01.qadomain.net@QADOMAIN.NET`

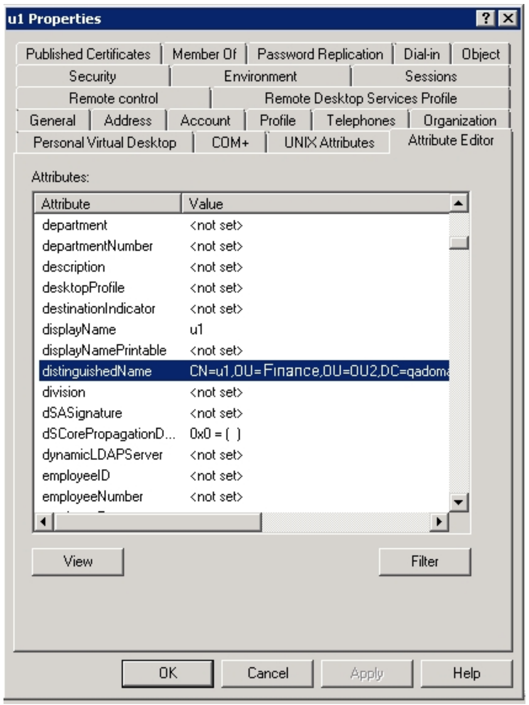
userAccountControl	4130

Note If the domain you are joining is `department.company.com`, make sure to use that whole name in *Step 7*.

4. In the **distinguishedName** attribute of the computer object, take note of the Organizational Unit names, in this format: *OU=name1,OU=name2*, etc. You will need this for *Step 7*.

   Note You can create a new OU at the root of the domain tree or use an existing user-defined OU.

   In the example below, you would use *OU=Finance,OU=OU2*.



Attribute	Value
department	<not set>
departmentNumber	<not set>
description	<not set>
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	u1
displayNamePrintable	<not set>
distinguishedName	CN=u1,OU=Finance,OU=OU2,DC=qadoma
division	<not set>
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
dynamicLDAPServer	<not set>
employeeID	<not set>
employeeNumber	<not set>

5. Repeat **step 3** above for the computer object that you added for the 2nd controller node.
6. Configure Unity using the Nexsan Unity System Configuration wizard (if not already configured).
7. Join Unity to the Microsoft Active Directory Domain in Nexsan Unity. See also Joining a Microsoft Active Directory domain on page 33

   Make sure you specify the user name and password for the non-Administrator domain user account that you granted the ability to perform the operation for integrating Unity with the Active Directory Domain.

   Make sure to use the same (whole) domain name as in *Step 3*.

   a. At the Configure User Authentication Mode step, click the **Advanced** button.
   b. Enter the Organizational Unit (OU) names obtained in *Step 4*.
   c. Select the **Use pre-defined computer objects** option.
   d. Click the **Apply** button.
8. After configuring Unity and successfully joining the system to the Microsoft Active Directory Domain, reset the **userAccountControl** attribute to **69632**—for each Unity computer object that you added to the Active Directory Server: DONT_EXPIRE_PASSWORD | WORKSTATION_TRUST_ACCOUNT.

Delegating control to a non-Administrator user account

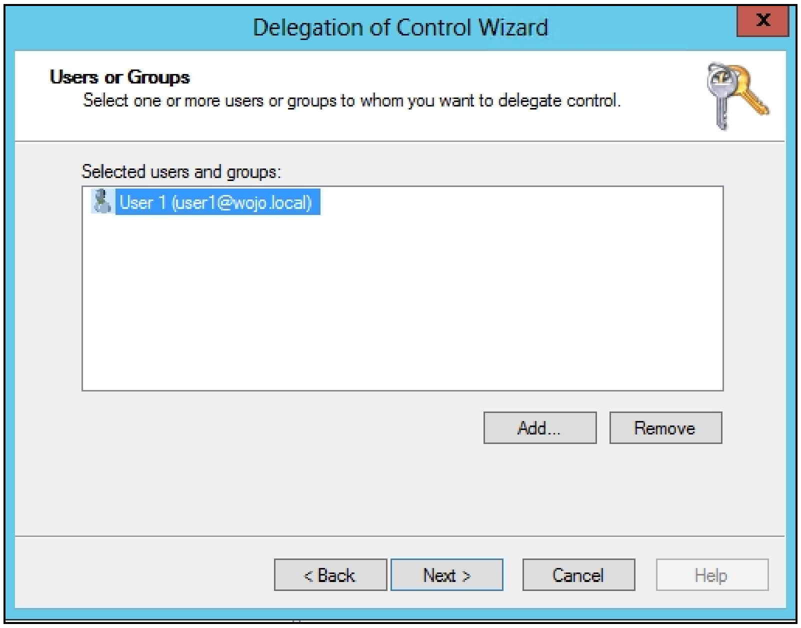
After creating a computer object in the Active Directory server, you must give full control to the non-Administrator user account for the selected Organization Unit (OU), so that this user can operate Unity in your Active Directory environment.

▶ **To delegate control:**

1. To open Active Directory Users and Computers:
    a. Click **Start** then select **Control Panel**.
    b. Double-click **Administrative Tools**.
    c. Double-click **Active Directory Users and Computers**.

   To open Active Directory Users and Computers in Windows Server 2012, click **Start**, and type `dsa.msc`.
2. In the console tree, right-click the organizational unit (OU) for which you want to delegate control, under *Active Directory Users and Computers\ domain node*.
3. Click **Delegate Control** to start the Delegation of Control wizard.
4. Click **Add** and select the non-Administrator user account used in the previous section. Click the **Next** button.

