Application Note

Using DirectControl with Network Appliance Filers

Published: January 2013

Abstract

This Application Note describes the integration between Network Appliance servers and Centrify DirectControl so that users authenticating with their Active Directory credentials to UNIX systems can access remote shares on the NetApp Filers with a consistent user ID and name mapping centrally managed by DirectControl.

Contents

Introduction

NetApp storage systems help enterprises to provide a highly available and scalable data storage service that delivers a higher level of data protection at a much lower cost of ownership. However, in a mixed environment where both Windows and UNIX systems need to access common files or directories, there is a need for a common security model to control access. Centrify DirectControl provides the interface to this common authentication method for non-Windows computers in an Active Directory environment.

Through proper configuration of the NetApp storage system, you can share a common volume to both a Windows network using the CIFS file- sharing protocol and a UNIX network using the NFS file-sharing protocol. Since it is possible for the user to access the same shared volume from either Windows or a UNIX system using two different file sharing protocols (CIFS and NFS), it is important that a mapping exists between the UNIX and Windows identities in order to preserve proper ownership and permission settings for files. If the user is accessing the volume from a Windows machine, the user's Windows identity is used. If the user is accessing the volume using NFS, the user's UNIX identity is used.

Centrify DirectControl provides an identity mapping mechanism centrally managed within Active Directory that links a user's Windows account to a UNIX profile containing the user's UNIX account attributes. This mapping can then be used by the NetApp server to provide consistent ownership and access rights to files and directories accessed by the user.

For example, the NetApp system needs to determine that "tom.smith" (the user's Windows name) is also "tom" (UNIX name) and tom has a UNIX UID of 801. The system also needs to make the reverse translation. Without a solution that provides some type of mapping, there is no obvious relationship between these identities. Two translations need to be made:

- tom.smith = tom (Windows name to UNIX name)
- tom = 801 (UNIX name to UNIX UID)

This document describes the various ways to integrate the NetApp servers with the mapping data that Centrify DirectControl maintains for users and groups.

1 Initial NetApp Configuration

This Application Note describes how to configure a NetApp server to allow both Windows and UNIX users to access a shared volume. This section describes how to configure the server for both Active Directory, to enable the Windows users to gain access, and UNIX user mapping, to enable UNIX users to gain access as well as to associate the Windows users with an appropriate UNIX identity. The next section describes the three different methods to configure the server to find the user's UNIX profile in order to establish the mapping between the two access methods.

The NetApp server stores configuration files on its **\c$\etc** share. You can access the **c$** volume from a Windows machine using the standard UNC naming convention in Windows Explorer. For example:

```
\\mynetappserver\c$\etc
```

1.1 Joining the NetApp Server to Active Directory

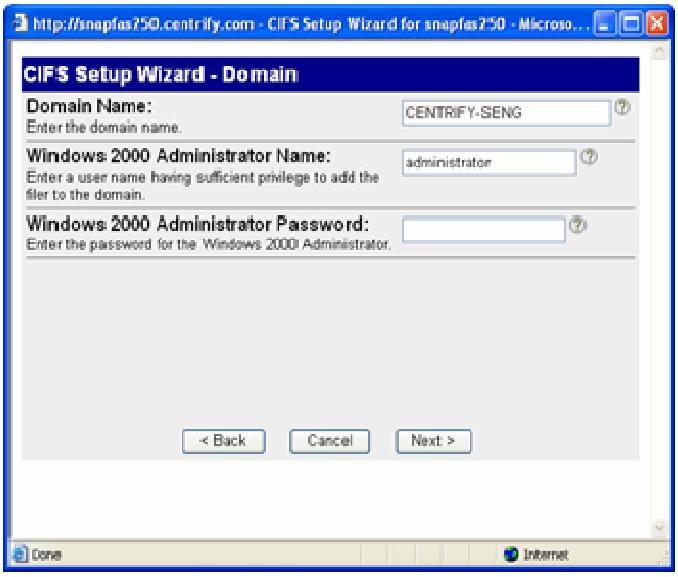
In order for the NetApp server to recognize Active Directory users, the server must be joined to the Active Directory domain.

These instructions do not describe every step necessary to set up a NetApp server. Please consult the NetApp documentation for complete instructions. The steps listed below are for configuring the NetApp Server to use Active Directory.

