

IBM Storwize V7000 Unified 1.4 Authentication

The how-to guide

*Ulf Troppens, Pankaj Ahire, Varun Mittal,
Kaustubh Katruwar, and Saurabh Gawande*

IBM Systems and Technology Group ISV Enablement

November 2012

Table of contents

Abstract.....	3
Document Source	3
Changes in the document since previous document release.....	3
Introduction.....	3
Basic concepts.....	4
Identification and ID mapping.....	4
Authentication.....	5
Directory service.....	6
Authorization.....	8
Storwize V7000 Unified authentication.....	9
Storwize V7000 Unified with AD.....	13
Microsoft AD.....	13
Microsoft AD with SFU.....	18
Microsoft AD with NIS.....	24
Storwize V7000 Unified with NT4 / Samba PDC.....	30
Which ID mapping methods are available for NT4 / Samba PDC?.....	30
NT4 / Samba PDC.....	30
NT4 / Samba PDC with NIS.....	33
Storwize V7000 Unified with LDAP.....	38
Which ID mapping methods are available for Storwize V7000 Unified with LDAP.....	38
LDAP.....	39
Secure LDAP.....	43
Secure LDAP and MIT Kerberos.....	48
Storwize V7000 Unified with Local Authentication.....	54
Netgroup basic concepts.....	60
What are netgroups.....	60
Where are netgroups maintained?.....	60
Storwize V7000 Unified storage support for netgroups.....	60
Configuration for authentication none and ID mapping none.....	60
Configuration for AD authentication and auto ID mapping	61
Configuration for AD authentication and NIS ID mapping	62
Configuring authentication AD and ID mapping SFU.....	63
Configuring authentication LDAP and id mapping LDAP.....	64
Options in absence of external authentication server.....	66
Limitations.....	67
Summary.....	70
Resources.....	71
About the authors	72
Trademarks and special notices.....	73

Abstract

This white paper explains the basic concepts of user management of UNIX, Microsoft Active Directory (AD), and UNIX netgroups and their application to IBM Storwize V7000 Unified storage system. The target audience of this white paper includes IT architects and system administrators who can plan and configure authentication and netgroups of the Storwize V7000 Unified system.

Document Source

The location of the official version of this controlled document is at:

<http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004060>

Readers are requested to refer to the latest document from this location always.

Changes in the document since previous document release

Storwize V7000 Unified Local Authentication
Choosing idMapConfig Options
Limitations

Introduction

This paper explains the different authentication methods supported by the IBM® Storwize® V7000 Unified system with detailed information on when to select a particular authentication method along with the prerequisites, step-by-step setup procedure, and limitations of each authentication configuration. It also describes the basics of user authentication, authorization, ID mapping and directory service.

The primary authentication methods include:

- Microsoft® Active Directory (AD) server
 - With or without Services for UNIX® (SFU) / Subsystem for UNIX-based Application (SUA)
 - With or without Network Information Service (NIS)
- Samba primary domain controller (PDC)
- Lightweight Directory Access Protocol (LDAP) with:
 - Secure communication using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
 - Secure SSL/TLS and Kerberos
- Local Authentication

This paper also describes the basics of netgroup and the different configuration with which it is supported with IBM Storwize V7000 Unified storage system. This paper also provides an example how to configure netgroup stored with Network Information Server (NIS) capabilities with the IBM Storwize V7000 Unified system.

This paper does not deal with upgrade and maintenance of IBM Storwize V7000 Unified.

Basic concepts

Identification and ID mapping

What is identification?

The objective of identification is to identify users and infrastructure components. Identification methods includes unique user IDs (for example, different people use different Storwize V7000 Unified admin IDs), keys or finger prints (for example, public SSH key) and digital certificates (for example, certificate of web server).

What are user names and user identifier (UID)?

UNIX system and UNIX-based appliances such as Storwize V7000 Unified systems use user names and UIDs to represent users of the system. The user name is typically a human readable sequence of alphanumeric characters and the UID is a positive integer value. When users log in to a UNIX system, the operating systems looks up the UID and then uses this UID for further representation of the user.

User names, UIDs, and the mapping of user names to UIDs are stored locally in the `/etc/passwd` file or on an external directory service such as AD, LDAP, or NIS.

What are group names and group identifier (GID)?

UNIX systems use groups to maintain sets of users having the same permissions to access certain system resources. Similar to user names and UIDs, a UNIX system also maintains group names and GIDs. A UNIX user can be member of one or more groups, where one group is the primary or default group. UNIX groups are not nested; they contain users only but not other groups.

Group names, GIDs, the mapping of group names to GIDs, and the membership of users to groups are stored locally in the `/etc/group` file or on an external directory service such as AD, LDAP or NIS. The primary group of an user is stored in `/etc/passwd` or in an external directory service.

What are resource names and security identifier (SID)?

Microsoft Windows® system refers all operating system entities as resources, including users, groups, computers and other resources. Each resource is represented by an SID. Windows groups may be nested, for example, one group might include one or more users, or groups, or both.

Resource names and SIDs are stored locally in the Windows registry or in an external directory service such as Active Directory or LDAP.

What is UID / GID / SID mapping?

The Storwize V7000 Unified system stores user file data on IBM General Parallel File System (IBM GPFS™), which uses UIDs and GIDs for access control.

For CIFS access, Storwize V7000 Unified needs to map Windows SIDs to UNIX UIDs and GIDs to enforce access control.

Network File System (NFS) clients send UID and GID of a user who requests access to a file. Storwize V7000 Unified uses Linux® default access control mechanism by comparing the received UID and GID with the UIDs and GIDs stored in GPFS.

The UIDs and GIDs used by the NFS clients must match the UIDs and GIDs stored inside GPFS.

For HTTP, HTTPS, SFTP and SCP access, Storwize V7000 Unified requires users to authenticate through a valid user name. Storwize V7000 Unified needs to map the user name to one UID and one or more GIDs for GPFS access control.

Authentication

What is authentication?

The objective of authentication is to verify the claimed identity of users and components. Authentication methods include the use of passwords and the exchange of digital keys.

What is UNIX authentication?

UNIX authentication is machine based. A user uses the user name and a credential (for example password, private SSH key) to logon on a UNIX workstation. The workstation looks up the user's UID, GID and credential in local files or an external directory service, such as LDAP, and then verifies the received credential. The information for credential verification might be stored locally (for example, hashes of passwords are stored in /etc/shadow, public SSH keys are stored in the ssh/authorized_key file) or for external directory service (such as LDAP).

After successfully logging on a UNIX server, the user is trusted not only on this server but also by all other servers which trust this server. For instance, for file sharing through the NFSv3 protocol, a Storwize V7000 Unified administrator creates a Storwize V7000 Unified network-attached storage (NAS) export and grants access to the user's workstation. For NAS access, the UNIX NFSv3 client running on the user's workstation just sends the user's UID with each file access request and the NFSv3 server running on the Storwize V7000 Unified system considers this UID as authenticated, assuming that the workstation correctly authenticated the user's UID.

What is Windows authentication?

Windows authentication is session based. A user logs on to a Windows workstation using the user name. The workstation then looks up the user's SID in the local Windows registry or on the Windows domain controller and then verifies the received credential. The information for credential verification might be stored locally (for example, in the Windows registry) or on the external Windows domain controller (for example, Active Directory).

After successful logon to a Windows server, the user is trusted on this server, but the user still must authenticate to other services in the network before the user can access them. For instance, for file sharing through the Windows CIFS protocol, a Storwize V7000 Unified administrator creates a Storwize V7000 Unified NAS export, and a Windows administrator customizes the GPFS NFSv4 access control list (ACL) of this NAS export to grant the user access to this new NAS export. For NAS access, the CIFS

client running on the user's workstation sends an authentication request to an authentication server (for example, Active Directory). The authentication server checks if the requesting user is allowed to use the service and then returns a session credential that is encrypted with the key of the CIFS server to the CIFS client. The CIFS client sends the session credential to the CIFS server running on the Storwize V7000 Unified system. The CIFS server decrypts the session credential and verifies its content. After the session credential is verified, the CIFS server knows that the user was authenticated and authorized by the authentication server. The session credential also allows the CIFS server to identify the user.

How to integrate UNIX and Windows authentication?

To provide heterogeneous file sharing for UNIX and Windows, Storwize V7000 Unified must support the authentication methods for UNIX and Windows. Storwize V7000 Unified uses Windows authentication for the incoming CIFS connections and UNIX authentication for incoming NFS, HTTP, SFTP, and SCP connections.

What is Kerberos?

Kerberos is a network authentication protocol for client/server applications by using symmetric key cryptography. User passwords are never sent over network. The Kerberos server grants a ticket to the client for a short span of time. This ticket is used while communicating with the server to get access to the service (for example, a file server).

Windows-based authentication is based on Kerberos. The Massachusetts Institute of Technology (MIT) Kerberos, a free implementation of the Kerberos protocol provided by the MIT, is used in Storwize V7000 Unified.

Directory service

What is a directory service?

Storing user and group information in local files works well for small organizations which operate only a very few servers. Whenever a user is added or deleted, the group membership is changed, or a password is updated, this information must be updated on all servers. Storing this information in local files does not scale for large organizations having tens, hundreds, or thousands of users which need selected access to hundreds or thousands of servers and services.

Directory services store and maintain user and group information centrally on an external server. Other servers such as workstations and Storwize V7000 Unified systems look up this information in the directory server instead of storing this information in local files.

What is Microsoft Active Directory (AD)?

Active Directory (AD) is a technology created by Microsoft and introduced since Microsoft Windows 2000 which provides many services including following key network services:

- Directory Service
- Kerberos-based authentication
- Domain Name System (DNS)

What is Services for UNIX (SFU) / Subsystem for UNIX-based Application (SUA)?

SFU/SUA is a Microsoft Windows component that provides interoperability between Microsoft Windows and UNIX environments. Storwize V7000 Unified uses SFU/SUA primarily for UID/GID to SID mapping.

In a typical environment for a Microsoft Windows 2003 Server , SFU 3.5 (available on Microsoft site on download) is to be installed separately.

On Windows Server 2003 R2 and higher version, the rfc2307 compliant schema is installed by default. Generally, to manage the unix attributes, Identity Management for Unix (available with the installation) may be enabled.

What is Lightweight Directory Access Protocol (LDAP)?

LDAP is a directory service access protocol over the TCP/IP network. LDAP is a lightweight alternative to the traditional Directory Access Protocol (DAP), and therefore it is called LDAP.

The latest version of LDAP is version 3 and is specified in series of Internet Engineering Task Force (IETF) standard track Request for Comments (RFCs) as mentioned in RFC 4510.

LDAP directory is usually structured hierarchically, as a tree of nodes. Each node represents an entry within the LDAP database. A single LDAP entry might consists of multiple attribute-value pairs, and is uniquely identified by a distinguished name.

For details about LDAP Directory structure refer - <http://www.openldap.org/doc/>

What is Local Authentication?

Local Authentication is the authentication facility provided in Storewize V7000 Unified, to be used in cases where there is no external authentication server available. The user and group data will be maintained locally on Storewize V7000 Unified.

What is Network Information Service (NIS)?

NIS is a directory service protocol for centrally storing configuration data of a computer network. NIS protocols and commands were originally defined by Sun Microsystems; the service is now widely implemented by other vendors. Originally called Yellow Pages (YP), some of the binary names still start with yp.

The original NIS design was seen to have inherent limitations, specifically in the areas of scalability and security. Therefore, modern and secure directory systems (primarily LDAP) are used as alternatives.

The NIS information is stored in NIS maps, typically providing the following primary information:

- Password-related data similar to data stored in /etc/passwd
- Group-related data similar to data stored in /etc/group
- Network configuration, such as netgroups

What is Microsoft Windows NT 4.0 Domain Controller (NT4) / Samba Primary Domain Controller (PDC)?

A domain is a concept introduced in Windows NT where a user might be granted access to a number of computer resources with the use of user credentials. A Domain Controller (DC) is a server that responds to security authentication requests and controls access to a variety of computer resources. Microsoft Windows 2000 and higher versions introduced Active Directory, which largely eliminated the concept of PDC and backup domain controller (BDC).

PDCs are still used by customers. The Samba software can be configured as PDC and customers can run Samba on Linux, acting as PDC. The Samba4 project has the goal to run Samba as AD server.

Authorization

What is authorization?

The objective of authorization is to grant or deny access to an already authenticated identity (for example Storwize V7000 Unified NAS user, Storwize V7000 Unified administrative user, IBM service personnel) to resources (for example, to read a file stored on Storwize V7000 Unified, run a privileged command, and so on).

What is access control?

The objective of access control is to assure that only authenticated and authorized identities get access to certain resources. Access control must prevent unauthorized access (for example, reject the running of a Storwize V7000 Unified CLI command or reject read access of a Storwize V7000 Unified user to a file stored on Storwize V7000 Unified which is owned by another user).

What is an access control list (ACL)?

Generally, an ACL is a list of permissions which is attached to a resource. An ACL describes the identities that are allowed to access (for example, read, write, and execute) the respective resource. ACLs are the built-in access control mechanism of UNIX and Windows systems. Storwize V7000 Unified uses the Linux built-in ACL mechanism for access control to files that are stored on GPFS.

What are GPFS NFSv4 ACLs?

There are a broad range of ACL formats which differ in syntax and semantics. The ACL format defined by NFSv4 is called NFSv4 ACL. GPFS ACLs implement the NFSv4 style ACL format; they are also referred to as GPFS NFSv4 ACL. Storwize V7000 Unified system stores all user files in GPFS. The GPFS NFSv4 ACLs are used for access control of files stored on Storwize V7000 Unified.

The implementation of NFSv4 ACLs in GPFS does not imply that GPFS or Storwize V7000 Unified support the full NFSv4 protocol at the time of this publication:

What are POSIX bits?

The POSIX bits of a file are a different way the specify access permissions to files. UNIX file systems allow you to specify the owner and the group of a file. The POSIX bits of a file allow you to configure access control for the owner, the group, and for all other users to read, update, or run the file. POSIX bits are less flexible than ACLs.

Note: The change of the POSIX bits of a GPFS file system can trigger a modification of its GPFS NFSv4 ACL. As Storwize V7000 Unified uses GPFS NFSv4 ACLs for access control, Storwize V7000 Unified administrators and IBM service personnel should never change the POSIX bits of files stored on GPFS.

What is ACL mapping?

GPFS NFSv4 ACLs and CIFS ACLs are not compatible. For instance, CIFS supports unlimited nested groups, which is not fully supported by GPFS NFSv4 ACLs. Storwize V7000 Unified can map only certain CIFS ACLs to GPFS NFSv4 ACLs, which results in some limitations. It is a known limitation that in this aspect current Storwize V7000 Unified is not fully compatible with CIFS ACLs.

Refer to the Storwize V7000 Unified Information Center for all the Authorization limitation details at:

http://pic.dhe.ibm.com/infocenter/storwize/unified_ic/topic/com.ibm.storwize.v7000.unified.140.doc/mng_t_auth_configure_integ.html

Storwize V7000 Unified authentication

What are the elements of Storwize V7000 Unified authentication configuration?

The elements include:

- Configuration of directory service
- Refinement of ID mapping (optional)
- Configuration of other authentication elements

Which authentication methods are supported by Storwize V7000 Unified?

Storwize V7000 Unified supports the following authentication methods:

- Microsoft AD
- Microsoft AD and SFU
- LDAP
- LDAP with MIT Kerberos
- NIS
- Microsoft Windows NT 4.0 Domain Controller (NT4) / Samba PDC
- Local Authentication

Which other authentication elements are supported by Storwize V7000 Unified?

Storwize V7000 Unified supports the following other authentication elements:

- **netgroups**
A netgroup is a group of hosts used to restrict access for mounting NFS exports on a set of hosts and deny mounting on the rest of the hosts.
- **Kerberos**
In general, user authentication is done by sending user credentials over the network in a

clear text format, which introduces a security risk. Kerberos reduces this risk by not sending credentials over the network. Storwize V7000 Unified supports Kerberos with AD (mandatory) and LDAP (optional).

- **SSL or TLS**

The SSL or TLS protocols are primarily used to increase the security and integrity of data being sent to directory service over the network. These protocols are based on public-key cryptography and uses digital certificates based on X509 for identification. Storwize V7000 Unified supports SSL- or TLS-based communication with LDAP.

Which are the different authentication and ID mapping configurations supported by Storwize V7000 Unified?

The different authentication and ID mapping configurations supported by Storwize V7000 Unified are listed in the following table. You can click a section name to navigate to the corresponding section for more details.