Figure 4-1: Active Directory - Delegation of Control wizard: select a user



Delegation of Control Wizard

Users or Groups

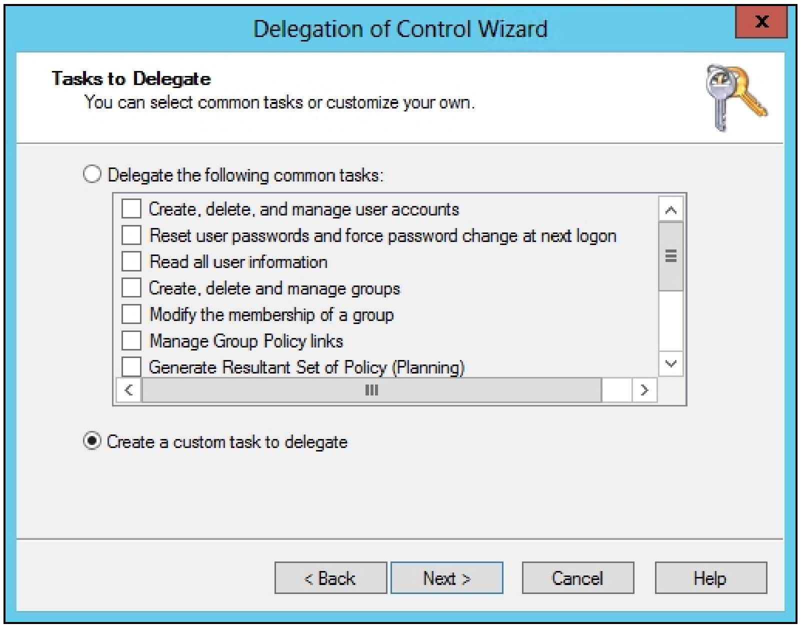
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

User 1 (user1@wojo.local)

5. Select **Create a custom task to delegate** and click the **Next** button.

Figure 4-2: Active Directory - Delegation of Control wizard: select tasks to delegate



Delegation of Control Wizard

Tasks to Delegate

You can select common tasks or customize your own.

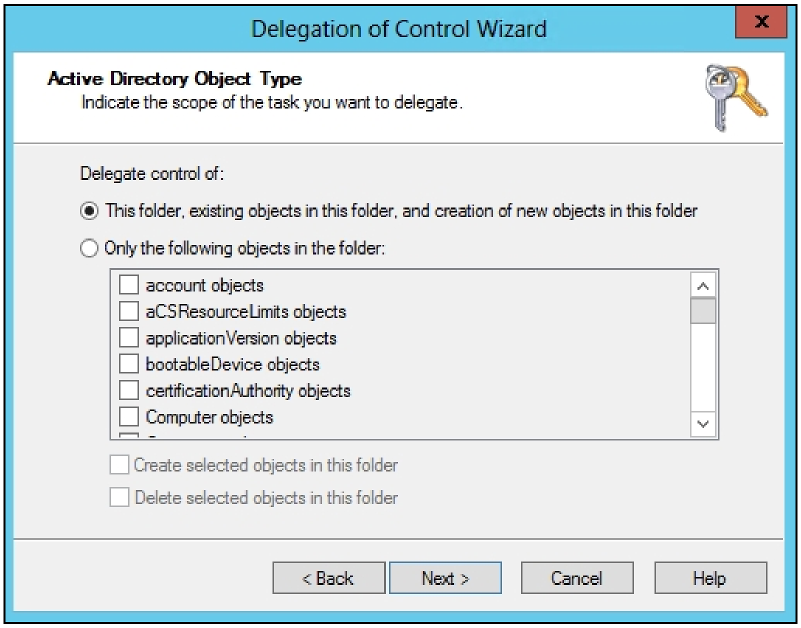
○ Delegate the following common tasks:

- ☐ Create, delete, and manage user accounts
- ☐ Reset user passwords and force password change at next logon
- ☐ Read all user information
- ☐ Create, delete and manage groups
- ☐ Modify the membership of a group
- ☐ Manage Group Policy links
- ☐ Generate Resultant Set of Policy (Planning)

● Create a custom task to delegate

6. Select **This folder...** and click the **Next** button.

Figure 4-3: Active Directory - Delegation of Control wizard: select the task scope



Delegation of Control Wizard

Active Directory Object Type

Indicate the scope of the task you want to delegate.

Delegate control of:

● This folder, existing objects in this folder, and creation of new objects in this folder

○ Only the following objects in the folder:

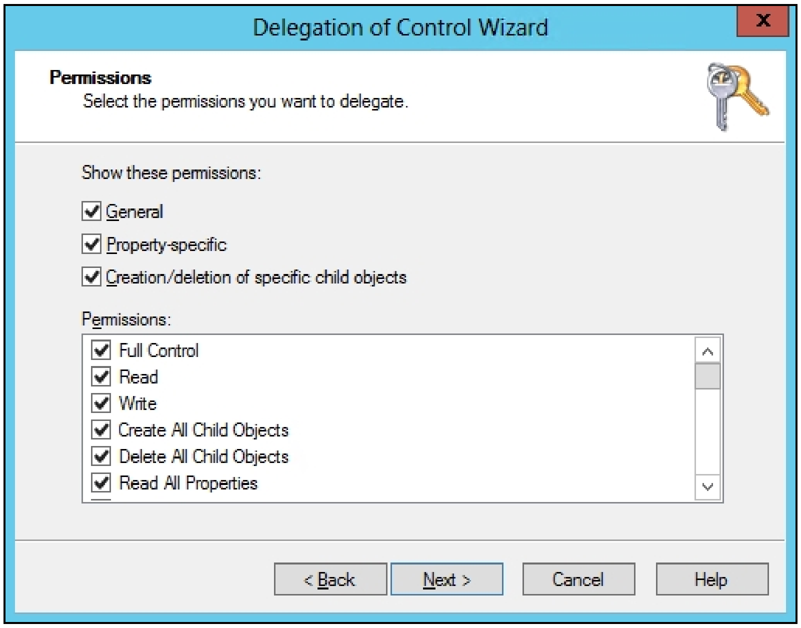
- ☐ account objects
- ☐ aCSResourceLimits objects
- ☐ applicationVersion objects
- ☐ bootableDevice objects
- ☐ certificationAuthority objects
- ☐ Computer objects

☐ Create selected objects in this folder

☐ Delete selected objects in this folder

7. Give **Full Control** access to the non-Administrator user account and click **Next**.

Figure 4-4: Active Directory - Delegation of Control wizard: select permissions



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

☑ Property-specific

☑ Creation/deletion of specific child objects

Permissions:

☑ Full Control

☑ Read

☑ Write

☑ Create All Child Objects

☑ Delete All Child Objects

☑ Read All Properties

8. Click **Finish**.

Joining a Microsoft Active Directory domain

The Unity Authentication service is preconfigured by default during initial system setup. Use this procedure if you want to instead join a Microsoft Active Directory domain.