- Open the NetApp Administration Web Console in a web browser using the address:

  ```
  http://mynetappserver/na_admin
  ```

- In the left frame, select CIFS -> Configure -> Setup Wizard and complete the wizard steps. There is one wizard page that asks for the Domain Name, Administrator ID and Administrator Password for Active Directory.

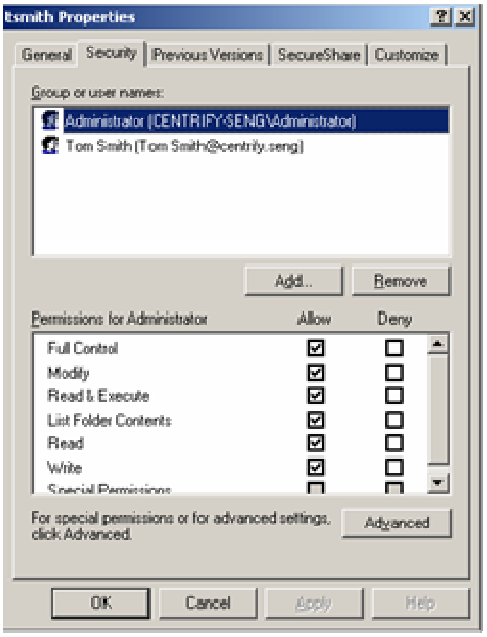


- Complete this wizard and save the information, this will join the NetApp server to Active Directory.

1.2 Creating a Shared Directory Using the Windows Interface

These instructions can be used to create a directory on a NetApp share. This example creates a user's home directory.

- Mount the **\\mynetappserver\c$\Home** directory. Make sure you have the permissions to create new directories in the Home directory.
- Create the new directory and then select Properties.
- Select the Security Tab. Add the Windows user to the Security window, and give the user Full Control.



If you are creating home directories, you must decide which "Home Directory Name Style" you will use on the NetApp Server.

The Home Directory Name Style setting is located at: CIFS -> Configure -> Home Directories in the NetApp Web Console. Here are the possible options.

Ntname	This is compatible with the current homedir function. The PC user name, without the domain name, is in lowercase letters and the home directory is searched for an entry of that name. If the CIFS homedir option specifies a list of directories, they are searched in order for the entry; this is a case-insensitive search.
Domain	The domain of the user is also used to find the user's home directory. The directory paths are searched for a directory with the domain name (case-insensitive) that contains a directory with the PC user name (also case-insensitive). For example, if netapp\john attempts to connect to \\filer\john, the home directories listed are searched for netapp\john. If this directory is not found, an error is returned.
Mapped	The PC user name is mapped to a UNIX user name (and user ID) using the usermap.cfg file, if present, and the usual (existing) mapping rules. If the user does not map to a UNIX user name, the default UNIX user name is used (pcuser by default). The /etc/passwd file (or NIS passwd file) entry for the user is used to identify the user's home directory. Because the home directory path is likely to be specified in a UNIX client path format (for example, /u/users/john, where /u/users is an NFS mount point), a translation file similar to the /etc/symlinks.translations file is needed to map it to a filer relative path or, possibly, a UNC name.