Authentication	ID mapping	When to Choose this Authentication Option	Section
Active Directory	Auto	• Customer uses Microsoft Active Directory (AD) to store user information and user passwords. • Customer does not use SFU. • Customer does not plan to use Storwize V7000 Unified remote replication. • Customer does not plan to use any unix clients for data access or use Unix user credentials.	“Microsoft AD”
Active Directory	SFU	• Customer uses Microsoft AD to store user information and user passwords. • Customer plans to use NFS along with CIFS for NAS access. • Customer plans to use Storwize V7000 Unified remote replication.	“Microsoft AD with SFU”
Active Directory	NIS	• Customer uses Microsoft AD to store user information and user passwords. • Customer plans to use NFS for NAS access. • Customer does not plan to use the Storwize V7000 Unified remote replication. • User and group IDs are stored and managed in NIS.	“Microsoft AD with NIS”
NT4/ Samba PDC	Auto	• Customer uses Samba PDC to store user information and user passwords.	“NT4 / Samba PDC”

		• Storwize V7000 Unified is used with the environment having legacy Windows 2000 and NT4 domain users.	
NT4 / Samba PDC	NIS	• Customer uses Samba PDC to store user information and user passwords. Samba can serve as a NT4 server when configured as a PDC. • Customer plans to use NFS for NAS access. • Customer does not plan to use Storwize V7000 Unified remote replication. • User ID are stored and managed in NIS.	“NT4 / Samba PDC with NIS”
LDAP	LDAP	• Storwize V7000 Unified will be used in an IT infrastructure where LDAP is used as a Directory service and all user information is maintained in same LDAP server. • Storwize V7000 Unified will be used with both CIFS and NFS data access protocols. • Customer plans to use Storwize V7000 Unified for remote replication.	“LDAP”
LDAP (Secure)	LDAP (Secure)	• Storwize V7000 Unified needs to be used in the IT infrastructure where LDAP is used as a Directory service and all user information is maintained in the same LDAP server. • Storwize V7000 Unified needs to be used with both CIFS and NFS data access protocols. • To have secure communication with LDAP server with SSL or TLS protocols. • Customer plans to use Storwize V7000 Unified for remote replication.	“ Secure LDAP”
LDAP (Kerberos)	LDAP (Kerberos)	• Existing environment is based on an LDAP directory service • Secure communication with LDAP server using SSL or TLS protocol is required. • NAS services are required to be Kerberos server enabled (which increases security by not sending plain text passwords via the wire to Storwize V7000 Unified.) • Customer plans to use Storwize V7000 Unified for remote replication.	“Secure LDAP and MIT Kerberos”
Local Authentication	None	• No external authentication server such as Active Directory, LDAP etc are available in the IT infrastructure. • No async replication is needed by the customer.	“Local Authentication”

Which CLI commands are available to configure authentication?

Command	Purpose
cfgad	Configure Storwize V7000 Unified with AD Server
cfgsfu	Configure SFU for Storwize V7000 Unified, which is already configured with AD
cfgldap	Configure Storwize V7000 Unified with LDAP
cfgnis	Configure Storwize V7000 Unified with NIS
cfgnt4	Configure Storwize V7000 Unified with Microsoft Windows NT 4.0 Domain Controller (NT4) (Samba PDC)
cfglocalauth	Configure Storwize V7000 Unified with Local authentication.
lsauth	List the authentication settings
chkauth	Check the authentication settings
cleanupauth	Cleanup authentication settings to unconfigure current authentication settings
rmidmapcacheentry	Removes the ID map cache entry

Note : It is recommended that you refer to the man page of every command to understand every option and its usage .

Does Storwize V7000 Unified support support configuration of authentication using GUI?

Storwize V7000 Unified GUI does support authentication configurations. However, some advanced functionalities are provided by CLI only. This paper illustrates Storwize V7000 Unified CLI as well as GUI to be used for authentication configurations.

Can Storwize V7000 Unified admin users be authenticated through an external directory service, similar to that in case of other NAS users?

No. Only Storwize V7000 Unified NAS users can be authenticated through an external directory service. Accounts for Storwize V7000 Unified admin users must be created on the Storwize V7000 Unified system using the **mksuser** CLI command or the Storwize V7000 Unified GUI.

Can Storwize V7000 Unified be configured with multiple directory services?

Multiple directory services are not supported simultaneously. Only one authentication method (please see the list of supported methods) is supported at one time for user authentication.

Can Storwize V7000 Unified be configured with multiple instances of the same directory services?

No, only one instance (for example one AD domain) can be configured.

AD – The trust relationships of multiple AD domains to the principle AD domain can be configured. Storwize V7000 Unified should be configured with the principle AD domain. Once IBM Storwize V7000 Unified is configured with one AD domain, user information from all the other domains in a trust with this primary domain can be accessed.

LDAP – Multiple LDAP servers can be configured and must be replicas of the same master LDAP server, or they can be any LDAP host with the same schema, which contain data that is mirrored from the same LDAP Data Interchange Format (LDIF) file.

Storwize V7000 Unified with AD

Which ID mapping methods are available for Storwize V7000 Unified with AD?

The following ID mapping methods are available for Storwize V7000 Unified with AD.

- Microsoft AD with Storwize V7000 Unified internal automatic ID mapping
- Microsoft AD with SFU
- Microsoft AD with NIS

Microsoft AD

When to choose Storwize V7000 Unified with AD?

Storwize V7000 Unified with AD is the right choice for customers with the following conditions:

- When only Windows users and clients will be using Storwize V7000 Unified.
- Customer uses Microsoft Active Directory (AD) to store user information and user passwords.
- Customer does not use SFU.
- Customer does not plan to use Storwize V7000 Unified remote replication.

What are the prerequisites for configuring Storwize V7000 Unified with AD?

The **cfgad** CLI command configures Storwize V7000 Unified with AD. The **cfgad** command requires an AD administrator user ID and password to join the Storwize V7000 Unified system as a member into the AD domain. The provided AD administrator ID must have the privilege to add a new computer account to the AD domain. Storwize V7000 Unified does not store the provided AD administrator ID and password. A temporary AD administrator ID is sufficient which can be removed from the AD server after the Storwize V7000 Unified is configured with AD successfully.

What are the limitations of Storwize V7000 Unified with AD?

Data access through different protocols such as CIFS and NFS can be done only if UIDs and GIDs are identical on client and Storwize V7000 Unified. To configure heterogeneous data access using CIFS and NFS, you need to use the **chkauth** CLI command to figure out UIDs and GIDs generated by Storwize V7000 Unified and assign to UNIX users on NFS clients. Instead, to avoid such situation, it is recommended to use central ID mapping such as SFU or NIS.

After the data is stored on Storwize V7000 Unified with AD, it is very difficult to add SFU later on, because the UIDs and GIDs used internally by Storwize V7000 Unified must match the UIDs and GIDs stored in SFU. This is impossible if conflicting UIDs and GIDs are already present in SFU. So, such customers should configure Storwize V7000 Unified with AD and SFU right from the beginning.

Another limitation is the ability to configure Storwize V7000 Unified remote replication, because the source and target Storwize V7000 Unified systems are very likely to generate different UIDs / GIDs for same user or group. The ACLs copied from the source to the target include UIDs and GIDs of the source which are inconsistent with the UIDs and GIDs of the target. Central ID mapping such as SFU should be used for remote replication.

How to configure Storwize V7000 Unified with AD using CLI?

The **cfgad** command configures Storwize V7000 Unified with AD:

```
cfgad -s <adServerName> -u <userName> [-p <password>] [--preferredDC  
<preferredDC>] [--idMapConfig <idMapConfig>] [-c < clusterID | clusterName >]
```

It is best practice to omit the **--preferredDC** option. Storwize V7000 Unified can find all additional available domain controllers automatically.

Recommended usage of **cfgad** for configuring Storwize V7000 Unified with AD:

```
cfgad -s adServerName -p password -u userName
```

Warning: Storwize V7000 Unified must not be configured with any authentication method before using **cfgad**.

Example of configuring Storwize V7000 Unified with AD

To configure the Storwize V7000 Unified system with AD:

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.virtual11.com]$ lsauth  
EFSSG0571I Cluster st001.virtual11.com is not configured with any type of  
authentication server.
```

2. Run **cfgad** to configure Storwize V7000 Unified with AD.

```
[st001.virtual11.com]$ cfgad -s ad1 -u administrator -p test01  
(1/9) Fetching the list of cluster Nodes.  
(2/9) Check if cfgcluster has done the basic configuration successfully.  
(3/9) Check whether Interface nodes are reachable from management node.  
(4/9) Detection of AD server and fetching domain information from AD  
server.  
(5/9) Check whether AD server is reachable from Interface nodes.  
(6/9) Joining the domain of the specified ADS.  
(7/9) Updating the system with ADS configuration details.  
(8/9) Finalizing configuration.  
(9/9) Updating the database.  
EFSSG1000I The command completed successfully.
```

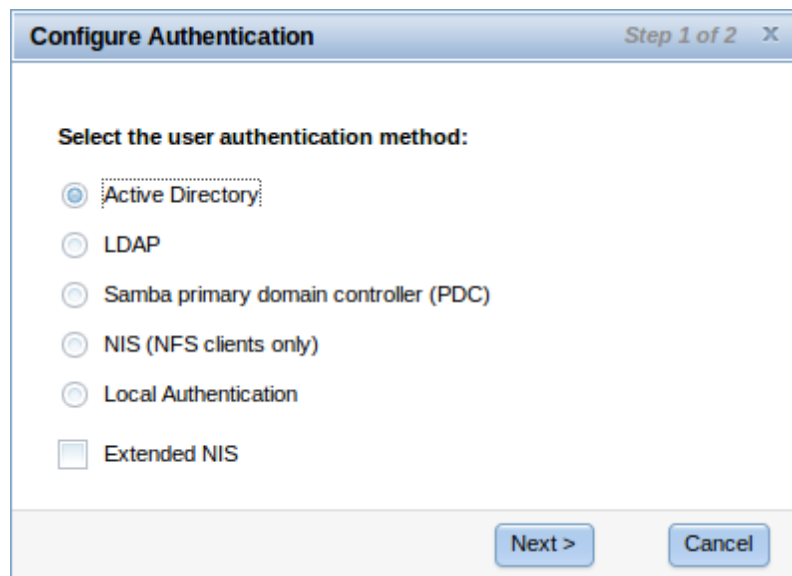
3. Run **lsauth** to verify that AD authentication method is configured.

```
[st001.virtual11.com]$ lsauth  
AUTH_TYPE = ad  
idMapConfig = 10000000-299999999,1000000  
idMappingMethod = auto  
domain = virtual11  
clusterName = st001.virtual11.com  
userName = administrator  
adHost = ad1.virtual11.com  
passwordServer = *  
realm = virtual11.com  
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with AD using the GUI?

To configure the Storwize V7000 Unified system with AD using the GUI:

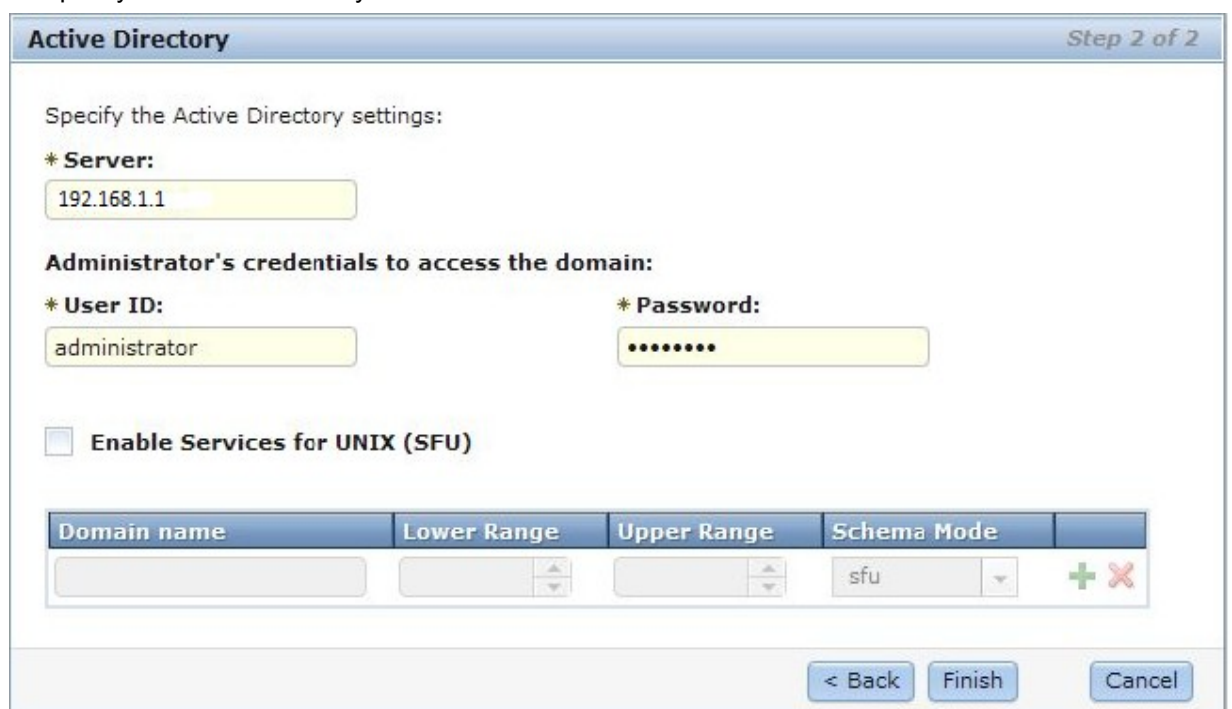
1. Select **Active Directory** as the authentication method.



The dialog box is titled "Configure Authentication" with a subtitle "Step 1 of 2". It contains a section "Select the user authentication method:" with six radio button options: "Active Directory" (selected), "LDAP", "Samba primary domain controller (PDC)", "NIS (NIS clients only)", "Local Authentication", and "Extended NIS". At the bottom right are "Next >" and "Cancel" buttons.

Figure 1: Specifying the authentication method

2. Specify the Active Directory server and administrator user credentials and click **Finish**.



The dialog box is titled "Active Directory" with a subtitle "Step 2 of 2". It contains the following fields and controls:

- "Specify the Active Directory settings:"
- * **Server:** 192.168.1.1
- Administrator's credentials to access the domain:**
- * **User ID:** administrator
- * **Password:** (masked with dots)
- ☐ **Enable Services for UNIX (SFU)**
- A table with columns: Domain name, Lower Range, Upper Range, Schema Mode, and a status column with a green plus icon and a red X icon.
- Buttons at the bottom: "< Back", "Finish", and "Cancel".

Figure 2: Specifying the AD server and administrator credentials

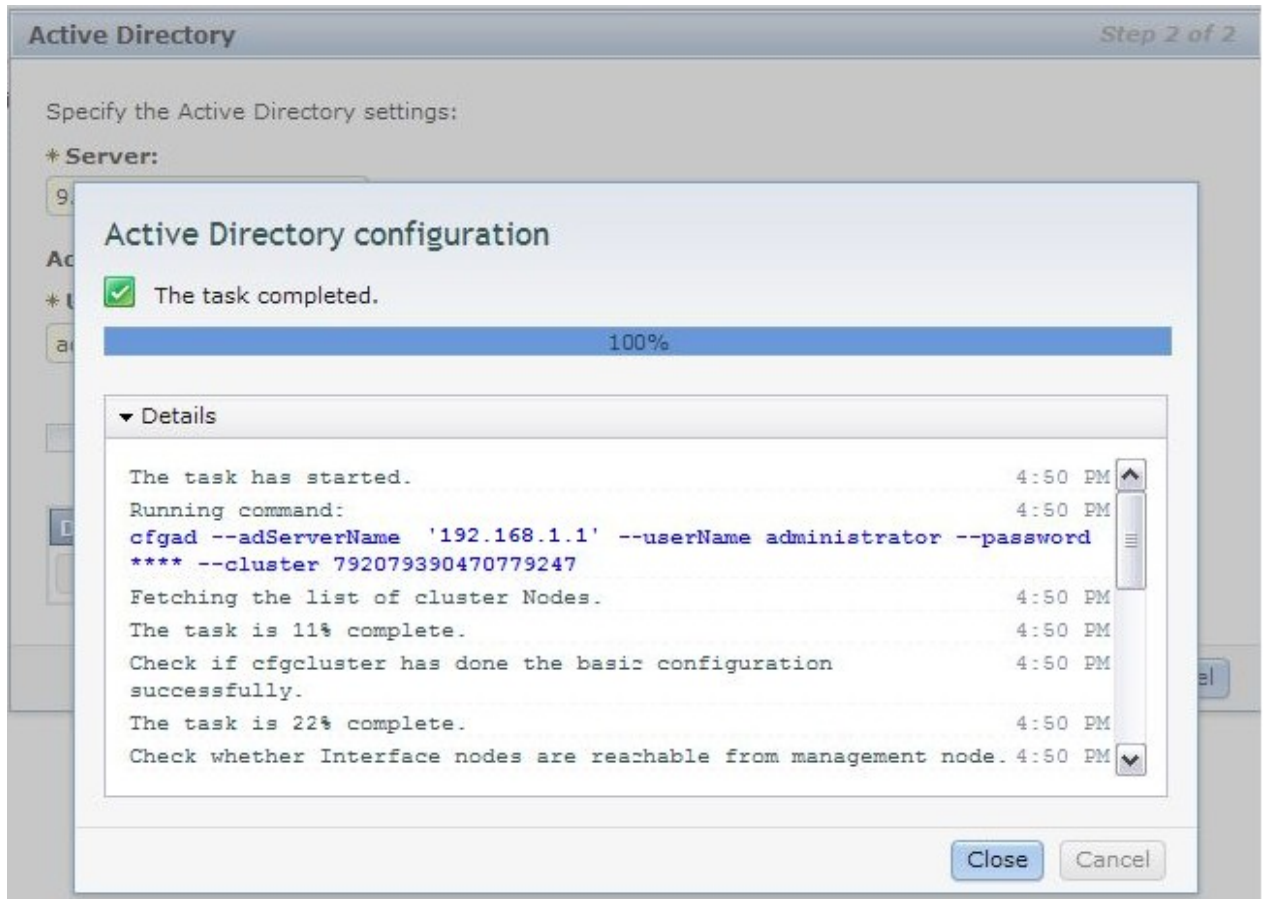


Figure 3: Successful completion of Active Directory configuration

3. Wait for successful completion of configuration and click **Close**.

Choosing idMapConfig Options

The idMapConfig option of cfkad command has two parts - range & rangesize.

range

Unix ID are allocated from this *range*.