CAUTION: If Unity is currently connected to a domain, and you subsequently join Unity to a new domain, all file system-level access permissions are also removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged.

However, when you rejoin the previous domain that Unity was connected to, or if the new domain has the same set of user and/or group accounts as the previous domain, Unity restores Site and Storage Pool Administrators, as well as all file system-level access permissions on the system.

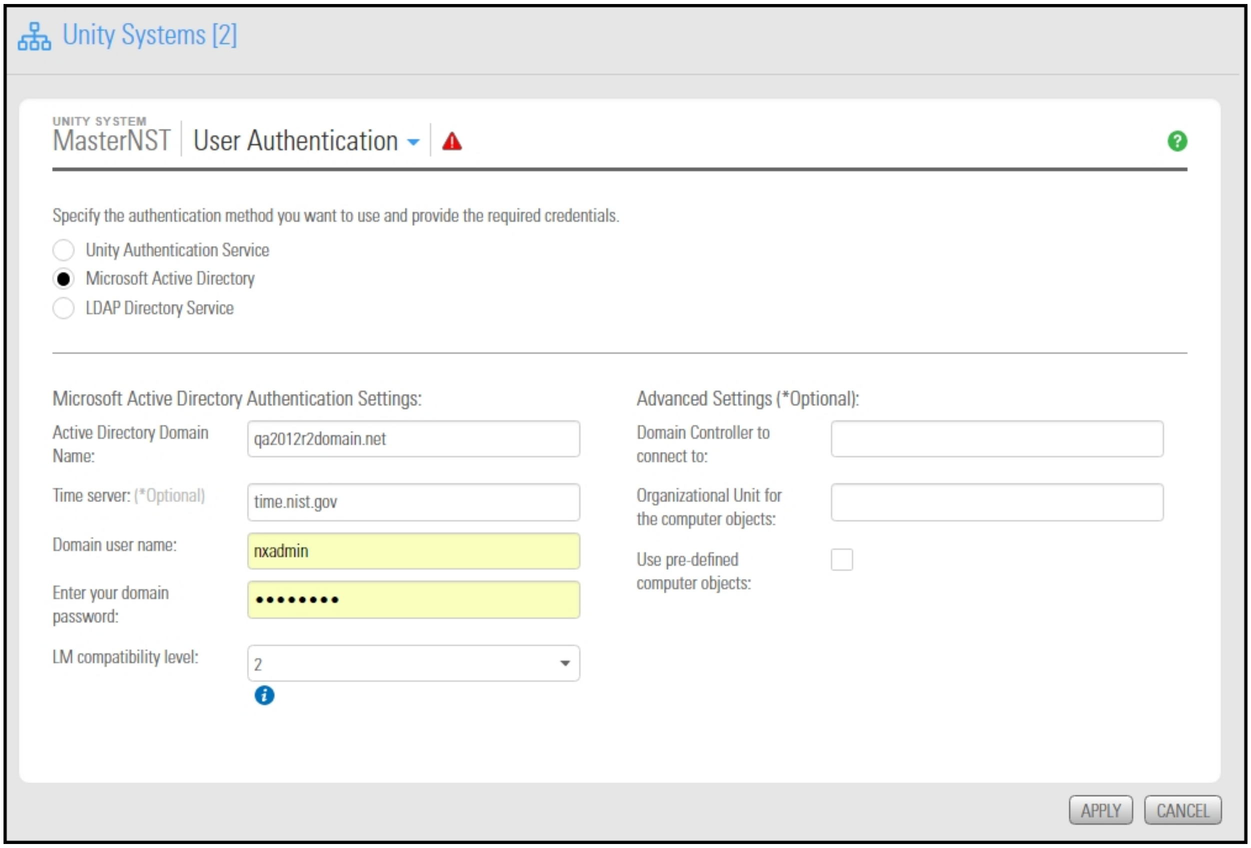
CAUTION: Joining a new domain or rejoining a former domain

If Kerberos is configured to access file systems, the Kerberos configuration gets disabled when unjoining a domain. After joining a new domain or rejoining an old domain, you must reconfigure Kerberos as described in Enabling Kerberos for accessing a CIFS file system on page 36.

▶ **Before you begin:**

Read the Microsoft Active Directory domain requirements on page 25.

Figure 4-5: Joining a Microsoft Active Directory domain



Specify the authentication method you want to use and provide the required credentials.

○ Unity Authentication Service
● Microsoft Active Directory
○ LDAP Directory Service

Microsoft Active Directory Authentication Settings:

Active Directory Domain Name: qa2012r2domain.net

Time server: (*Optional) time.nist.gov

Domain user name: nxadmin

Enter your domain password: ••••••••

LM compatibility level: 2

Advanced Settings (*Optional):

Domain Controller to connect to:

Organizational Unit for the computer objects:

Use pre-defined computer objects: □

▶ **To join a Microsoft Windows Active Directory domain:**

1. From the **System** menu, select **Unity Systems**.
2. Click **Summary** > **User Authentication**.

3. Select **Microsoft Active Directory**. The connection settings for Microsoft Active Directory display.
4. In the **Active Directory Domain Name** field, type the fully qualified domain name (FQDN) of the Microsoft Active Directory domain server that you want Unity to connect to.

   Note If you are integrating Unity in a multiple domain environment (Microsoft Active Directory forest implementation), and you want Nexsan Unity to display all users and groups from all domains, make sure to specify the domain name of the root, or top-level domain server of your network's Microsoft Active Directory implementation.
5. Optionally, in the **Time Server** field, type the IP address or the fully qualified domain name of the time server that you want Unity to synchronize its date and time with. A default time server is already defined.

   Note Unity supports multiple time servers: if you specify a time server in the **Time Server** field, we highly recommend that you specify at least two time servers; this ensures that date and time synchronization on Unity continues in the event that one of the time servers you specify is no longer available.

   To specify multiple time servers, use a comma to separate each entry, for example: `tick.utoronto.ca,time.nrc.ca`.
6. In the **Domain user name** and **Domain password** fields, type the user name and password of the domain administrator, or of a user that has administrative access to the Microsoft Active Directory server.

   For **LM compatibility level**, we recommend that you use the recommended level (2). The security level allows NTLMv1 client authentication, or NTLMv2 session security if the NFS server supports it. The Domain Controller accepts LM, NTLM, and NTLMv2 authentication.
7. Optionally, under **Advanced Settings**:
   - **Domain Controller to connect to**: If you are working in a multi-domain environment (that is, a Microsoft Active Directory forest implementation), enter the IP address of the domain controller in the field. This step may also be required if the fully qualified domain name (FQDN) of the Microsoft Active Directory domain server that you specify in the **Active Directory Domain Name** field does not resolve to the IP address of the domain controller that you want Unity to connect to.
   - **Organizational Unit (OU) for the computer objects**: Computer objects are stored under `Computers` by default. To change the default location where Unity adds its computer objects on your Active Directory server, enter Organizational Unit (OU) names in the format: `OU=NAME1,OU=NAME2`

     If the names do not exist, Unity will create them. If they already exist, the OU names are part of the existing **distinguishedName** attribute of the Organizational Unit (OU).

     Note IDMU is not supported in AD environments containing multiple top-level organizational units.
   - **Use pre-defined computer objects**: If you are joining the Active Directory domain with a user that has domain administrator privileges, you do not need to select this option. The Organizational Unit path you provide creates the computer objects. If you want to use the system defaults, check this option without entering a path.

     If you are joining the Active Directory domain with a user that does NOT have domain administrator privileges: you must select this option in addition to entering the OU path mentioned above to use computer objects already created on your Active Directory server.
8. Click the **Apply** button.

9. When the **Confirm DNS Settings** prompt appears, do one of the following:
    a. If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and click the **Apply** button, or
    b. If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to keep the current DNS settings.
10. When the **Domain controllers** window appears, select the primary and secondary controllers to be used for AD, and click the **Apply** button.
11. The wizard applies your settings and if all are successful, prompts you to click the **OK** button.

Note If you need to change your User Authentication method later,

- On the **Unity navigation bar**, select **System.**
- Click the link to the **Unity System** that you want to update.
- Select **Summary > User Authentication**.
- Make changes as required.

Joining a domain using the CLI

The `nxcmd Site JoinDomain` command enables you to join the Unity Storage System to an Active Directory domain. You can also use this command to switch from one domain to another.

⚠ **CAUTION:** If Unity is currently connected to a domain, and you subsequently join Unity to a new domain, allfile system-level access permissions are also removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged.

However, when you rejoin the previous domain that Unity was connected to, or if the new domain has the same set of user and/or group accounts as the previous domain, Unity restores Site and Storage Pool Administrators, as well as all file system-level access permissions on the system.

⚠ **CAUTION:** Joining a new domain or rejoining a former domain

If Kerberos is configured to access file systems, the Kerberos configuration gets disabled when unjoining a domain. After joining a new domain or rejoining an old domain, you must reconfigure Kerberos as described in Enabling Kerberos for accessing a CIFS file system on the facing page.

► **To run this command:**

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

```
nxcmd Site JoinDomain /Domain:<domain name> /User:<domain user name>
/Password:<domain user password>
[/BaseDomain:<base domain name>]
[/DomainController:<domain controller>]
[/PreferredDNSServer:<preferred domain name server IP>]
[/AlternateDNSServer:<alternate domain name server IP>]
[/CurrentDomainUser:<current domain user name>]
[/CurrentDomainPassword:<current domain user password>]
```

Site JoinDomain parameters	Description
/Domain	Specifies the name of the Microsoft Active Directory domain to join.
/User	Specifies the name of a user with access to the specified domain.
/Password	Specifies the password of that user to join the specified domain.
Optional parameters:	
/BaseDomain	Specifies the Organizational Unit (OU) for the computer objects. Enter the path of the OU; for example, CN=u1,OU=Computers,OU=OU2,DC=qadomain,DC=net
/DomainController	Specifies the IP address of the Active Directory domain controller.
/PreferredDNSServer	Specifies the IP address of the preferred DNS server in your network.
/AlternateDNSServer	Specifies the IP address of the alternate DNS server in your network.
/CurrentDomainUser	Refers to the user currently connected to the domain. This parameter is required if you are unjoining the current domain to switch to a different domain (as specified with the Domain parameter).
/CurrentDomainPassword	Refers to the password of the user specified in the CurrentDomainUser parameter. This parameter is required if you are unjoining the current domain to switch to a different domain.

▶ **Example:**

We join the qadomain using Bob Smith as domain administrator and bob!password as his domain password.

```
nxcmd Site JoinDomain /Domain:qadomain.net /User:bobsmith
/Password:bob!password
```

Enabling Kerberos for accessing a CIFS file system

To enable Kerberos support on Unity, you must perform these configuration tasks:

1. Add a Reverse Lookup Zone for the subnet of your Resource Groups in DNS Manager on your Active Directory domain.
2. Add a host in DNS Manager for each Resource Controller.
3. Configure the host in Active Directory Users and Computers.

Note Your Unity must have CIFS server version 2.1 to be able to use Kerberos.

Appendix A

Reverting to Unity Authentication

Use this procedure if you have the Microsoft Active Directory Service or LDAP Directory Service, and want to revert to the default Unity Authentication for your Unity Storage System. Unity is not connected to a user directory or authentication service on the network.

With Unity authentication, you create Unity user and group accounts for user authentication for operations with file systems and CIFS shares.