Use syntax: <lowerID of the range> - <higherID of the range>

The lowerID of the range must be at least 1000. Default value for range is 10000000-299999999.

rangesize

The *rangesize* signifies the number of IDs per domain. It defines the available number of UIDs/GIDs per domain. If the 'range' is defined as 10000-20000, and range size is 2000, then it means that 5 domains each consisting of 2000 IDs can be mapped.

The *rangesize* must be at least 2000. Default value for *rangesize* is 1000000.

When a user or group is defined in Active Directory it is identified by an SID which includes a component called RID(Relative Identifier). If RID of any user is greater than the *rangesize*, then ***that user cannot access Storwize V7000 Unified exports***. So, *rangesize* should be chosen to allow highest possible RID of users and groups. Choose this value carefully, as this cannot be changed after the first ranges for domains have been defined. The RID value depends on the number of users and groups. Ensure that the *rangesize* takes into account the planned growth of users or groups.

The following section gives an example of how to choose *rangesize*.

Example:

Step1: Figure out the highest RID that has been assigned till now. To determine the highest RID find the '*rIDNextRID*' attribute in Active Directory

One way to figure that out is to use 'dcdiag' command on the command prompt of the operating System hosting Active Directory.

for example:

Command => "dcdiag /s:{IP of system hosting AD} /v /test:ridmanager"

C:\Program Files\Support Tools>C:\Program Files\Support Tools>dcdiag /s:10.0.0.123 /v /test:ridmanager

```
Starting test: RidManager
* Available RID Pool for the Domain is 1600 to 1073741823
* win2k8.pollux.com is the RID Master
* DsBind with RID Master was successful
* rIDAllocationPool is 1100 to 1599
* rIDPreviousAllocationPool is 1100 to 1599
* rIDNextRID: 1174
```

Here, the *rIDNextRID* is 1174.

Another way to find out *rIDNextRID* is to run an ldap query on the following DN Path:
CN=Rid Set,Cn=computername,ou=domain controllers,DC=domain,DC=COM

If there is more than 1 domain controller serving the AD domain, then highest RID among the domain controllers should be used.

Step2: Figure out the expected number of users that will be added on top of current number of users.

Step3: Add the highest RID from step1 to number of users from step2. This forms your *rangesize*.

Why does cfgad require ID and password of an AD administrator?

Storwize V7000 Unified requires a temporary AD administrator ID for secure joining of the AD domain. This behavior is consistent with joining a native Windows server to an AD domain.

Microsoft AD with SFU

When to choose Storwize V7000 Unified with AD and SFU?

Storwize V7000 Unified with AD and SFU is the right choice for customers under the following conditions:

- Customer uses Microsoft AD to store user information and user passwords.
- Customer plans to use NFS along with CIFS for NAS access.
- Customer plans to use Storwize V7000 Unified remote replication.

What are the prerequisites for configuring Storwize V7000 Unified with AD and SFU?

- Storwize V7000 Unified is configured with AD authentication (for example, **cfgad** was executed successfully).
- Microsoft Windows SFU is installed along with on the AD server.
- So far no files have been stored on Storwize V7000 Unified (refer to the limitations in the following section).
- **Warning:** The SFU ID range must not overlap with `-idMapConfig` (default range 10000000-299999999). This range is used by Storwize V7000 Unified to automatically generate UID or GIDs for domains that are not configured in SFU. The command will not allow you to overlap the range
- The primary Windows group assigned to AD users must have a GID assigned. Otherwise users will be denied access to the system.
- Each user in AD must have a valid UID and GID assigned in order to be able to mount and access Storwize V7000 Unified NAS exports. The UID and GID number assigned must be within the range used in the **cfgsfu** command.

What are the limitations of Storwize V7000 Unified with AD and SFU?

- **Warning:** The ID range specified with the **cfgad** parameter `-idMapConfig` (default range 10000000-299999999) is reserved for Storwize V7000 Unified and must not be used in SFU.
- SFU should not be configured, once data is stored on Storwize V7000 Unified. Refer to the limitations of Storwize V7000 Unified with AD for further details.
- Enabling SFU for a trusted domain requires a two-way trust between the principal and the trusted domain.
- The administrator is responsible for installing SFU on the desired Active Directory server and assign UID/GID to user and group. The command does not return an error if SFU/SUA is not installed or if UID/GID is not assigned.
- Once id mapping service from SFU is configured against the Storewize V7000 Unified system , re-executing the **cfgsfu** command will overwrite the earlier configuration with the new one.
- Group memberships defined under the 'Unix attributes' tab are not honored. Only the windows groups memberships will be recognized.

What are the best practices for Storwize V7000 Unified with AD and SFU?

- The **cfgsfu** command restricts the UID/GID range. Minimum value is 1 and the maximum value is 4294967295. Using UIDs/GIDs less than 1024 causes a UID/GID collision of Storwize V7000 Unified NAS user with Storwize V7000 Unified admin user. This collision is a security concern (for example, Storwize V7000 Unified administrators might be able to touch NAS data) and some Storwize V7000 Unified commands (for example, **lsquota**) might report incorrect information. When the **cfgsfu** command detects such collision, then it will ask you whether you are sure you want to go for it. **--force** option can be used to confirm that, at your own risk.
- All AD groups have a GID assigned to avoid any authorization issues.
- The primary UNIX group setting in Active Directory will not be used by Storwize V7000 Unified NAS. Storwize V7000 Unified will always use the primary Windows group as the primary group for the user. This results in new files and directories created by a user through CIFS being owned by his primary Windows group and not by the primary UNIX group. For this reason, it is recommended that the UNIX attribute primary group assigned be same as the Windows primary group defined for the user.

How to configure Storwize V7000 Unified with AD and SFU using CLI?

The **cfgsfu** command enables SFU user ID mapping for a Storwize V7000 Unified system which is already configured with AD:

```
cfgsfu [-c { clusterID | clusterName }] --configParameters  
{ domainName, range, schemaMode { sfu | rfc2307 } } [--force]
```

Before using **cfgsfu**, Storwize V7000 Unified must be configured with AD authentication.

Recommended usage of **cfgsfu** for enabling SFU mapping server:

```
cfgsfu --configParameters  
{ domainName, range, schemaMode { sfu | rfc2307 } }
```

Use **range** to define the matching UID and GID ranges. This range should not intersect with **idMapConfig** (default range 10000000-299999999), which is reserved by Storwize V7000 Unified to automatically generate UID and GID for users and groups that are not configured with SFU.

Use **schemaMode** as follows based on operating system of the domain:

- **rfc2307**: Microsoft Windows Server 2008 or Windows 2003 with R2
- **sfu**
: Windows Server 2000 and Windows 2003 with SP1

The command does not validate the schema mode against the Active Directory domain controller. Ensure that the correct **schemaMode** has been specified else the functionality may not work.

Example of enabling SFU user mapping

To enable SFU user mapping:

1. Run **lsauth** to verify that authentication method configured is AD.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ad
idMapConfig = 10000000-299999999,1000000
idMappingMethod = auto
domain = virtual1
clusterName = st001.virtual1.com
userName = administrator
adHost = ad1.virtual1.com
passwordServer = *
realm = virtual1.com
EFSSG1000I The command completed successfully.
```

2. Run **cfgsfu** to configure Storwize V7000 Unified with SFU.

```
[@st001.mgmt001st001 ~]# cfgsfu --configParameters "virtual1,1024-9999,sfu"
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that AD authentication method is configured with SFU.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ad
idMapConfig = 10000000-299999999,1000000
SFU_virtual1 = ad,1024-9999,sfu
idMappingMethod = sfu
domain = virtual1
clusterName = st001.virtual1.com
userName = Administrator
adHost = ad1.virtual1.com
passwordServer = *
realm = virtual1.com
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with AD and SFU using the GUI?

To configure Storwize V7000 Unified with AD and SFU using the GUI:

1. Select **Active Directory** as the authentication method.

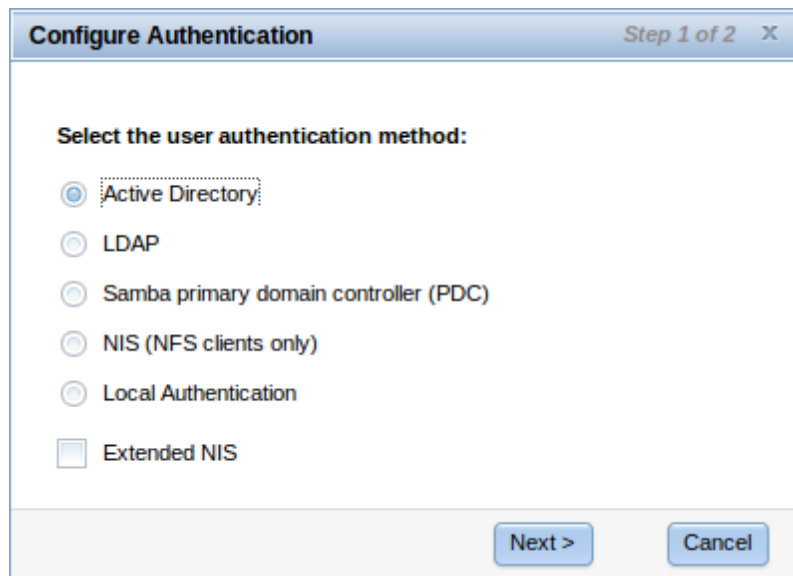


Figure 4: Specifying the authentication method – AD

2. Specify the AD server and administrator credentials and enable SFU with domain, ID range, schema mode and click **Finish**.

Active Directory Step 2 of 2

Specify the Active Directory settings:

*** Server:**

Administrator's credentials to access the domain:

*** User ID:** *** Password:**

☒ **Enable Services for UNIX (SFU)**

Domain name	Lower Range	Upper Range	Schema Mode	
virtual11	1024	9999	rfc2307	+ X

Figure 5: Specifying the AD server and administrator credentials and SFU options

3. Wait for successful completion of configuration and then click **Close**.

Active Directory configuration

☒ The task completed.

100%

▼ Details

```

The task is 38% complete.                                     4:54 PM
Finalizing configuration.                                     4:54 PM
The task is 44% complete.                                     4:54 PM
Updating the database.                                         4:54 PM
The task is 50% complete.                                       4:54 PM
Running command:                                              4:54 PM
cfgsfu --configParameters'virtual11, 1024-9999, rfc2307' --force --cluster
792079390470779247                                           4:54 PM
The task is 100% complete.                                     4:54 PM
The task completed.                                           4:54 PM
  
```

Figure 6: Successful completion of Active Directory and SFU configuration

Microsoft AD with NIS

When to choose Storwize V7000 Unified with AD and NIS?

Storwize V7000 Unified with AD and NIS is the right choice for customers under the following conditions:

- Customer uses Microsoft AD to store user information and user passwords.
- Customer plans to use NFS for NAS access.
- User and group IDs are stored and managed in NIS.

What are the prerequisites for configuring Storwize V7000 Unified with AD and NIS?

- Storwize V7000 Unified is configured with AD authentication (for example, `cfgad` was executed).
- NIS is used for all UID and GID mapping.
- So far no files have been stored on Storwize V7000 Unified (refer to limitations in the following section).
- All NIS users and groups name should be in lower case with blank spaces replaced with underscores.

What are the limitations of Storwize V7000 Unified with AD and NIS?

- NIS should not be configured once data is stored on Storwize V7000 Unified. Refer to the limitations of Storwize V7000 Unified with AD for further details.
- Lower value of the `idMapUserRange` and `idMapGroupRange` option in the `cfgnis` command cannot be less than 1024. (`cfgnis` command will not allow minimum range value less than 1024.)
- UNIX style names do not allow spaces in the name. For mapping Active Directory users or group to NIS users, consider the following conversion on NIS server
 - Convert all upper case alphabets to lower case.
 - Replace all blank spaces with underscores.

For example, an Active Directory user or group name **CAPITAL Name** should have a corresponding name on NIS as **capital_name**.

Warning: If the above mentioned naming convention is not used for users, then NIS mapping will not happen, and idmapping for such users will follow user map rules defined in `cfgnis --userMap` option for that AD domain.

What are the best practices for Storwize V7000 Unified with AD and NIS?

Administrator must ensure that the existing NIS IDs do not fall in `idmapUserRange` and `idmapGroupRange`. For more information, refer to the **Reference > CLI Reference > cfgnis > --userMap** section in Information Center.

How to configure Storwize V7000 Unified with AD and NIS using CLI?

The **cfgnis** command enables NIS user ID mapping for a Storwize V7000 Unified system which is already configured with AD:

```
cfgnis [-c { clusterID | clusterName }] [--extend { extend }] [-m { modify }]
[-d { nisDomain }] [--domainMap { domainMap }] [--serverMap { serverMap }
        [--userMap { userMapping }] [--disableVerifyServer
{ disableVerifyServer }]
        [--useAsIdmap { useAsIDmap }] [--idmapUserRange { idmapUserRange }]
[--idmapGroupRange { idmapGroupRange }]
```

Recommended usage of **cfgnis** for configuring AD with NIS:

```
cfgnis --extend -d Nis --serverMap 192.168.1.3:Nis --domainMap virtual1:Nis
--idmapUserRange 100000-200000 --idmapGroupRange 100000-200000 --useAsIdmap
```

Storwize V7000 Unified must be configured with AD authentication, before using **cfgnis** for configuring NIS user and group ID mappings.

Example of enabling NIS user mapping

To enable NIS user mapping:

1. Run **lsauth** to verify that the authentication method configured is AD.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ad
idMapConfig = 10000000-299999999,1000000
idMappingMethod = auto
domain = virtual1
clusterName = st001.virtual1.com
userName = administrator
adHost = ad1.virtual1.com
passwordServer = *
realm = virtual1.com
EFSSG1000I The command completed successfully.
```

2. Run **cfgnis** to configure Storwize V7000 Unified with NIS.