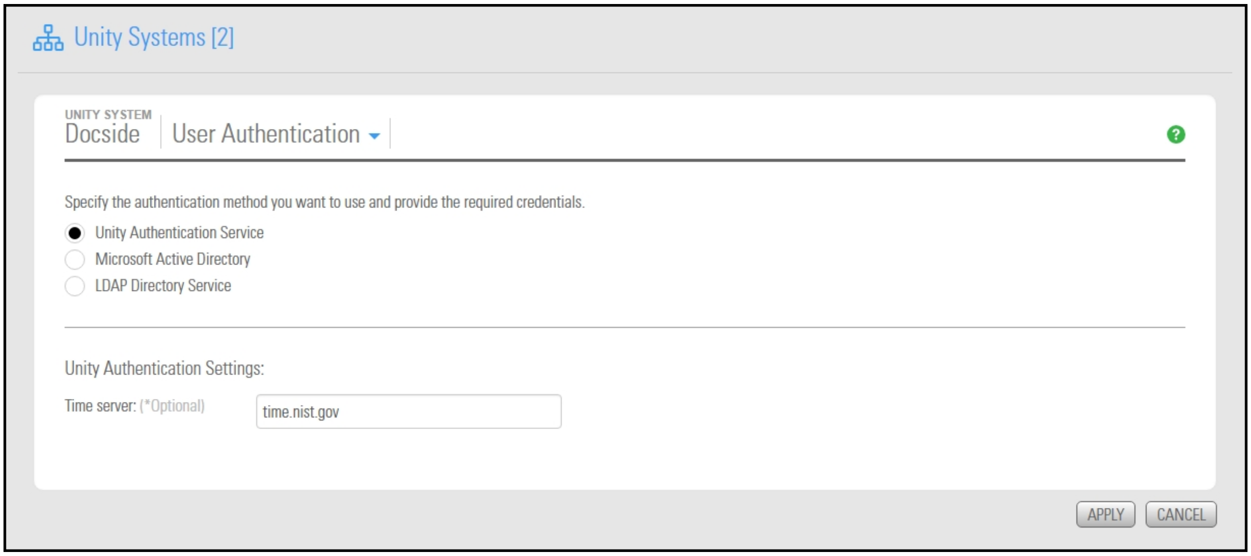
CAUTION: If Unity is currently connected to a domain, and you subsequently configure Unity authentication for the system, all file system-level access permissions are removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged.

When you rejoin the previous domain that Unity was connected to, Unity restores all file system-level access permissions on the system.

► **To revert to Unity Authentication:**

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Select the Unity System you want to change the authentication method for.
3. Select **Summary > User Authentication**.
4. Select **Unity Authentication Service**.

Figure A-1: Unity Systems panel—User Authentication view



Specify the authentication method you want to use and provide the required credentials.

● Unity Authentication Service
○ Microsoft Active Directory
○ LDAP Directory Service

Unity Authentication Settings:

Time server: (*Optional) time.nist.gov

5. Optionally, specify a time server in the **Time Server** field.
6. Click the **Apply** button.
7. When prompted confirm your DNS settings.
   - If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and then click the **Apply** button, or
   - If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to keep the current DNS settings.
8. Click **OK** to confirm.

A

Appendix B

Applicable NestOS commands

This section includes these topics:

domainname

▶ **To run this command:**

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays or sets the domain name used for NIS integration. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller

Run this command on both controllers.

Syntax

```
domainname
[<domain> | -s]
```

Options

`<domain>`

This is the domain name that you wish to assign for NIS integration.

`-s`

This option displays the current domain name.

Example

```
domainname -s
qadomain.net
```

setdefaultdomain

▶ **To run this command:**

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command defines the default domain used with your the Unity Storage System. You can create, remove, or show the default domain. This command can also be used for NIS domain integration. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller

You can run this command on any controller.

Syntax

```
setdefaultdomain [-d] [-s] [<domain name>]
```

Options

`-d`

This option deletes the current default domain.

`-s`

This option displays the current default domain.

`domain name`

This command sets the default domain to the domain name you specify.

Example

We change the default domain to **qadomain.net**.

```
setdefaultdomain qadomain.net
```

changenameservices

▶ **To run this command:**

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command defines the properties of naming services. You can add or remove switches, or show if the switch is configured.

For NIS integration, this command reconfigures the `etc/nsswitch.conf` file after changing the authentication mode in the user interface so that the NIS authentication settings are added to the password and group files. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller

Run this command on both controllers.

Syntax

```
changenameservices
-c <command>
-s <switch>
```

Options

`-c`

This option lets you run one of the following commands:

- `add`: Adds the specified switch to nameservices.
- `remove`: Removes the specified switch from nameservices.
- `show`: Shows whether or not the switch is configured.

`-s`

This option lets you specify a switch to run a command on. Currently, the only supported switch is `nis`, which is used for NIS integration.

Example

```
changenameservices -c add -s nis
Setting the current node...
Setting the peer node...
```

ypinit

▶ **To run this command:**

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command initializes the NIS client, including building a master NIS server database and a slave database on the NIS server. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller

Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax

```
ypinit [-c] [-m] [-s <master server>]
```

Options

```
-c
```

This command sets an NIS client. You must run the `ypinit -c` command whenever a new NIS server is added to the network or when an existing one is decommissioned.

Note: The `ypinit -c` command must be run on both controllers. This is required if you are integrating NIS with the Unity Storage System.

```
ypinit -m
```

This command builds a master server NIS database.

```
ypinit -s <master server>
```

This command builds a slave database on the NIS server. The Master Server must be the same server map name (or map nick name) returned by the `ipwhich` command.

Example

We create a slave database on the NIS master server.

```
ypinit - s nis.nisdomain2.lan
```

SVC

▶ **To run this command:**

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays all active services on the Unity Storage System.

Controller

You must run this command on both controllers.

Syntax

```
svc [show <service name> (default)]
svc [enable <service name>]
svc [disable <service name>]
svc [restart <service name>]
```

Options

```
show <service name> or (default)
```

This option displays the current status of the specified service. If you just type `show`, all services are displayed, including legacy, disabled, and enabled services.

```
enable <service name>
```

This option enables the specified service.

```
disable <service name>
```

This option disables the specified service.

CAUTION: Some services are dependent on other services to function properly. Only run this command if requested by Nexsan Technical Support.

```
restart <service name>
```

This option restarts the specified service.