```
[st001.mgmt001st001 ~]# cfgnis --extend -d Nis --serverMap
192.168.1.3:Nis --domainMap virtual1:Nis --idmapUserRange 200000-300000
--idmapGroupRange 300001-400000 --useAsIdmap
(1/9) Check if NIS can be extended or not.Checking if authentication
type is AD or NT4
(2/9) Fetching the list of CTDB cluster Nodes.
(3/9) Check whether Interface nodes are reachable from management node
(4/9) Check if primary NIS domain is served by any NIS server or not
(5/9) Checking if primary NIS domain is reachable from all interface
nodes or not
(6/9) Verifying NIS server
(7/9) Setting values into the registry
(8/9) Finalizing configuration
```

```
(9/9) Updating the database
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that AD authentication method is configured with NIS.

```
[st001.mgmt001st001 ~]# lsauth
idMapConfig = 1024-4294967295,1
domain = virtual1
clusterName = st001.virtual1.com
adHost = ad1.virtual1.com
NIS_Domain = Nis
realm = virtual1.com
AUTH_TYPE = ad
idMapUserRange = 200000-300000
NIS_ServerMap = 192.168.1.3:Nis
idMappingMethod = nis
userName = Administrator
NIS_virtual1 = Nis:none
passwordServer = *
idMapGroupRange = 300001-400000
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with AD and NIS using the GUI?

To configure Storwize V7000 Unified with AD and NIS using the GUI:

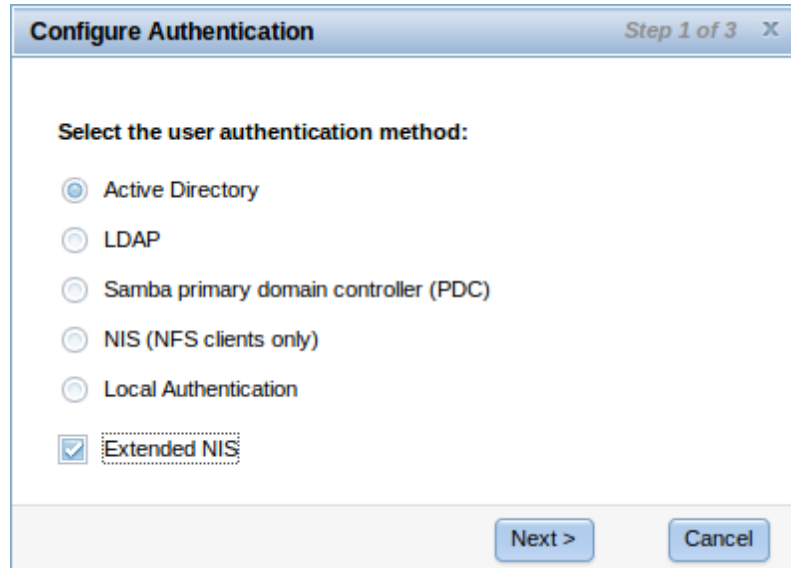


Figure 7: Specifying the authentication method – AD and NIS

1. Select **Active Directory** as the authentication method and select the **Extended NIS** check box, and click Next

2. Specify Active Directory server and administrator user credentials (as done in basic Active Directory configuration step 2).
3. Specify the NIS primary domain, NIS server-domain map, AD-NIS domain map, AD-NIS user map, and user and group ID ranges and then click **Finish**.

Extended NIS Step 3 of 3

* **Primary NIS domain:**
Nis

* **Server map:**

NIS Server	NIS Domain	
192.168.1.3	Nis	+ X

☒ **Enable user ID mappings**

Domain map:

Active Directory Domain	NIS Domains	
virtual1	Nis	+ X

User map:

Active Directory Domain	Action	Mapped User	
virtual1	AUTO		+ X

User ID range:

From: 100000 To: 200000

Group ID range:

From: 100000 To: 200000

< Back Finish Cancel

Figure 8: Specifying AD and NIS parameters

4. Wait for successful completion of configuration and then click **Close**.

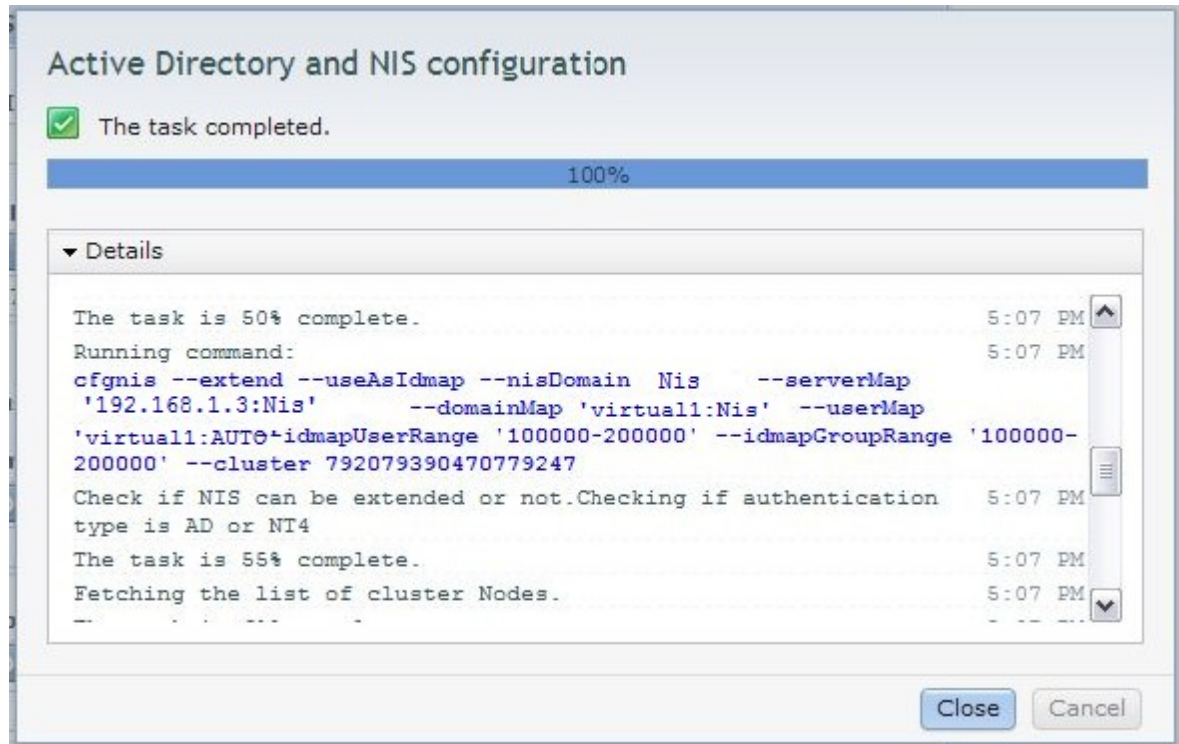


Figure 9: Successful completion of AD and NIS configuration

Storwize V7000 Unified with NT4 / Samba PDC

Which ID mapping methods are available for NT4 / Samba PDC?

- Samba PDC / NT4 with Storwize V7000 Unified internal automatic ID mapping
- Samba PDC / NT4 with NIS

NT4 / Samba PDC

When to choose Storwize V7000 Unified with NT4 / Samba PDC?

- Customer use Samba PDC to store user information and user passwords. Samba can serve as a NT4 server when configured as a PDC.
- Storwize V7000 Unified is used with the environment having legacy Windows 2000 and NT4 domain users.

What are the prerequisites for configuring Storwize V7000 Unified with NT4 / Samba PDC?

- Samba PDC server must be reachable from the Storwize V7000 Unified interface node.
- User name and password for a user must have administrator privileges on PDC.

How to configure Storwize V7000 Unified with NT4 / Samba PDC using CLI?

The **cfgnt4** command configures Storwize V7000 Unified with NT4 / Samba PDC:

```
cfgnt4 -s <nt4Host> --nt4NetbiosName <nt4NetbiosName> -d <nt4Domain> -u  
<nt4AdminUser> [-p <nt4AdminPw>] [-c <clusterID | clusterName >]
```

Recommended usage of **cfgnt4** for configuring Storwize V7000 Unified with NT4 / Samba PDC:

```
cfgnt4 -s <nt4Host> -p <nt4AdminPw> -u <nt4AdminUser> - nt4NetbiosName  
<nt4NetbiosName> -d <nt4Domain>
```

Warning: Storwize V7000 Unified must not be configured with any authentication method, before using the **cfgnt4** command.

Example of configuring Storwize V7000 Unified with NT4 / Samba PDC

To configure Storwize V7000 Unified with NT4 / Samba PDC:

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth  
EFSSG0571I Cluster st001.virtual11.com is not configured with any type of  
authentication server.
```

2. Run **cfgnt4** to configure Storwize V7000 Unified with NT4 / Samba PDC.

```
[st001.mgmt001st001 ~]# cfgnt4 -s 192.168.1.4 --nt4NetbiosName sonash1  
-d SMBPDC -u root -p test01  
(1/9) Fetching the list of CTDB cluster Nodes.  
(2/9) Check if cfgcluster has done the basic configuration successfully.  
(3/9) Check whether Interface nodes are reachable from management node  
(4/9) Check whether NT4 server is reachable from cluster nodes  
(5/9) Verification of NT4 server from a node using credentials provided  
(6/9) Joining the domain of the specified NT4.  
(7/9) Updating the system with NT4 configuration details  
(8/9) Finalizing configuration  
(9/9) Updating the database  
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that NT4 / Samba PDC authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth  
AUTH_TYPE = nt4  
idMappingMethod = auto  
domain = SMBPDC  
nt4NetbiosName = sonash1  
clusterName = st001.virtual11.com  
nt4Host = 192.168.1.4  
userName = root
```

EFSSG1000I The command completed successfully.

How to configure Storwize V7000 Unified with NT4 / Samba PDC using the GUI?

To configure Storwize V7000 Unified with NT4 / Samba PDC using the GUI:

1. Select **Samba primary domain controller (PDC)** as the authentication method and click **OK**.

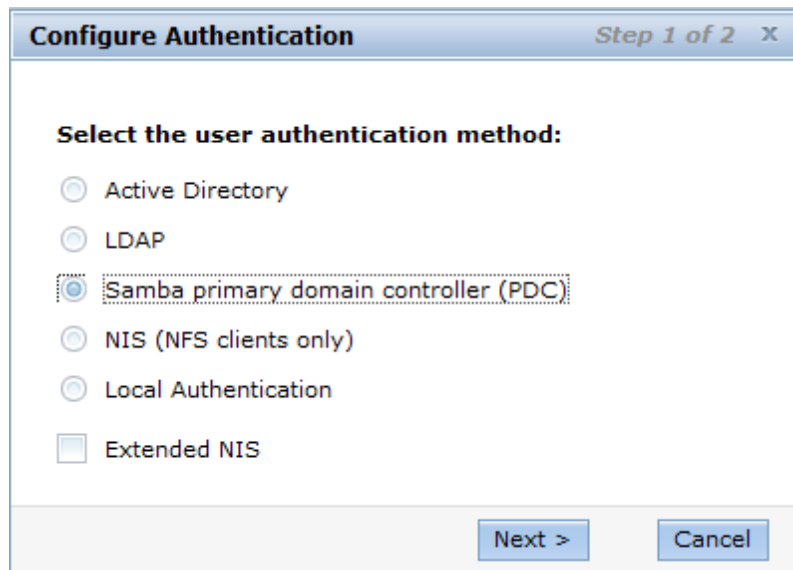


Figure 10: Specifying the authentication method – Samba PDC

2. Specify Samba PDC Server host name / IP address, NetBIOS name, domain name, and administrator user credentials and click **Finish**.



Figure 11: Specifying Samba PDC parameters

3. Wait for successful completion of configuration and then click **Close**.

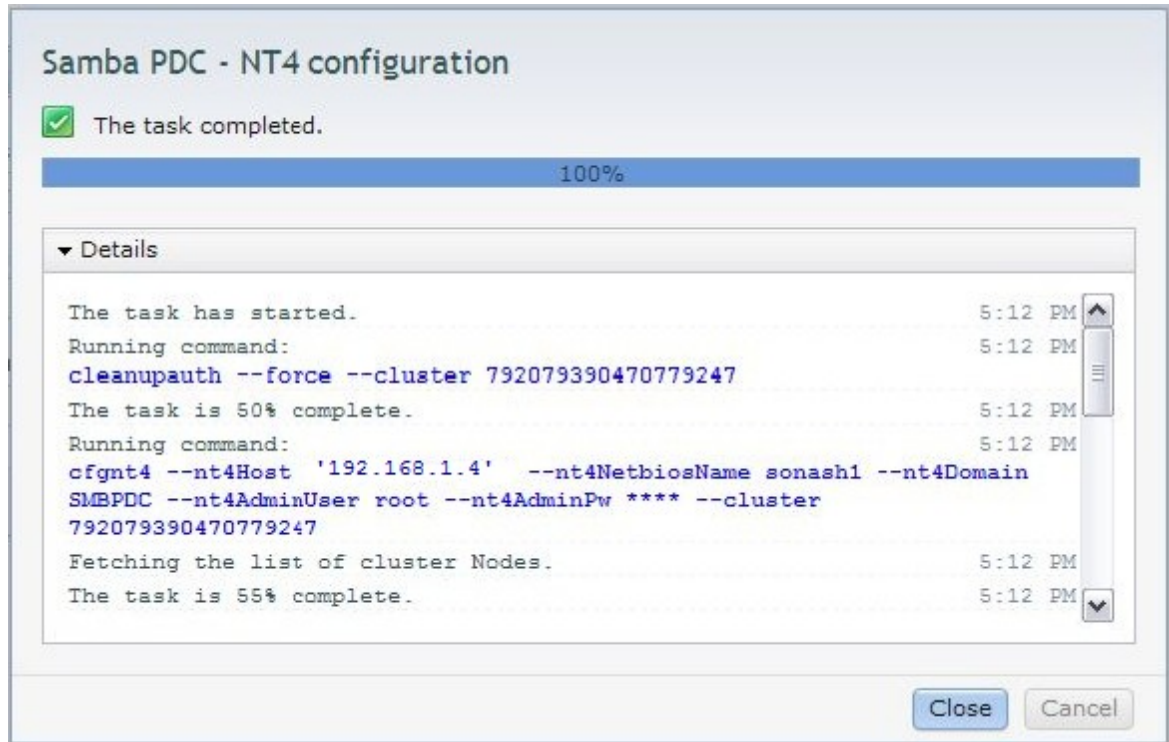


Figure 12: Successful completion of Samba PDC configuration

NT4 / Samba PDC with NIS

When to choose Storwize V7000 Unified with NT4 / Samba PDC and NIS?

Storwize V7000 Unified with AD and NIS is the right choice for customers with the following conditions:

- Customer uses Samba PDC to store user information and user passwords. Samba can serve as a NT4 server when configured as a PDC.
- Customer plans to use NFS for NAS access.
- User ID are stored and managed in NIS.

What are the prerequisites for configuring Storwize V7000 Unified with NT4 / Samba PDC and NIS?

- Storwize V7000 Unified is configured with Nt4 authentication (for example, `cfgnt4` was executed).
- NIS is used for all UID mapping.

- So far no files have been stored on Storwize V7000 Unified (refer to limitations in the following section).

What are the limitations of Storwize V7000 Unified with NT4 / Samba PDC and NIS?

- NIS should not be added, once data is stored on Storwize V7000 Unified. (Refer to the limitations of Storwize V7000 Unified with AD for further details)
- Lower value of idMapUserRange and idMapGroupRange option in cfgnis command cannot be less than 1024
- UNIX style names do not allow spaces in the name. For mapping AD users or group to NIS users, apply the following convention on NIS server
 - Convert all alphabets in upper case to lower case
 - Replace all spaces with underscores

For example, an AD user or group name '**CAPITAL Name**' should have a corresponding name on NIS as '**capital_name**'.

Warning: If above mentioned naming convention is not used for users, then NIS mapping will not happen, and idmapping for such users will follow user map rules defined in cfgnis --userMap option for that NT4/PDC domain.

What are the best practices for Storwize V7000 Unified with NT4 / Samba PDC and NIS?

Administrator must ensure that the existing NIS IDs do not fall in idmapUserRange and idmapGroupRange. For more information, refer to the **Reference > CLI Reference > cfgnis > userMap** section in Information Center.

How to configure Storwize V7000 Unified with NT4 / Samba PDC and NIS using CLI?

The **cfgnis** command enables NIS user mapping for a Storwize V7000 Unified system which is already configured with Samba PDC / NT4:

```
cfgnis [-c { clusterID | clusterName }] [--extend { extend }] [-m { modify }]
[-d { nisDomain }] [--domainMap { domainMap }] [--serverMap { serverMap }
      [--userMap { userMapping }] [--disableVerifyServer
{ disableVerifyServer }]
      [--useAsIdmap { useAsIDmap }] [--idmapUserRange { idmapUserRange }]
[--idmapGroupRange { idmapGroupRange }]
```

Recommended usage of **cfgnis** for enabling NIS mapping server:

```
cfgnis --extend -d PuneNis --serverMap 192.168.1.3:Nis --domainMap
virtual1:PuneNis --idmapUserRange 100000-200000 --idmapGroupRange 100000-200000
-useAsIdmap
```

Storwize V7000 Unified must be configured with Samba PDC / NT4 authentication, before using **cfgnis**.

Example of enabling NIS ID mapping

To enable NIS ID mapping:

1. Run **lsauth** to verify that the authentication method configured is NT4 / Samba PDC.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = nt4
idMappingMethod = auto
domain = SMBPDC
nt4NetbiosName = sonash1
clusterName = st001.virtual11.com
nt4Host = 192.168.1.4
userName = root
EFSSG1000I The command completed successfully.
```

2. Run **cfgnis** to configure Storwize V7000 Unified with NIS.

```
[st001.mgmt001st001 ~]# cfgnis --extend -d Nis --serverMap
192.168.1.3:Nis --domainMap virtual11:Nis --idmapUserRange 100000-200000
--idmapGroupRange 100000-200000 --useAsIdmap
(1/9) Check if NIS can be extended or not.Checking if authentication
type is AD or NT4
(2/9) Fetching the list of CTDB cluster Nodes.
(3/9) Check whether Interface nodes are reachable from management node
(4/9) Check if primary NIS domain is served by any NIS server or not
(5/9) Checking if primary NIS domain is reachable from all interface
nodes or not
(6/9) Verifying NIS server
(7/9) Setting values into the registry
(8/9) Finalizing configuration
(9/9) Updating the database
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that the NT4 / Samba PDC authentication method is configured with NIS.

```
[root@st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = nt4
idMapUserRange = 100000-200000
NIS_ServerMap = 192.168.1.3:Nis
domain = SMBPDC
idMappingMethod = nis
clusterName = st001.virtual11.com
nt4NetbiosName = sonash1
userName = root
nt4Host = 192.168.1.4
NIS_Domain = Nis
```

```
NIS_virtual1 = Nis;none  
idMapGroupRange = 100000-200000  
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with NT4 / Samba PDC and NIS using the GUI?

To configure Storwize V7000 Unified with NT4 / Samba PDC and NIS using the GUI:

1. Select **Samba primary domain controller (PDC)** as the authentication method and check the **Extended NIS** check box, and then click **Next**.

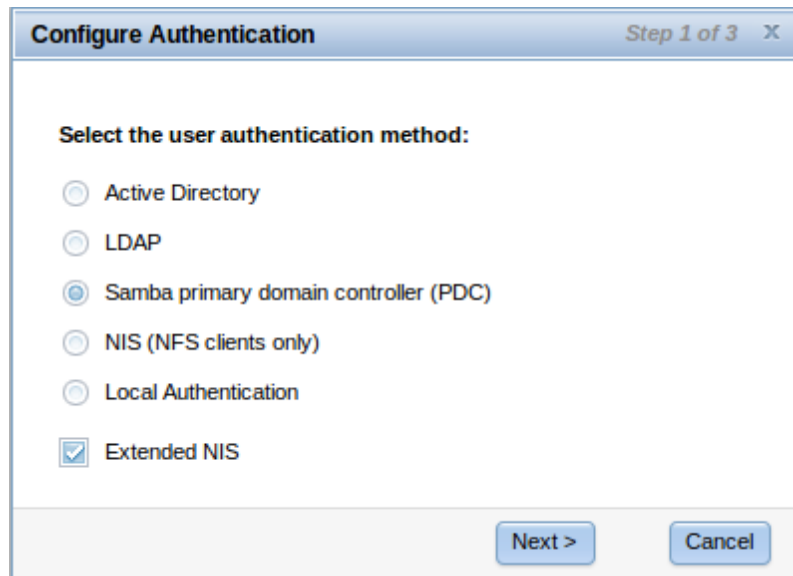


Figure 13: Specifying the authentication method for Samba PDC and NIS

2. Specify Samba PDC detail as mentioned in step 2 of Samba PDC configuration using the GUI.
3. Specify NIS primary domain, NIS server- map, Samba PDC-NIS domain map, Samba PDC-NIS user map, user and group ID range and click **Finish**.

Extended NIS

Step 3 of 3

* Primary NIS domain:

Nis

* Server map:

NIS Server	NIS Domain	
192.168.1.3	Nis	+ X

☒ Enable user ID mappings

Domain map:

Active Directory Domain	NIS Domains	
SMBPDC	Nis	+ X

User map:

Active Directory Domain	Action	Mapped User	
SMBPDC	AUTO		+ X

User ID range:

From:

100000

To:

200000

Group ID range:

From:

100000

To:

200000

< Back

Finish

Cancel

Figure 14: Specifying Samba PDC and NIS parameters

4. Wait for successful completion of configuration and then click **Close**.

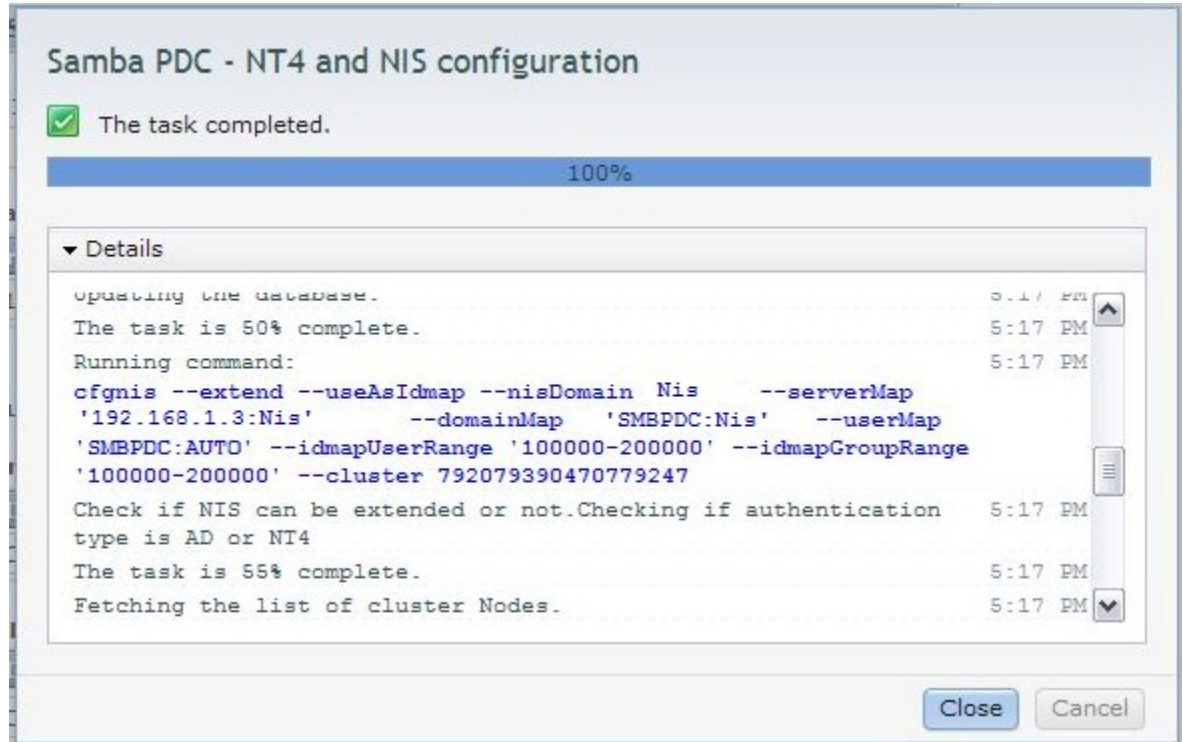


Figure 15: Successful completion of Samba PDC and NIS configuration

Storwize V7000 Unified with LDAP

LDAP-based authentication can be used mainly in the following ways:

- LDAP
- Secure LDAP based on SSL / TLS
- Secure LDAP based on SSL / TLS with Kerberos

Note: It is a best practice to use SSL / TLS and Kerberos-based LDAP to have maximum security.

Which ID mapping methods are available for Storwize V7000 Unified with LDAP

With LDAP, Storwize V7000 Unified does not need any external ID mapping method; LDAP server itself holds the ID mappings. Storwize V7000 Unified fetches ID mapping information from the LDAP server.

LDAP

When to choose Storwize V7000 Unified with LDAP?

- Storwize V7000 Unified will be used in an IT infrastructure where LDAP is used as a Directory service and all user information is maintained in same LDAP server.
- Storwize V7000 Unified will be used with both CIFS and NFS data access protocols.
- Customer needs support for remote replication

What are the prerequisites for configuring Storwize V7000 Unified with LDAP?

To support the CIFS protocol, one needs to extend the schema, which requires more attributes for POSIX user objects (mainly to store SID, Windows password hash and domain information, and so on). The details of this are explained in the following InfoCenter sections:

Administering > Administering the file system> Managing > Managing authentication and ID mapping > Setting up LDAPserver prerequisites

and

Administering > Administering the file system> Managing > Managing authentication and ID mapping > Setting up LDAPserver prerequisites > Updating LDAP user information with unique Samba attributes

What are the limitations of Storwize V7000 Unified with LDAP?

Communication with an LDAP server is not secure.

How to configure Storwize V7000 Unified with LDAP using CLI?

The **cfgldap** command configures Storwize V7000 Unified with LDAP:

```
cfgldap -s ldapServers> -b <ldapBase> -D <ldapBindDn> [-p <ldapBindPw>] [--krbKDC <krbKdc>] [--krbRealm <krbRealm>] [--krbKeytabFile <krbKeytabFile>] [--caCertFile <caCertFile>] [--ldapUserSuffix <ldapUserSuffix>] [--ldapGroupSuffix <ldapGroupSuffix>] [--sslMode <sslMode>] [-c < clusterID | clusterName >]
```

All command line options are categories in the following main functionality.

Common options include:

```
[-c { clusterID | clusterName }]  
  
-b ldapBase  
  
-D ldapBindDn  
  
[-p ldapBindPw]  
  
-s ldapServers  
  
[--ldapUserSuffix ldapUserSuffix]  
  
[-- ldapGroupSuffix ldapGroupSuffix]
```

Options for SSL / TLS

```
[--caCertFile caCertFile]

--sslMode { ssl | tls | off }
```

Options for Kerberos

```
[-- krbKDC krbKdc]

[--krbRealm krbRealm]

[ -- krbKeytabFile krbKeytabFile]
```

Recommended usage of **cfgldap** for configuring Storwize V7000 Unified with LDAP is:

```
cfgldap -s ldapserver -p secret -b dc=ldapserver,dc=com -D
cn=manager,dc=ldapserver,dc=com --sslMode off
```

Note: For multiple LDAP servers, you need to combine the server certificates of all LDAP servers into a single certificate file, which will then be applied to all the LDAP servers. Certificates are created with specific LDAP server name; this server name must match with the LDAP host names (as otherwise configuration might fail).

Warning: Storwize V7000 Unified must not be configured with any authentication method before using the **cfgldap** command.

Example of configuring Storwize V7000 Unified with LDAP:

To configure Storwize V7000 Unified with LDAP:

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth
EFSSG0571I Cluster st001.virtual1.com is not configured with any type of
authentication server.
```

2. Run **cfgldap** to configure Storwize V7000 Unified with LDAP.

```
[st001.mgmt001st001 ~]# cfgldap -s ldap1 -b dc=storwizeldap,dc=com -D
cn=manager,dc=sonasldap,dc=com -p secret --sslMode off
(1/9) Fetching the list of CTDB cluster Nodes.
(2/9) Check if cfgcluster has done the basic configuration successfully.
(3/9) Check whether Interface nodes are reachable from management node
(4/9) LDAP Configuration started
(5/9) Check whether LDAP server is reachable from Interface nodes
(6/9) Verification of LDAP server from a node using credentials provided
(7/9) Updating the system with LDAP configuration details
(8/9) Finalizing configuration
(9/9) Updating the database
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that LDAP authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth
clusterName = st001.virtual11.com
ldapUri = ldap://ldap1
nscdMode = on
ldapBindDn = cn=manager,dc=sonasldap,dc=com
sslMode = off
AUTH_TYPE = ldap
ldapVersion = 3
ldapBase = dc=sonasldap,dc=com

krbMode = off
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with LDAP using the GUI?

To configure Storwize V7000 Unified with LDAP using the GUI:

1. Select **LDAP** as the authentication method and click **Next**.

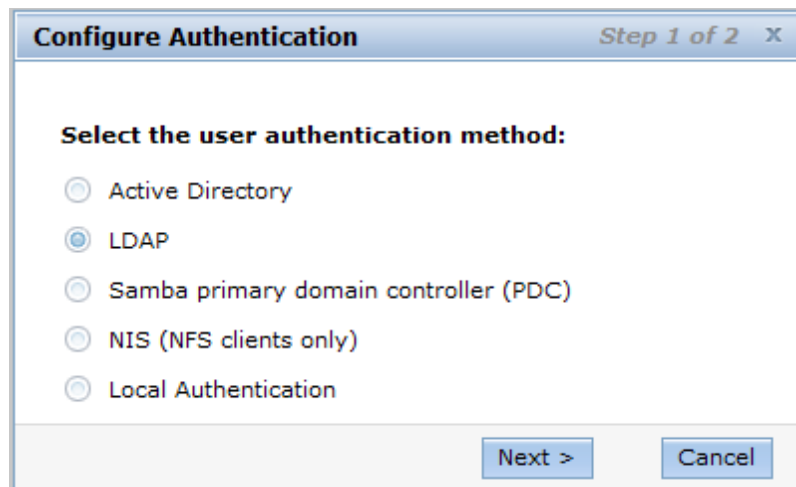


Figure 16: Specifying the authentication method for LDAP

2. Specify LDAP Server host name or IP address along with port number, search base for users and groups, and bind distinguished name, password, and the workgroup that this system should be part of. Security method needs to be set to **off**.

3. Wait for successful completion of configuration and click **Close**.

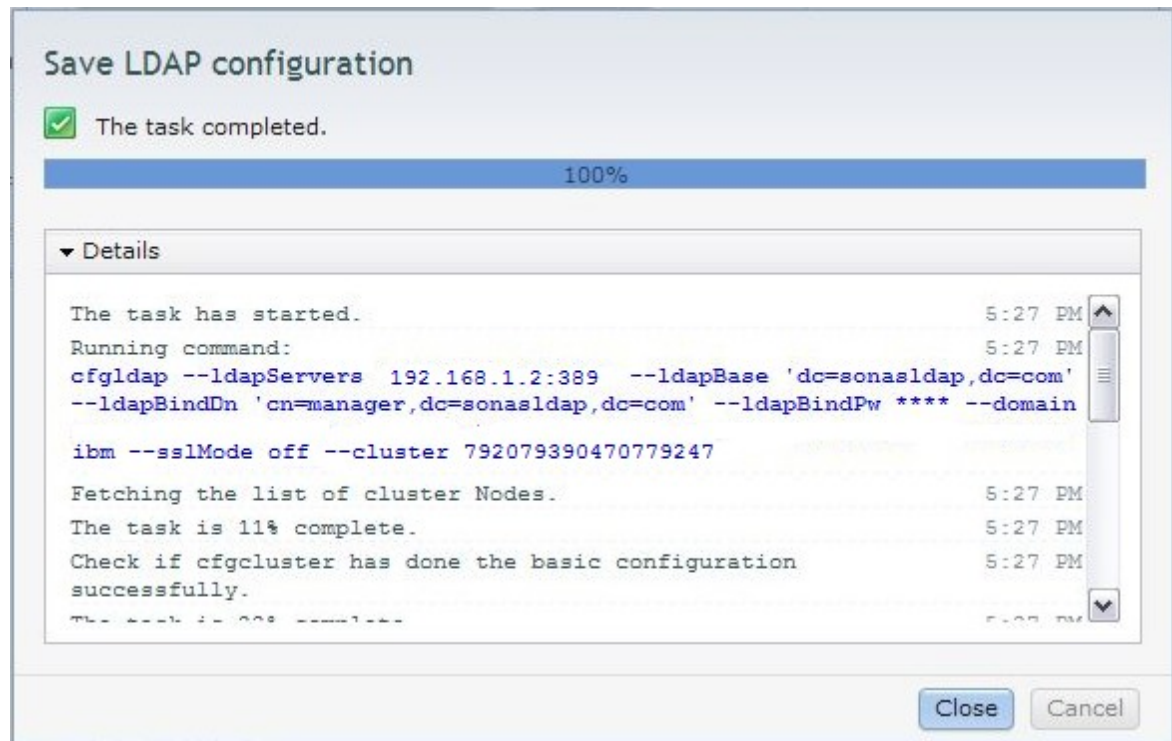


Figure 18: Successful completion of LDAP configuration

Secure LDAP

When to choose Storwize V7000 Unified with secure LDAP?

- Storwize V7000 Unified needs to be used in the IT infrastructure where LDAP is used as a Directory service and all user information is maintained in the same LDAP server.
- Storwize V7000 Unified needs to be used with both CIFS and NFS data access protocols.
- To have secure communication with LDAP server with SSL or TLS protocols.
- Customer wants to use remote replication.

What are the prerequisites for configuring Storwize V7000 Unified with secure LDAP?

- For CIFS protocol-based data access, extend schema. (The CIFS protocol requires more attributes than POSIX user objects (mainly to store SID, Windows password hash and domain information, and so on)).
- To support secure communication between Storwize V7000 Unified and LDAP server using SSL / TLS, you need to have LDAP server certificate.

How to configure Storwize V7000 Unified with secure LDAP using CLI?

The **cfgldap** command configures Storwize V7000 Unified with LDAP:

```
cfgldap -s <ldapServers> -b <ldapBase> -D <ldapBindDn> [-p <ldapBindPw>] [--  
krbKDC <krbKdc>] [--krbRealm <krbRealm>] [--krbKeytabFile <krbKeytabFile>] [--  
caCertFile <caCertFile>] [--ldapUserSuffix <ldapUserSuffix>] [--ldapGroupSuffix  
<ldapGroupSuffix>] [--sslMode <sslMode>] [-c <clusterID | clusterName >]
```

Warning: Storwize V7000 Unified must not be configured with any authentication method, before using **cfgldap**.

Example of configuring Storwize V7000 Unified with secure LDAP

To configure Storwize V7000 Unified with secure LDAP:

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth  
EFSSG0571I Cluster st001.virtual11.com is not configured with any type of  
authentication server.
```

2. Run **cfgldap** to configure Storwize V7000 Unified with secure LDAP with SSL.

```
[st001.mgmt001st001 ~]# cfgldap -s ldap1 -b dc=sonasldap,dc=com -D  
cn=manager,dc=sonasldap,dc=com -p secret --sslMode ssl --caCertFile  
/etc/cacert/cacert.pem  
(1/9) Fetching the list of CTDB cluster Nodes.  
(2/9) Check if cfgcluster has done the basic configuration successfully.  
(3/9) Check whether Interface nodes are reachable from management node  
(4/9) LDAP Configuration started  
(5/9) Check whether LDAP server is reachable from Interface nodes  
(6/9) Verification of LDAP server from a node using credentials provided  
(7/9) Updating the system with LDAP configuration details  
(8/9) Finalizing configuration  
(9/9) Updating the database  
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that LDAP authentication method is configured with SSL. (This step is optional)

```
[st001.mgmt001st001 ~]# lsauth  
clusterName = st001.virtual11.com  
ldapUri = ldaps://ldap1  
nscdMode = on  
ldapBindDn = cn=manager,dc=sonasldap,dc=com  
sslMode = on  
AUTH_TYPE = ldap  
ldapVersion = 3  
ldapBase = dc=sonasldap,dc=com  
caCertFile = /etc/cacerts/cacert.pem  
krbMode = off  
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with secure LDAP using the GUI?