CAUTION: Some services are dependent on other services to function properly. Restarting a service may affect other services.

Example

► **svc output excerpt:**

```
svc
legacy_run May_16 rc2_d/S05checkmem
legacy_run May_16 rc2_d/S12rebootnxrequired
legacy_run May_16 rc2_d/S13upgradenxversion
legacy_run May_16 rc2_d/S98nest
legacy_run May_16 rc2_d/S99rsf
legacy_run May_16 rc3_d/S98refreshidmapcache
legacy_run May_16 rc3_d/S99nest
disabled May_16 network/physical:nwam
disabled May_16 network/install:default
disabled May_16 system/install/config:default
disabled May_16 network/location:default
disabled May_16 network/ipsec/manual-key:default
online May_16 system/nxglassfishservice:default
online May_16 network/nfs/rquota:default
online May_16 network/nfs/server:default
online May_16 network/updateports-rpc:default
online 16:39:51 system/nest-discovery-server:default
online 10:55:30 network/ldap/client:default
online 10:55:30 milestone/name-services:default
online 10:55:30 system/filesystem/reparse:default
online 10:55:30 network/nfs/mapid:default
online 10:55:30 network/nfs/client:default
online 10:55:30 system/filesystem/autofs:default
online 10:55:32 network/nstcifs/client:default
online 14:38:00 network/nstcifs/server:default
```

ypcat

To run this command:

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays values from a NIS database in an NIS integration. Since `ypcat` uses the NIS network, you do not need to specify a NIS server. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller

Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax

```
ypcat [-k <key>] [-d <domain name>] [-t <map name>] [-x]
```

Options

```
-k <key>
```

This option displays the database values for the specified key.

```
-d <domain name>
```

This option specifies the domain name of the NIS server.

```
-t <map name>
```

This option inhibits the translation of database map nick names for the specified name. The name can be a map name or map nickname.

```
-x
```

This option displays the translation table for map nick names.

Example

We display the list of NIS users.

```
ypcat -k passwd
```

chmod

To run this command:

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command changes file permissions.

TIP: Use `helpacl` to view help on this command, as follows: `chmod helpacl`.

NOTE: This command is intended for advanced users, and thus should be used with caution.

Controller

Run this command on the controller where the files are located.

Syntax

```
chmod [-fR] absolute-mode file
chmod [-fR] symbolic-mode-list file
chmod [-fR] acl_operation file
chmod [-fR] [-@ named_attribute] attribute_specification_list
file
chmod [filesystems]
chmod [helpacl]
chmod [help]
```

Options

`-f`

This is the Force option. `chmod` does not complain if it fails to change the mode of a file.

`-R`

This option recursively descends through directory arguments, setting the mode for each file. When symbolic links are encountered, the mode of the target file is changed, but no recursion takes place.

`-@ named_attribute`

Performs the attribute operation on the named extended attribute file of each file operand instead of the file operand itself. If multiple `-@` operations are supplied, the attribute specification mode is applied to each of the named attribute files.

A named attribute of `*` carries meaning to `chmod`, and is considered to mean all extended attribute files associated with a file operand. This does not refer to the special files `.` and `..`.

A named attribute of `..` carries special meaning to `chmod`, and is considered to mean the file operand itself. This allows the command to apply the attribute specification mode to the specified named attribute file of the file operand and the file operand itself.

Absolute Mode

`chmod [-fR] absolute-mode file`

The `absolute-mode` argument is specified using octal numbers `nnnn` defined as `n`, a number from 0 to 7. An absolute mode is constructed from the OR of any of the following modes:

- `4000`: Sets user ID on execution.
- `20#0`: Sets group ID on execution if `#` is 7, 5, 3, or 1. Enables mandatory locking if `#` is 6, 4, 2, or 0. For directories, files are created with BSD semantics for propagation of the group ID. With this option, files and subdirectories created in the directory inherit the group ID of the directory, rather than of the current process. For directories, the setgid bit can only be set or cleared by using symbolic mode.
- `1000`: Turns on sticky bit.
- `0400`: Allows read by owner.
- `0200`: Allows write by owner.
- `0100`: Allows execute (search in directory) by owner.
- `0700`: Allows read, write, and execute (search) by owner.
- `0040`: Allows read by group.
- `0020`: Allows write by group.

- `0010`: Allows execute (search in directory) by group.
- `0070`: Allows read, write, and execute (search) by group.
- `0004`: Allows read by others.
- `0002`: Allows write by others.
- `0001`: Allows execute (search in directory) by others.
- `0007`: Allows read, write, and execute (search) by others.

Symbolic Mode

```
chmod [-fR] symbolic-mode-list file
```

The symbolic-mode-list argument is a comma-separated list (with no intervening white space) of symbolic mode expressions of the form:

`[who]` *operator* `[permissions]`

Operations are performed in the order given. Multiple permissions letters following a single operator cause the corresponding operations to be performed simultaneously.

- `who`: zero or more of the characters `u` (user's permissions), `g` (group's permissions), `o` (others' permissions), and `a` (all permissions for users, groups and others) specifying whose permissions are to be changed or assigned.
- `+`, – or `=` operator, signifying how permissions are to be changed:
  - `+`: Add permissions. If permissions are omitted, nothing is added. If `who` is omitted, adds the file mode bits represented by permissions, except for the those with corresponding bits in the file mode creation mask. If `who` is present, adds the file mode bits represented by the permissions.
  - `-`: Take away permissions. If permissions are omitted, do nothing. If `who` is omitted, clear the file mode bits represented by permissions, except for those with corresponding bits in the file mode creation mask. If `who` is present, clear the file mode bits represented by permissions.
  - `=`: Assign permissions absolutely. If `who` is omitted, clears all file mode bits; if `who` is present, clears the file mode bits represented by `who`. If permissions are omitted, does nothing else. If `who` is omitted, adds the file mode bits represented by permissions, except for the those with corresponding bits in the file mode creation mask. If `who` is present, add the file mode bits represented by permissions.