To configure Storwize V7000 Unified with secure LDAP using the GUI:

1. Select **LDAP** as the authentication method and click **Next**.

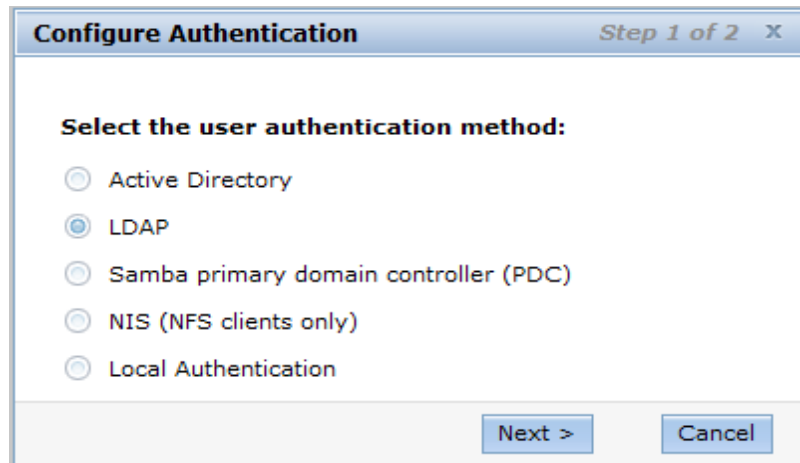


Figure 19: Specifying the authentication method for LDAP

2. Specify LDAP Server host name or IP address along with port number, search base for users and groups, bind distinguished name and password, and workgroup that this system should be part of. Security method needs to be set to **ssl** or **tls**. Specify the LDAP server certificate and click **Upload**.

LDAP Step 2 of 2

*** Specify one or more LDAP servers:**

LDAP Server	Port	
192.168.1.2	636	+ X

*** Search base for users and groups:**

*** Bind distinguished name (DN):**

*** Bind password:**

*** Confirm bind password:**

User suffix:

Group suffix:

*** Workgroup:**

Security Method:

Certificate:

Figure 20: Specifying LDAP parameters

3. After the certificate file is successfully uploaded, click **Finish**.

LDAP

Step 2 of 2

* Specify one or more LDAP servers:

LDAP Server	Port	
192.168.1.2	636	+ x

* Search base for users and groups:

dc=sonasldap,dc=com

* Bind distinguished name (DN):

cn=manager,dc=sonasldap,dc=com

* Bind password:

.....

* Confirm bind password:

.....

User suffix:

Group suffix:

* Workgroup:

ibm

Security Method:

SSL

Certificate:

Upload succeeded

Browse...

< Back

Finish

Cancel

Figure 21: Successful completion of file upload

4. Wait for successful completion of configuration and then click **Close**.

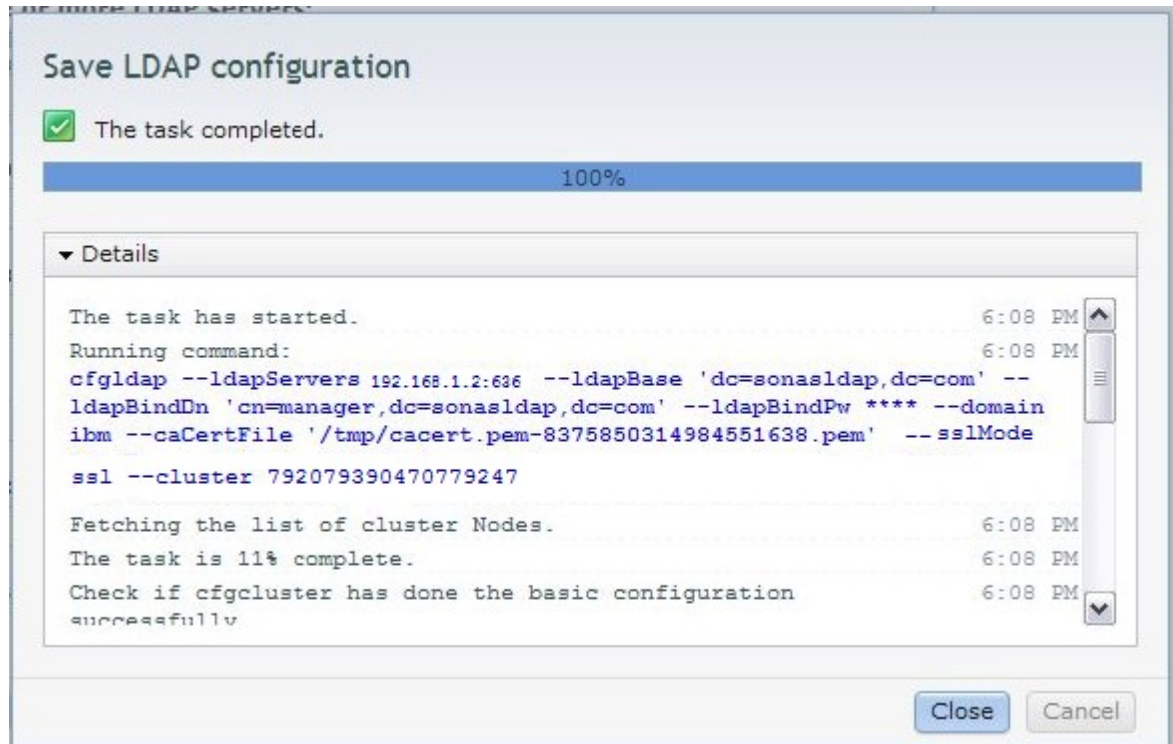


Figure 22: Successful completion of LDAP configuration

Secure LDAP and MIT Kerberos

When to choose Storwize V7000 Unified with secure LDAP and MIT Kerberos

- Existing environment is based on an LDAP directory service
- Secure communication with LDAP server using SSL or TLS protocol is required.
- NAS services are required to be Kerberos server enabled (which increases security by not sending passwords in clear text over the wire to Storwize V7000 Unified.)
- Customer wants to use remote replication.

What are the prerequisites for configuring Storwize V7000 Unified with secure LDAP and MIT Kerberos?

- Existing Kerberos infrastructure is configured and accessible from Storwize V7000 Unified.
- LDAP server certificate is available (to support secure communication between Storwize V7000 Unified and LDAP server using SSL / TLS).

- KeyTab file to authenticate to the Kerberos Key Distribution Center (KDC) is available (to support secure communication between Storwize V7000 Unified and systems accessing file services using Kerberos.)

What are the limitations of Storwize V7000 Unified with LDAP and MIT Kerberos?

- Storwize V7000 Unified does not support kerberized data access using the following protocols:
 - FTP
 - HTTPS
 - SCP
- Only NFSv3 and CIFS protocol support kerberized data access.
- The user's SID is comprised of the user's RID and SID of the domain account created in the LDAP server after Storwize V7000 Unified LDAP based authentication configuration. For example, a Storwize V7000 Unified machine with the NetBIOS name, **st001** will have an entry in the following format:

```
dn: sambaDomainName=ST001,dc=sonasldap,dc=com
sambaDomainName: ST001
sambaSID: S-1-5-21-3315143710-1287377127-4281028267
```

So the users should have SID of the format <domain account SID>- <RID>

For example, for **st001**, it should be S-1-5-21-3315143710-1287377127-4281028267-<RID>.

Refer to the Information Center to find more information on the following topic:

Administering > Administering the file system> Managing > Managing authentication and ID mapping > Setting up LDAPserver prerequisites > Updating LDAP user information with unique Samba attributes

How to configure Storwize V7000 Unified with secure LDAP and MIT Kerberos using CLI?

The **cfgldap** command configures Storwize V7000 Unified with secure LDAP and Kerberos.

Example of configuring Storwize V7000 Unified with secure LDAP and Kerberos

To configure Storwize V7000 Unified with secure LDAP and Kerberos:

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]$ lsauth
EFSSG0571I Cluster st001.virtual1.com is not configured with any type of
authentication server.
```

2. Run **cfgldap** to configure Storwize V7000 Unified with secure LDAP and Kerberos KDC. With secure communication between Storwize V7000 Unified and LDAP server based on SSL protocol.

```
[st001.mgmt001st001 ~]# cfgldap -s ldap1 -b dc=sonasldap,dc=com -D
cn=manager,dc=sonasldap,dc=com -p secret -d virtual1.com --krbKDC ldap1
--krbRealm PUNE-KDC.COM --krbKeytabFile /root/krb5.keytab --sslMode ssl
--caCertFile /root/cacert.pem
```

```
(1/9) Fetching the list of CTDB cluster Nodes.
(2/9) Check if cfgcluster has done the basic configuration successfully.
(3/9) Check whether Interface nodes are reachable from management node
(4/9) LDAP Kerberos Configuration started
(5/9) Check whether LDAP server is reachable from Interface nodes
(6/9) Verification of LDAP server from a node using credentials provided
(7/9) Updating the system with LDAP-KRB configuration details
(8/9) Finalizing configuration
(9/9) Updating the database
EFSSG1000I The command completed successfully.
```

3. Run `lsauth` to verify that LDAP authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth
ldapUri = ldaps://ldap1
clusterName = st001.virtual11.com
nscdMode = on
krbKeytabFile = /etc/krb5.keytab
ldapBindDn = cn=manager,dc=sonasldap,dc=com
krbKdc = ldap1
sslMode = on
AUTH_TYPE = ldap_krb
ldapVersion = 3
krbRealm = KDC.COM
ldapBase = dc=sonasldap,dc=com
krbMode = on
caCertFile = /etc/cacerts/cacert.pem
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified with secure LDAP and MIT Kerberos using the GUI?

This is not supported in current release. Use the CLI method to complete this configuration.

How to configure Storwize V7000 Unified with LDAP and MIT Kerberos using the GUI?

To configure Storwize V7000 Unified with LDAP and MIT Kerberos using the GUI:

1. Select **LDAP** as the authentication method and click **Next**.



Figure 23: Specifying the authentication method for LDAP

- LDAP

Step 2 of 2

* Specify one or more LDAP servers:

LDAP Server	Port	
192.168.1.2	389	+ X

* Search base for users and groups:

dc=sonasldap,dc=com

* Bind distinguished name (DN):

cn=manager,dc=sonasldap,dc=com

* Bind password:

* Confirm bind password:

User suffix:

Group suffix:

* Workgroup:

ibm

Security Method:

off

☒ Enable Kerberos

* Server Name:

192.168.1.2

* Realm:

PUNE-KDC.COM

* Key Tab File:

Browse... C:\fakepath\krb5.keytab Upload Cancel

< Back Finish Cancel

Figure 24: Specifying LDAP parameters

3. After the key tab file is successfully uploaded, click **Finish**.

LDAP

Step 2 of 2

* Specify one or more LDAP servers:

LDAP Server

Port

192.168.1.2

389

+×

* Search base for users and groups:

dc=sonasldap,dc=com

* Bind distinguished name (DN):

cn=manager,dc=sonasldap,dc=com

* Bind password:

.....

* Confirm bind password:

.....

User suffix:

Group suffix:

* Workgroup:

ibm

Security Method:

off

☒ Enable Kerberos

* Server Name:

192.168.1.2

* Realm:

PUNE-KDC.COM

* Key Tab File:

Upload succeeded

Browse...

< Back

Finish

Cancel

Figure 25: Successful completion of key tab file upload

Wait for successful completion of configuration, and then click **Close**.

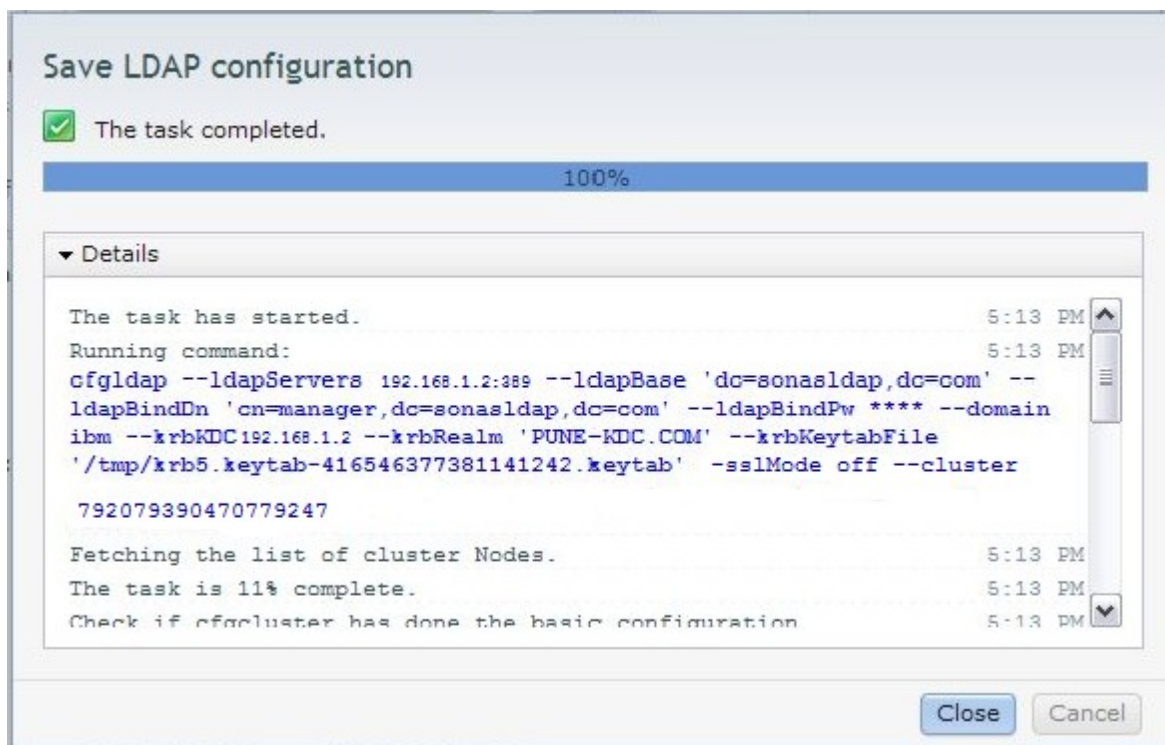


Figure 26: Successful completion of LDAP and Kerberos configuration

Storwize V7000 Unified with Local Authentication

Customers who don't have external authentication servers or those who don't want to configure them can configure Storwize V7000 Unified to use Local Authentication. Local Authentication supports up to 1000 users and 100 groups.

When to choose Storwize V7000 Unified with Local Authentication?

- Storwize V7000 Unified will be used in an IT infrastructure without any authentication servers such as AD, LDAP, etc.
- Customer does not need to configure more than 1000 users and 100 groups.
- Customer does not want to use remote replication.

What are the limitations of Storwize V7000 Unified with Local Authentication?

1. Currently there is no support for importing / exporting user and group data from another authentication server to local authentication server.
2. Local (NAS) User names and local (NAS) Group names are case insensitive.
3. Secured (kerberized) CIFS / NFS based access is not supported.
4. Local authentication server cannot be used as an external authentication server in customer infrastructure.
5. Async replication is not supported.

How to configure Storewise V7000 Unified with Local Authentication using CLI?

The **cfglocalauth** command configures Storwize V7000 Unified with Local authentication,

```
cfglocalauth [-c < clusterID | clusterName >]
```

Warning: Storwize V7000 Unified must not be configured with any authentication method, before using **cfglocalauth**.

Example of configuring Storewise V7000 Unified with Local Authentication:

To configure the Storwize V7000 Unified system with local authentication:

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]$lsauth
EFSSG0571I Cluster st001.virtual1.com is not configured with any type of
authentication server
```

2. Run command **cfglocalauth** to configure Storewise V7000 Unified with Local Authentication

```
[st001.mgmt001st001 ~]# cfglocalauth
(1/6) Setting up the Local authentication server
(2/6) Local authentication configuration started
(3/6) Verification of Local authentication server
(4/6) Updating the system with Local authentication configuration
details
(5/6) Finalizing configuration.
(6/6) Updating the database.
EFSSG1000I The command completed successfully.
```

3. Run command **lsauth** to verify that Local Authentication is configured.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = local
LocalAuthServerName = localserver
idMappingMethod = none
clusterName = st001.virtual1.com
LocalAuthServerSID = S-1-5-21-270495115-3834229809-3311785262
EFSSG1000I The command completed successfully.
```

To start using the system for NAS based access it is must to add users and groups when local authentication is configured. Set of CLI commands have been provided to help create the users and

groups.

1. Run command **mknasgroup** to add a group.

```
[st001.mgmt001st001 ~]# mknasgroup grp1
EFSSG1000I The command completed successfully.
```

2. Run command **lsnasgroup** to list groups.

```
[st001.mgmt001st001 ~]# lsnasgroup
Group Name Group ID
grp1      1024
EFSSG1000I The command completed successfully.
```

3. Run command **mknasuser** to add a user.

```
[root@99k4927.mgmt001st001 ~]# mknasuser usr1 -p password123 -g grp1
EFSSG1000I The command completed successfully.
```

4. Run command **lsnasuser** to list users.

```
[st001.mgmt001st001 ~]# lsnasuser
User Name User ID Primary Group Supplementary Group
Email ID
usr1      1024      grp1
EFSSG1000I The command completed successfully.
```

5. Run command **chnasuser** to modify user properties. In this example we modify password.

```
[st001.mgmt001st001 ~]# chnasuser usr1 -p newpassword
EFSSG1000I The command completed successfully.
```

To enable the NAS user to change their own password an HTML portal can be accessed hosted on the public IP's served by the nodes of the cluster. The URL to access the webpage is:

<https://<Public IP or Cluster Name>/changepassword.html>

6. Run command **rmnasuser** to remove a user.

```
[st001.mgmt001st001 ~]# rmnasuser usr1
Do you really want to perform the operation (yes/no - default no):yes
EFSSG1000I The command completed successfully.
```

7. Run command **rmnasgroup** to remove a group.

```
[st001.mgmt001st001 ~]# rmnasgroup grp1
Do you really want to perform the operation (yes/no - default no):yes
EFSSG1000I The command completed successfully.
```

How to configure Storewize V7000 Unified with Local Authentication using GUI?

To configure Storewize V7000 Unified with Local Authentication using GUI:

1. Select **Local Authentication** as authentication method and click **Finish**.

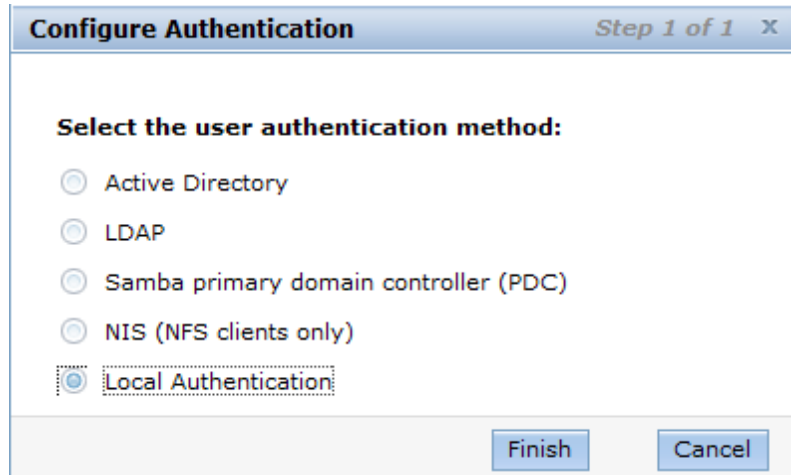


Figure 27: Specifying the authentication method as Local Authentication

2. Wait for successful completion of configuration.
3. To add a group, select **Groups** tab on the left pane and click on **New Group** button on the top. Specify Group Name and Group ID (if required) and click **OK**.

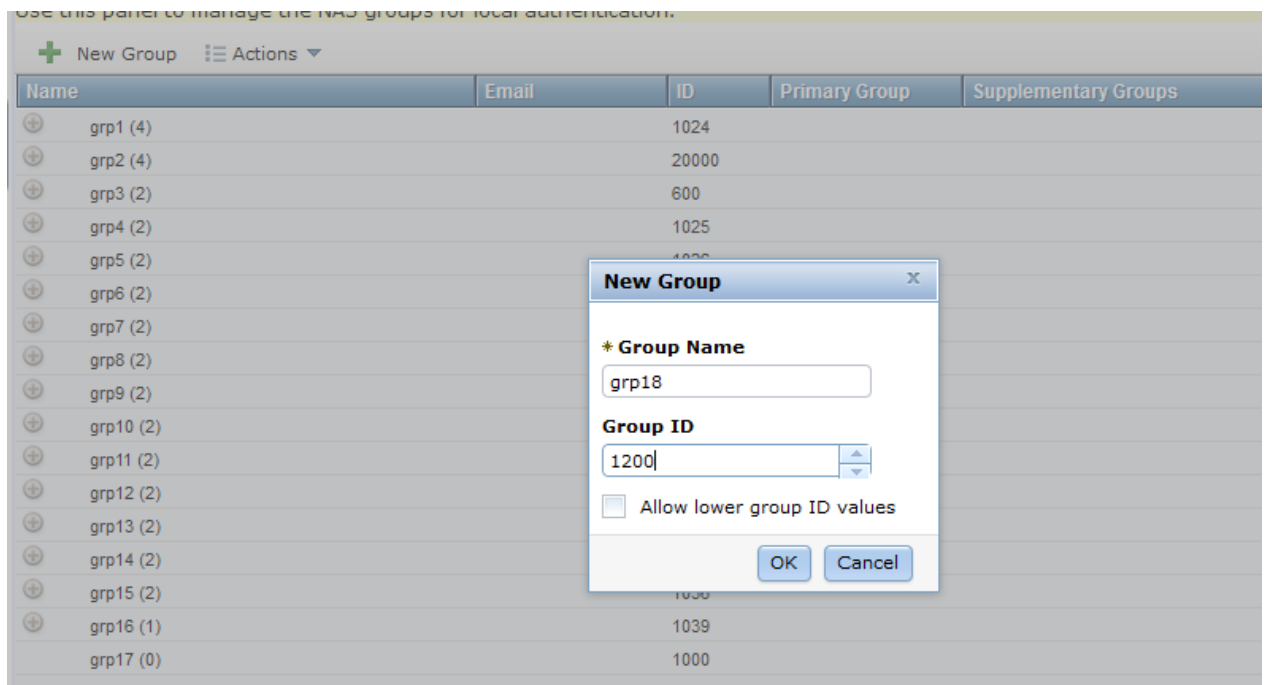


Figure 28: Adding group

4. Wait for successful completion and click **Close**.
5. To add user, select **Users** tab on the left and click on **New User** button on the top. Specify User Name and other details and click **OK**.

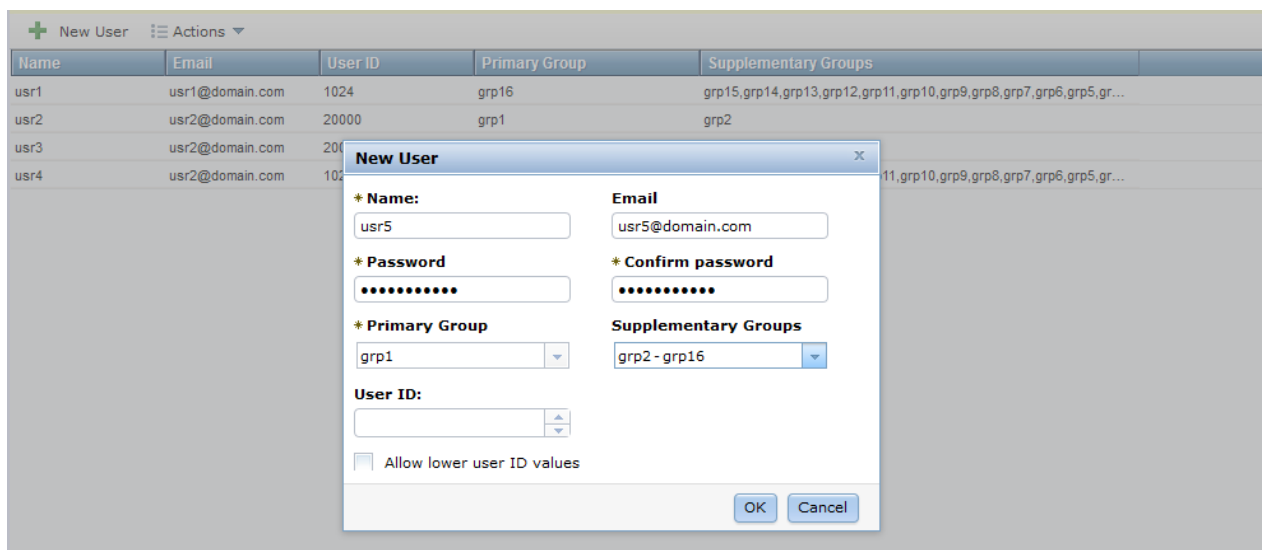
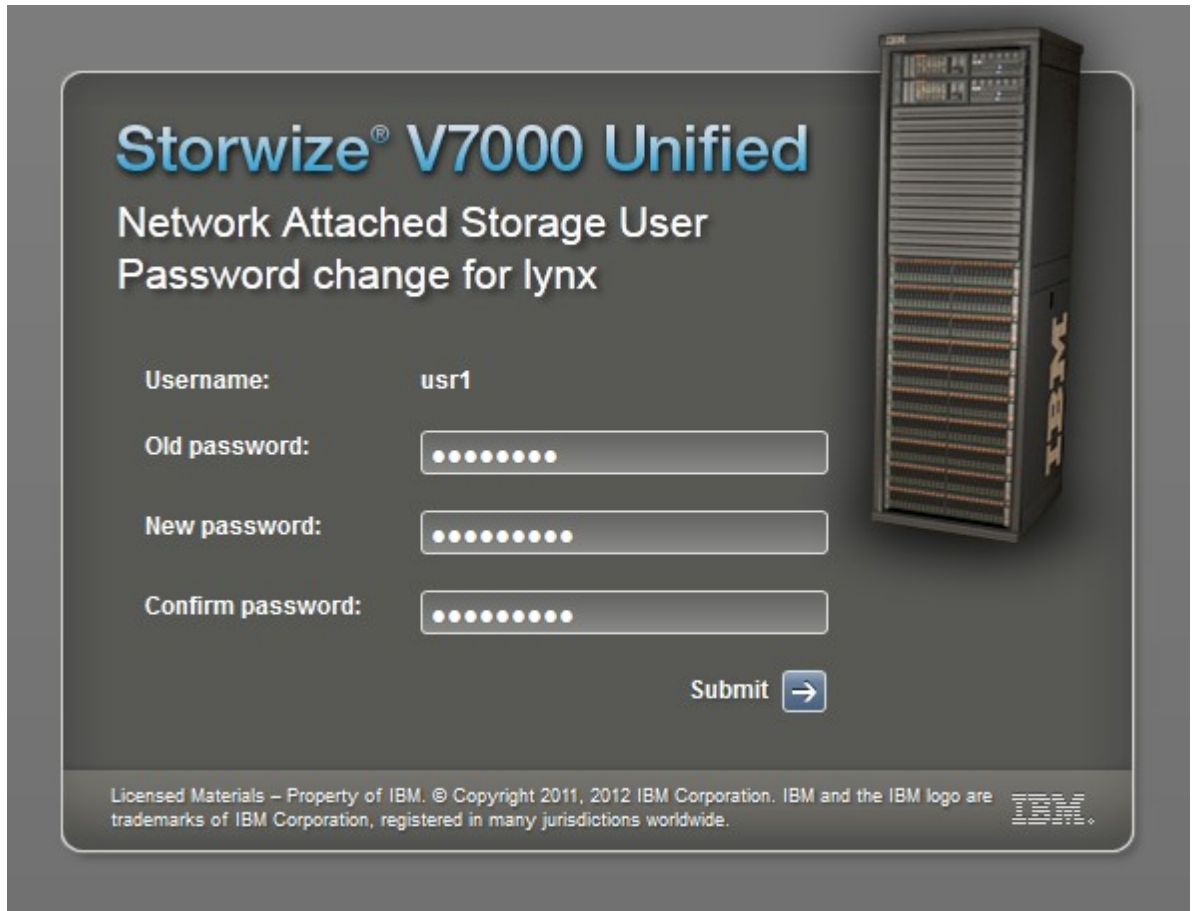


Figure 29: Adding User

6. To modify user properties, select **Users** tab on the left pane, click on the **user**, and select operation from **Action** list on the top.
7. To remove a group, select **Groups** tab on the left pane, click on the **group**, and select operation from **Action** list on the top.
8. For a user to change his/her password, use the link <https://<Public IP or Cluster Name>/changepassword.html>.



The screenshot displays a web-based interface for changing a user's password on an IBM Storwize V7000 Unified Network Attached Storage system. The interface is titled "Storwize® V7000 Unified Network Attached Storage User Password change for lynx". It features four input fields: "Username:" with the value "usr1", "Old password:", "New password:", and "Confirm password:", each followed by a masked password field represented by dots. A "Submit" button with a right-pointing arrow is located at the bottom right of the form. To the right of the form is a 3D rendering of the IBM Storwize V7000 server rack. At the bottom of the interface, there is a copyright notice: "Licensed Materials – Property of IBM. © Copyright 2011, 2012 IBM Corporation. IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide." followed by the IBM logo.

Figure 30: Changing Password

Netgroup basic concepts

What are netgroups

Generally, netgroups are used in UNIX environments to control access for NFS exports, remote logins, and remote shells. Each netgroup has a unique name and builds a set of hosts, users, groups, and other netgroups.

Where are netgroups maintained?

Originally netgroups were introduced with Sun Microsystem's NIS. Netgroups could also be stored in LDAP, a server with NIS in SFU, or in local files.

Storwize V7000 Unified storage support for netgroups

Which elements of netgroups are supported by Storwize V7000 Unified?

Storwize V7000 Unified storage system supports netgroups for the only purpose of grouping hosts to restrict access to NFS file systems exported by Storwize V7000 Unified

What is the Storwize V7000 Unified support matrix for netgroups?

Netgroup database	Authentication	ID mapping	CLI command to configure
NIS	None	None	cfgnis
NIS	AD	Auto	cfgad, cfgnis
NIS	AD	NIS	cfgad, cfgnis
NIS	AD	SFU	cfgad, cfgsfu, cfgnis
LDAP	LDAP	LDAP	cfgldap

Configuration for authentication *none* and ID mapping *none*

If Storwize V7000 Unified storage is to be configured with no authentication and no ID mapping, and netgroups from NIS, then follow the steps listed below -

Example-

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]$lsauth
EFSSG0571I Cluster st001.virtual1.com is not configured with any type of
authentication server.
```

2. Run **cfgnis**

```
[st001.mgmt001st001 ~]# cfgnis -d Nis --serverMap 192.168.1.3:Nis
(1/9) Check if basic NIS can be configured on the system.
(2/9) Fetching the list of CTDB cluster Nodes.
(3/9) Check whether Interface nodes are reachable from management node
(4/9) Check if primary NIS domain is served by any NIS server or not
(5/9) Checking if primary NIS domain is reachable from all interface
nodes or not
(6/9) Verifying NIS server
(7/9) Setting values into the registry
(8/9) Finalizing configuration
(9/9) Updating the database
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that NIS method is configured.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = nis
NIS_ServerMap = 192.168.1.3:Nis
idMappingMethod = none
clusterName = st001.virtual1.com
NIS_Domain = Nis
EFSSG1000I The command completed successfully.
```

Note: In above configuration, only NFS protocol is supported.

Configuration for **AD authentication and auto ID mapping**

If Storwize V7000 Unified storage is configured with AD authentication and auto ID mapping, then the **cfgnis** command must be run to lookup netgroups in NIS.