- The permission can be any compatible combination of the following letters. Permissions to a file can vary depending on your user identification number (UID) or group identification number (GID). Permissions are described in three sequences each having three characters rwx.
    - `l`: mandatory locking
    - `r`: read permission
    - `s`: user or group set ID
    - `t`: sticky bit
    - `w`: write permission
    - `x`: execute permission
    - `X`: execute permission if the file is a directory or if there is execute permission for one of the other user classes
    - `u`, `g`, `o`: indicates that permission is to be taken from the current user, group or other mode respectively.

ACL Operation

```
chmod [-fR] acl_operation file
```

An Access Control List (ACL) is a list of Access Control Entries (ACEs), each of which define access permissions for a particular class of user. The list of ACEs is numbered, starting from zero. The position of an ACE within an ACL is called an *index*. This index is used as an argument in many of the chmod commands described below.

An ACL operation ommand line has the following format:

```
chmod [options]A[index]- file ...
chmod [options]A-acl_specification file ...
chmod [options]A[index]{+|=}acl_specification file ...
```

Where `acl_specification` is a comma-separated list (with no intervening whitespace) of the form:

- `A[`*`index`*`]+`*`acl_specification`*: Prepends the access control entries (ACE) specified in acl_specification to the beginning of the file's ACL. Depending on the file system, the ACL can be reordered when applied to the file. If the optional index is specified, then new ACEs are inserted before specified index.
- `A-`: Removes all ACEs for current ACL on file and replaces current ACL with new ACL that represents only the current mode of the file.
- `A`*`index`*`-`: Removes ACE specified by index number.
- `A-`*`acl_specification`*: Removes ACEs specified by *acl_specification*, if they exist in current file's ACL.
- `A=`*`acl_specification`*: Replaces a files entire ACL with *acl_specification*.
- `A [`*`index`*`]=`*`acl_specification`*: Replaces ACEs starting at a specific index number in the current ACL on the file. If multiple ACEs are specified, then each subsequent ACE in acl_specification replaces the corresponding ACE in the current ACL.

The permissions argument is a (`/`) separated string of the following flags:

Note: Other flags may appear but are not supported.

- `read_data (r)`: Permission to read the data of a file.
- `list_directory (r)`: Permission to list the contents of a directory.
- `write_data (w)`: Permission to modify a file's data anywhere in the file's offset range.
- `add_file (w)`: Permission to add a new file to a directory.
- `add_subdirectory (p)`: Permission to create a subdirectory to a directory.
- `read_xattr (R)`: Ability to read the extended attributes of a file.
- `write_xattr (W)`: Ability to create extended attributes or write to the extended attribute directory.
- `execute (x)`: Permission to execute a file.
- `read_attributes (a)`: The ability to read basic attributes (non-ACLs) of a file.
- `write_attributes (A)`: Permission to change the times associated with a file or directory to an arbitrary value.
- `delete (d)`: Permission to delete a file.
- `delete_child (D)`: Permission to delete a file within a directory.
- `read_acl (c)`: Permission to read the ACL of a file.
- `write_acl (C)`: Permission to write the ACL of a file.
- `write_owner (o)`: Permission to change the owner of a file.

There are permissions aliases that set multiple flags using the following:

- `full_set`: All permissions.
- `modify_set`: All permissions except `write_acl` and `write_owner`.
- `read_set read_data, read_acl, read_attributes`, and `read_xattr`.
- `write_set write_data`, `append_data`, `write_attributes`, and `write_xattr`.

The inheritance argument is a `/` separated string of the following flags:

- `file_inherit (f)`: Inherit to all newly created files.
- `dir_inherit (d)`: Inherit to all newly created directories.
- `inherit_only (i)`: When placed on a directory, do not apply to the directory, only to newly created files and directories. This flag requires that either `file_inherit` and/or `dir_inherit` is also specified.
- `no_propagate (n)`: Indicates that ACL entries should be inherited to objects in a directory, but inheritance should stop after descending one level. This flag is dependent upon either `file_inherit` and/ or `dir_inherit` also being specified.

Attribute Operation

```
chmod [-fR] [-@ named_attribute] attribute_specification_list
file
```

The `attribute_specification_list` argument is the character `S` followed by a comma-separated list of one or more attribute_specifications. Each `attribute_` specification is of the form [operator]attribute_specifier.

An operator is one of the following:

- +: Each attribute specified by the associated attribute_specifier is adjusted to match the value specified by the attribute_specifier.
- -: Each attribute specified by the associated attribute_specifier is adjusted to match the inverse of the value specified by the attribute_specifier.
- =: Each attribute specified by the associated attribute_specifier is adjusted to match the value specified by the attribute_specifier. Any boolean read-write extended system attributes associated with the current file that are not specified by attribute_specifier is cleared.

If an operator is not specified in an attribute_specification, chmod behaves as if + had been specified.

An attribute_specifier takes one of the following values:

- a: Sets all boolean read-write extended system attributes associated with the current file.
- c[*compact_attribute_setting*]: Sets each boolean read-write extended system attribute identified by compact_attribute_list. A compact_attribute_list is a list of zero or more adjacent attribute abbreviation characters from list of Attribute Names and Abbreviation Characters later in this section. An arbitrary number of hyphen (-) characters can be included in a compact_attribute_list. These are ignored.
- v[*verbose_attribute_setting*]: Sets each boolean read-write extended system attribute identified by verbose_attribute_setting. A verbose_attribute_setting is an attribute name from the list of Attribute Names and Abbreviation Characters later in this section, optionally, immediately preceded by no. If the attribute name is used without no, the attribute is set; otherwise the attribute is cleared.
- A verbose_attribute_setting_list is zero or more comma-separated verbose_attribute_settings.

Multiple operations specified for a file are accumulated and are all set for a file operand as a single attribute setting operation. If an attribute is specified more than once in an attribute_specification_list, the last specified operation is applied.

List of Attribute Names and Abbreviation Characters:

- hidden (H)
- sparse (s)
- system (S)
- readonly (R)
- archive (A)
- nounlink (u)
- immutable (i)
- appendonly (a)
- nodump (d)

- `av_quarantined (q)`
- `av_modified (m)`

file systems

Displays all Unity Storage System file systems and their folders. To change permissions on a file system, you must enter the exact path of the file system; for example, `/pools/pool name/file system name`.