Example -

1. Run **lsauth** to verify that authentication method configured is AD.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ad
idMapConfig = 10000000-299999999,1000000
idMappingMethod = auto
domain = virtual1
clusterName = st001.virtual1.com
userName = administrator
adHost = ad1.virtual1.com
passwordServer = *
realm = virtual1.com
EFSSG1000I The command completed successfully.
```

2. Run **cfgnis**

```
[st001.mgmt001st001 ~]# cfgnis -d Nis --serverMap 192.168.1.3:Nis
(1/9) Check if NIS can be extended or not. Checking if authentication
type is AD or NT4
(2/9) Fetching the list of CTDB cluster Nodes.
(3/9) Check whether Interface nodes are reachable from management node
(4/9) Check if primary NIS domain is served by any NIS server or not
(5/9) Checking if primary NIS domain is reachable from all interface
nodes or not
(6/9) Verifying NIS server
(7/9) Setting values into the registry
(8/9) Finalizing configuration
(9/9) Updating the database
EFSSG1000I The command completed successfully.
```

3. Run **lsauth**

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ad
NIS_ServerMap = 192.168.1.3:Nis
idMapConfig = 10000000-299999999,1000000
domain = VIRTUAL1
idMappingMethod = auto
clusterName = st001.virtual1.com
userName = administrator
adHost = AD1.VIRTUAL1.COM
NIS_Domain = Nis
passwordServer = *
realm = VIRTUAL1.COM
EFSSG1000I The command completed successfully.
```

Configuration for AD authentication and NIS ID mapping

If Storwize V7000 Unified storage is configured with AD authentication and NIS ID mapping, then netgroups in NIS are already configured.

Example-

1. Run **lsauth** to verify that the authentication method configured is AD.

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ad
idMapConfig = 10000000-299999999,1000000
idMappingMethod = auto
domain = virtual1
clusterName = st001.virtual1.com
userName = administrator
adHost = ad1.virtual1.com
```

```
passwordServer = *  
realm = virtual1.com  
EFSSG1000I The command completed successfully.
```

2. Run **cfgnis**

```
[st001.mgmt001st001 ~]# cfgnis --extend -d Nis --serverMap  
192.168.1.3:Nis --domainMap virtual1:Nis --idmapUserRange 200000-300000  
--idmapGroupRange 300001-400000 --useAsIdmap  
(1/9) Check if NIS can be extended or not.Checking if authentication  
type is AD or NT4  
(2/9) Fetching the list of CTDB cluster Nodes.  
(3/9) Check whether Interface nodes are reachable from management node  
(4/9) Check if primary NIS domain is served by any NIS server or not  
(5/9) Checking if primary NIS domain is reachable from all interface  
nodes or not  
(6/9) Verifying NIS server  
(7/9) Setting values into the registry  
(8/9) Finalizing configuration  
(9/9) Updating the database  
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that AD authentication method is configured with NIS ID Mapping

```
[st001.mgmt001st001 ~]# lsauth  
idMapConfig = 1024-4294967295,1  
domain = virtual1  
clusterName = st001.virtual1.com  
adHost = ad1.virtual1.com  
NIS_Domain = Nis  
realm = virtual1.com  
AUTH_TYPE = ad  
idMapUserRange = 200000-300000  
NIS_ServerMap = 192.168.1.3:Nis  
idMappingMethod = nis  
userName = Administrator  
NIS_virtual1 = Nis:none  
passwordServer = *  
idMapGroupRange = 300001-400000  
EFSSG1000I The command completed successfully.
```

Configuring authentication **AD** and ID mapping **SFU**

If Storwize V7000 Unified system is configured with AD authentication and SFU ID mapping, then the **cfgnis** command must be run to lookup netgroups in NIS.

1. Run **lsauth** to verify that system is configured with AD authentication along with SFU for ID mapping

```
[st001.mgmt001st001 ~]# lsauth
```

```

AUTH_TYPE = ad
SFU_virtual11 = ad,12000-99999,sfu
idMapConfig = 10000000-299999999,1000000
domain = virtual11
idMappingMethod = sfu
clusterName = st001.virtual11.com
userName = administrator
adHost = ad1.virtual11.com
passwordServer = *
realm = virtual11.com
EFSSG1000I The command completed successfully.

```

2. Run **cfgnis** to configure Storwize V7000 Unified to lookup netgroups from NIS.

```

[st001.mgmt001st001 ~]# cfgnis -d Nis --serverMap 192.168.1.3:Nis
(1/9) Check if NIS can be extended or not.Checking if authentication
type is AD or NT4
(2/9) Fetching the list of cluster Nodes.
(3/9) Check whether Interface nodes are reachable from management node.
(4/9) Check if primary NIS domain is served by any NIS server or not.
(5/9) Checking if primary NIS domain is reachable from all interface
nodes or not.
(6/9) Verification of NIS server serving the primary domain provided.
(7/9) Updating the system with the NIS configuration details.
(8/9) Finalizing configuration.
(9/9) Updating the database.
EFSSG1000I The command completed successfully.

```

3. Run **lsauth** to verify that AD authentication method is configured with SFU ID mapping and NIS:

```

[st001.mgmt001st001 ~]#lsauth
AUTH_TYPE = ad
SFU_virtual11 = ad,12000-99999,sfu
NIS_ServerMap = 192.168.1.3:Nis
idMapConfig = 10000000-299999999,1000000
domain = virtual11
idMappingMethod = sfu
clusterName = st001.virtual11.com
userName = administrator
adHost = ad1.virtual11.com
NIS_Domain = Nis
passwordServer = *
realm = virtual11.com
EFSSG1000I The command completed successfully.

```

Configuring authentication LDAP and id mapping LDAP

If Storwize V7000 Unified system is configured with LDAP authentication then netgroups from LDAP are implicitly supported.

1. Run **lsauth** to verify that no authentication method is configured.

```
[st001.mgmt001st001 ~]# lsauth
EFSSG0571I Cluster st001.virtual11.com is not configured with any type of
authentication server.
```

2. Run **cfgldap** to configure Storwize V7000 Unified with LDAP.

```
[st001.mgmt001st001 ~]# cfgldap -s ldap1 -b dc=sonasldap,dc=com -D
cn=manager,dc=sonasldap,dc=com -p secret
(1/9) Fetching the list of cluster Nodes.
(2/9) Check if cfgcluster has done the basic configuration successfully.
(3/9) Check whether Interface nodes are reachable from management node.
(4/9) LDAP Configuration started.
(5/9) Check whether LDAP server is reachable from Interface nodes.
(6/9) Verification of LDAP server from a node using credentials
provided.
(7/9) Updating the system with LDAP configuration details.
(8/9) Finalizing configuration.
(9/9) Updating the database.
EFSSG1000I The command completed successfully.
```

3. Run **lsauth** to verify that LDAP authentication method is configured,

```
[st001.mgmt001st001 ~]# lsauth
AUTH_TYPE = ldap
ldapVersion = 3
clusterName = st001.virtual11.com
ldapUri = ldap://ldap1
ldapBase = dc=sonasldap,dc=com
nscdMode = on
ldapBindDn = cn=manager,dc=sonasldap,dc=com
krbMode = off
sslMode = off
EFSSG1000I The command completed successfully.
```

How to configure Storwize V7000 Unified storage NFS export with a netgroup?

Storwize V7000 Unified command **mkexport** is used to configure NFS export with netgroup.

```
mkexport testnetgrp /ibm/gpfs0/netgroup --nfs "@myntgrp(rw,
no_root_squash)" --owner testuser1
```

Warning: It is very important to prepend **@** to the netgroup name. If one does not use '@' , then Storewize V7000 Unified server will treat that name as a client host. In case you neglect to prepend the '@' remove the export and create it again with '@'

Can netgroups be used to control access for other NAS protocols than NFS?

No.

How to check how Storwize V7000 Unified resolves a netgroup?

There is currently no Storwize V7000 Unified CLI command to verify how Storwize V7000 Unified resolves netgroups. As of this release, you would need to use a direct Linux command; see next.

Which Linux command can be used to look-up a netgroup?

The following Linux command can be used to check netgroup information. Root access is required on Storwize V7000 Unified to execute following command.

```
getent netgroup <Netgroup Name>
```

Which format must be used to specify a host in a netgroup?

A host can be specified by:

- Its name, myhost
- Its fully qualified domain name, myhost.mydom.com

It is not recommended to use IP addresses in netgroup definitions because NFS inherently works with host names for netgroups.

Note: The hostname used in the netgroup definition must have both forward and reverse DNS lookup configured. Thus, Storwize V7000 Unified must be able to resolve both the hostname and the host IP with which mount service is requested on Storwize V7000 Unified. Otherwise, mount might fail with an “access denied” error.

Options in absence of external authentication server

What should you do if you do not have external authentication server?

Local Authentication (please see section on Local Authentication for details) can be used if the customer does not need more than 1000 users and more than 100 groups. Otherwise, configuring OpenLDAP is one of the possible solution approaches. Perform the following steps to configure OpenLDAP.

1. Select any of the suitable Linux distribution that supports OpenLDAP. Install Linux operating system on the server on which you intend to install LDAP server.

Note: Refer to the documentation of selected Linux for complete prerequisite and installation procedure.

2. Install and configure OpenLDAP Server on Linux machine prepared in the previous step.

Note: Refer to the OpenLDAP documentation for pre-requisite, installation, and configuration of OpenLDAP server.

3. Create the required users and groups with LDAP server.

Note: Refer to the OpenLDAP documentation for user and group management.

4. For CIFS protocol-based data access, extend schema. (The CIFS protocol requires more attributes than POSIX user objects (mainly to store SID, Windows password hash and domain information, and so on)).

You can find more details in the following InfoCenter section:

Administering > Administering the file system > Managing > Managing authentication and ID mapping > Setting up LDAP server prerequisites

and

Administering > Administering the file system > Managing > Managing authentication and ID mapping > Setting up LDAP server prerequisites > Updating LDAP user information with unique Samba attributes

Refer to the “Storwize V7000 Unified with LDAP” section for configuring Storwize V7000 Unified authentication against LDAP.

Limitations

Consider the following authentication limitations when configuring and managing the Storwize V7000 Unified system:

4. An external authentication source is required to configure IBM Storwize V7000 Unified, unless local authentication option is used. Storwize V7000 Unified can be configured with only one external authentication source. We do support multiple Active Directories in trust with the Active Directory which is configured with IBM Storwize V7000 Unified, however multiple independent Active Directories cannot be configured with IBM Storwize V7000 Unified.
5. Authentication choice has to be made carefully since the Authentication method cannot be changed once configured.
6. When Storwize V7000 Unified system is configured with LDAP + Kerberos authentication, kerberized access for CIFS and NFS protocols is supported ; FTP, SCP and HTTPS are not kerberized.
7. For Active Directory (AD) with the Services for Unix (SFU) UID/GID/SID mappings extension:
 - a. Enabling SFU for a trusted domain requires a two-way trust between the principal and the trusted domain.
 - b. To access the Storwize V7000 Unified system, users and groups must have a valid UID/GID assigned to them in Active Directory. Allowed range is between 1 and 4294967295, both inclusive. It is advisable to keep the lower range greater than 1024 to avoid conflict with the CLI users. Invoking the command with lower range less than 1024 will generate a warning message and ask for confirmation. Use --force option to override it.
 - c. For user access, the primary group on the Storwize V7000 Unified system is the Microsoft Windows Primary group, not the Unix primary group that is listed in the Unix attribute tab in the user's properties. Therefore, the user's primary Microsoft Windows group must be assigned a valid GID.
8. For Active Directory (AD) with the Network Information Service (NIS) mappings extension:
 - a. Since Unix style names do not allow spaces in the name, the following conventions for mapping Active Directory users and groups to NIS are implemented:
 - i. Convert all upper case characters to lower case characters.
 - ii. Replace every space character with the underscore character. For example, an Active Directory user named CAPITAL Name has the corresponding name capital_name on NIS.

Note that the side effect of this is that if a user in AD had an underscore character, it cannot be supported because we would lookup a name after replacing underscore with a blank but such a user will not exist in AD

- b. We do not have a provision of user name mapping for AD user names to NIS user names (to handle the case of names with special characters in AD compared to NIS).
 - c. For CIFS access, we resolve group membership as defined in AD (ie do not lookup membership of a user for group defined in NIS; therefore authorization will be based on groups defined in AD (using groups defined in NIS but not in AD will result in inconsistent and unexpected results).
 - d. In this AD with NIS mappings extension configuration, some restrictions apply when using the `lsquota` and `setquota` Storwize V7000 Unified CLI commands. See the man pages for `lsquota` and `setquota` for details.
9. A user cannot belong to more than 1000 groups.
10. When IBM Storwize V7000 Unified is configured with Active Directory, we do not support `sidHistory` attribute of the user. Therefore if we try to migrate files from a storage which supports `sidHistory`, it will result in data access issues with resources that rely on the use of `sidHistory` on the source system.
11. IBM Storwize V7000 Unified configured with Active Directory cannot use LDAP as an ID mapping source.
12. If Active Directory is already configured on the Storwize V7000 Unified system, you can only use the `--idMapConfig` option of the `cfgad` Storwize V7000 Unified CLI command to change the high value of the range, and the high value of the range can only be changed to a higher value. You cannot change the high value of the range to a lower value. You cannot change the low value of the range, and you cannot change the range size. For example, if you used the `cfgad` Storwize V7000 Unified CLI command with the `--idMapConfig` option to configure Active Directory specifying a value for the `--idMapConfig` option as `3000-10000:2000`, you can only use the `cfgad` Storwize V7000 Unified CLI command with the `--idMapConfig` option to increase the value 10000 for the high value of the range. You cannot decrease the value of 10000 for the high value of the range. You cannot change the value 3000 for the low value of the range, and you cannot change the value 2000 for the range size.
13. Although, change of authentication and ID Mapping is not advised, if there is pressing need to change from NIS ID mappings to Active Directory ID mappings, or to change the ID mapping parameters of an already existing Active Directory configuration by using the `--idMapConfig` option of the `cfgad` Storwize V7000 Unified CLI command, either to change the low value of the range, decrease the high value of the range, or change the range size, you must perform the following steps in the following sequence:
- a. Submit the `cleanupauth` Storwize V7000 Unified CLI command and do not specify the `--idmapDelete` option.
 - b. Submit the `cleanupauth` Storwize V7000 Unified CLI command and do specify the `--idmapDelete` option.
 - c. Submit the `cfgad` Storwize V7000 Unified CLI command with the options and values that you want for the new Active Directory configuration.

Important: If you do not perform the above three steps in sequence, results are unpredictable and can include complete loss of data access. Additionally, when you execute `cleanupauth` command, exiting data/exports cannot be accessed. Be very sure if you really want to change authentication or id mapping methods.

14. UIDs and GIDs less than 1024 are denied access for the FTP, SCP and HTTPS protocols for all of the supported authentication schemes other than Active Directory with SFU.

15. When using Microsoft Active Directory (AD) as an authentication mechanism, Storwize V7000 Unified supports only pre-Windows 2000 logon name (also known as the Netbios logon name) for authentication and not the User Principle Name (UPN). Note that AD replaces some of the special characters used in the UPN with the underscore character (hexadecimal value 0x5F) for the related pre-Windows 2000 logon name. For the complete list of the special characters that are replaced in the pre-Windows 2000 logon name, see Microsoft Active Directory documentation.

Follow these steps to locate the pre-Windows 2000 logon name for an AD domain user:

- a. From the Windows Start menu, select Administrative Tools > Active Directory Users and Computers.
- b. Right-click the AD Domain user for which you require the pre-Windows 2000 logon name.
- c. Select Properties > Account Tab and check the value of the User logon name (pre-Windows 2000): field.

16. Users with the same username from different organizational units of the LDAP server are denied access to CIFS shares without regard to the LDAP User Suffix and LDAP Group suffix values configured on the system.

17. Authentication configuration commands stop and restart the NAS services CIFS, NFS, FTP, SCP and HTTPS. This action is disruptive for clients that are connected. Connected clients lose their connection, and file operations are interrupted. File services resume a few seconds after an authentication configuration command completes.

Summary

This white paper introduced the basics of user authentication, authorization, ID mapping, directory service and netgroup. It explained the different authentication mechanisms, and ID mapping and netgroup configurations supported by the IBM Storwize V7000 Unified system with detailed information on when to select a particular authentication method along with the prerequisites, step-by-step setup procedure, and limitations of each configuration.

Refer to the “Resources” section for related information.

Resources

These websites provide useful references to supplement the information contained in this paper:

- IBM Systems on PartnerWorld
ibm.com/partnerworld/systems
- IBM Redbooks
ibm.com/redbooks
- IBM Publications Center
www.elink.ibm.link.ibm.com/public/applications/publications/cgibin/pbi.cgi?CTY=US
- IBM Storwize 7000 Unified Information Center
http://pic.dhe.ibm.com/infocenter/storwize/unified_ic/index.jsp

About the authors

Ulf Troppens is a security architect for IBM Storwize V7000 Unified and author of the award winning book, *Storage Networks Explained*.

Pankaj Ahire was an authentication lead for IBM Storwize V7000 Unified development.

Varun Mittal, **Kaustubh Katruwar**, and **Saurabh Gawande** are the members of the IBM Storwize V7000 Unified Authentication development team.

Trademarks and special notices

© Copyright IBM Corporation 2012.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.