`helpacl`

Displays the complete help for the `chmod` command.

`help`

Displays the basic help for the `chmod` command.

Example

To display the Unity Storage System's file systems:

```
chmod file systems
```

```
File system              Node      Folder
s2p1                     1         /pools/p1/s2p1
```

To change permission on a file in a file system:

```
chmod o+x /pools/pool1/filesystem1/file1
```

nstusermaps

To run this command:

1. Access the CLI command shell.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to map local users to Microsoft Active Directory users.

Controller

Run this command on both controllers for changes to take effect.

Syntax

```
nstusermaps
[-f <command file>]
[add [-d] <name 1> <name 2>...
[dump [-n] [-v]
[export [-f <file name>] <format>]
[flush [-a]]
[get-namemap <name>]
[help]
[import [-F] [-f <file name>] <format>]
[list]
[remove [-a] | [-f|-t <name>] | [-d <name 1> <name2>...]]
```

```
[set-namemap [-a <authentication method>] [-D <bind DN>]
[-j <password file>] <name 1> <name 2>
```

```
[show [-c] [-v] identity <target type>]
```

```
[unset-namemap [-a <authentication method>] [-D <bind DN>]
[-j <password file>]
```

Options

`[-f <command file>]`

This option reads and executes sub-commands from the specified command file. The `nstusermaps -f` command reads from standard input.

`add [-d] <name 1> <name 2>`

This command creates a mapping to the corresponding user or group account in the Microsoft Active Directory domain.

```
nstusermaps add -d <windowsuser@AD.net> <unixusername>
```

`dump [-n] [-v]`

This command displays identity mapping information for users and groups existing on the Unity Storage System. It show the user or group SID (security ID) and the corresponding GID and UID.

- `-n` displays the Windows group maps.
- `-v` displays Windows group security IDs (SID) and their corresponding GIDs.

`export [-f <file name>] <format>`

This command exports user maps to the specified file and format.

`flush [-a]`

Flushes the identity mapping cache so that future mapping requests will be fully processed based on the current rules and directory information. This is a non-disruptive operation. A rule change automatically flushes the cache; this manual operation can be used to force newly changed directory information to take effect.

`get-namemap <name>`

This option displays the directory-based name mapping information from the specified name. The name can be a AD or native LDAP user or group object.

`help`

This command displays the help for the `nstusermaps` command.

`import [-F] [-f <file name>] <format>`

This command imports user maps from the specified file and format. The `-f` file option reads the rules from the specified file. The `-F` option flushes existing name-based mapping rules before adding new ones.

`list`

This command displays existing user idmaps. If there is no idmap, there is no output.

```
remove [-a] | [-f|-t <name>] | [-d <windowsuser@AD.net>
<unixusername>]
```

This command removes a mapping from the corresponding user or group account in the Microsoft Active Directory domain. Use `-a` to remove all mapping information.

```
set-namemap [-a <authentication method>] [-D <bind DN>] [-j
<password file>] <windowsusername> <unixusername>
```

This option sets name mapping information in the AD or native LDAP user or group object.

You can use these arguments with `set-namemap`:

- `-a` specifies the authentication method when modifying native LDAP entry. The default value is sasl/GSSAPI.
- `-D` uses the distinguished name to bind to the directory.
- `-j` specifies the file containing the password for authentication to the directory.

```
show [-c] [-v] identity <target type>
```

This option shows the identity of type, target-type, that the specified name maps to. If you do not specify the target type, the non-diagonal mapping is shown. By default, it shows only mappings that have been established already.

- `-c` forces the evaluation of name-based mapping configurations or the dynamic allocation of IDs.
- `-v` shows how the mapping was generated and also whether the mapping was just generated or was retrieved from the cache.

```
unset-namemap [-a <authentication method>] [-D <bind DN>] [-j
<password file>]
```

This option unsets directory-based name mapping information from the specified name and optional target type. The name can be AD or native LDAP user or group object.

Example 1

We map `Bob Summer`'s Microsoft Active Directory domain account to the account created for `Bob` on the Unity Storage System

```
nstusermaps add winuser:<bob.summers@AD.net> unixuser:<bsummers>
```

Example 2

We display user maps to view GIDs and UIDs.

```
nstusermaps dump
```

```
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
gid:2147483789

usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
uid:2147483649

gsid:S-1-5-21-3198797834-3143126336-2597567724-513 ==
gid:2147483650

gsid:S-1-5-2 == gid:2147483651
```

Example 3

We display Windows group GID and UID.

```
nstusermaps dump -n
```

```
wingroup:Domain Users@ES260786-176-01 == gid:2147483650

wingroup:Network == gid:2147483651

wingroup:Guests@BUILTIN == gid:2147483652
```

```
winuser:Guest@es260786-176-01.qadomain.net == gid:2147483790
winuser:Guest@ES260786-176-01 == uid:2147483649
```

Example 4 We display Windows group security IDs (SID) and their corresponding GIDs.

`nstusermaps dump -v`

```
gsid:S-1-5-21-3198797834-3143126336-2597567724-513 ==
gid:2147483650
Method: Ephemeral
gsid:S-1-5-2 == gid:2147483651
Method: Ephemeral
gsid:S-1-5-32-546 == gid:2147483652
Method: Ephemeral
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
gid:2147483790
Method: Ephemeral
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
uid:2147483649
Method: Ephemeral
```

Nexsan Headquarters

325 E. Hillcrest Drive, Suite #150
Thousand Oaks, CA 91360
United States of America

Nexsan Shipping

302 Enterprise Street , Suite A
Escondido, CA 92029
United States of America

Nexsan Unity Documents & Downloads page:
https://helper.nexsansupport.com/unt_support

Worldwide Web
www.nexsan.com

Document Reference: 20190927PM014858

Nexsan Canada

1405 Trans Canada Highway, Suite 300
Dorval, QC H9P 2V9
Canada

Nexsan UK

Units 33–35, Parker Centre, Mansfield Road
Derby, DE21 4SZ
United Kingdom

Nexsan Unity support:
https://helper.nexsansupport.com/unt_support