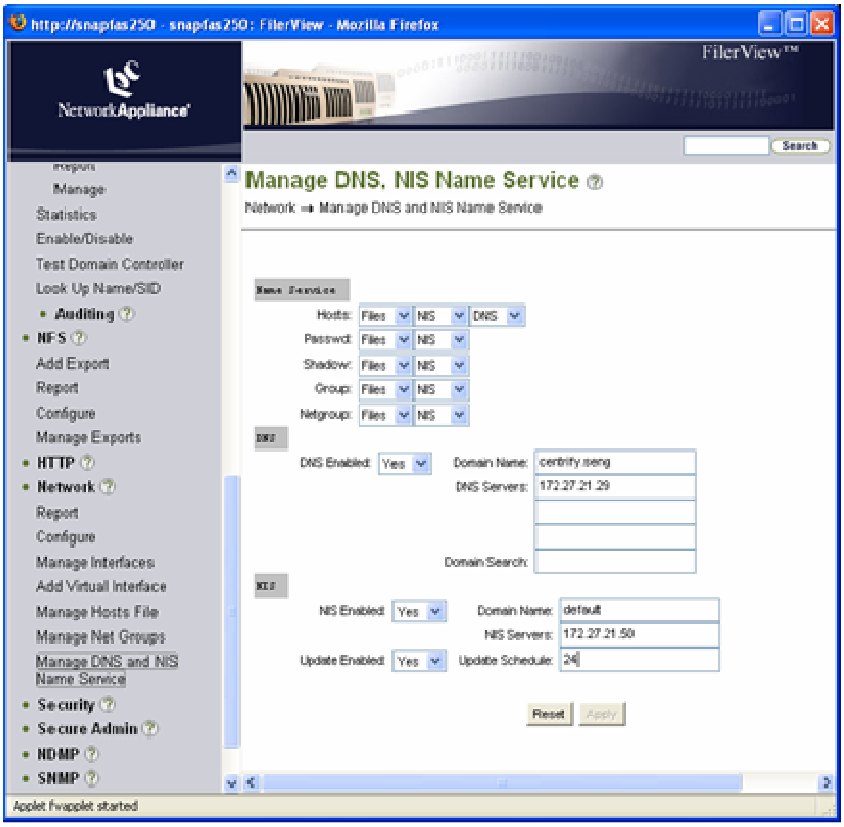
2 User Name Mapping

In order for the NetApp server to map correct file ownerships and attributes for Windows and UNIX users, it must be able to determine both the user's UNIX and Windows identity. Either of the following methods can be used to set up mapping, depending on whether you have a NIS server installed or not.

2.1 Mapping with DirectControl NIS Proxy

If you want to use the DirectControl NIS Proxy for mapping UNIX user information, use the following steps:

1. Install the DirectControl NIS Proxy on a UNIX or Linux machine in the local network. Consult the Centrify DirectControl Administrator's Guide for instructions on installation. The NIS Proxy must be installed on a machine along with the Centrify DirectControl UNIX agent.
2. You must join this server to a DirectControl Zone. Once this is done, only users in that Zone will be able to use files on the NetApp server.
3. The NIS domain name must be set to the DirectControl Zone name. You must configure your NetApp server to use the DirectControl NIS Proxy from the Manage DNS, NIS Service setting located at: Network -> Manage DNS and NIS Service in the NetApp Web Console.
    a. Select Yes for the NIS Enabled setting.
    b. Specify the name of the DirectControl Zone as the name of the Domain Name.
    c. Set the NIS Proxy Server to the IP address of the UNIX system running the DirectControl NIS Proxy.
    d. Check to be sure that Name Service maps of Passwd, Shadow and Group have NIS in the second column.



Resolving User Names

If the UNIX and Active Directory usernames are the same (e.g. “janedoe” on Windows is the same as “janedoe” on UNIX) then you do not need do anything. The system will work without additional configuration steps. The NetApp server will query the NIS server for the UNIX profile by searching for the Active Directory user’s login name and will find the correct UNIX profile for the Active Directory user.

If your UNIX and Active Directory user names are different, then you must edit the **\\mynetappserver\c$\etc\usermap.cfg** file on the NetApp server. For example, if the user’s name is “tom.smith” in the Active Directory “ADDOMAIN” domain and “tsmith” on UNIX, add the following line to the **usermap.cfg** file:

```
ADDOMAIN\tom.smith == tsmith
```

Note: There are two equal signs (==) in the assignment line.

If the Active Directory user name contains a space, then the name must be written with quotes. For example:

```
ADDOMAIN\"tom smith" == tsmith
```


You can edit the **\\mynetappserver\c$\etc\usermap.cfg** file from a Windows machine using a text editor such as Notepad.

2.2 Mapping with DirectControl LDAP Proxy

If you wish to leverage your Active Directory by using RFC2307 attributes available since Windows 2003 R2, you can use the DirectControl LDAP Proxy in order to present RFC2307 information stored into Centrify Zones to the Netapp server using LDAP client.

First, ensure that the Active Directory forest is set to a Windows Server 2003 functional level at minimum. You then need to create an RFC 2307 DirectControl Zone associated with the Active Directory domain that is set up on the Windows Server 2003 R2 domain controller. The NetApp server will be able to access user and group records visible in a specific DirectControl Zone through the DirectControl LDAP Proxy.

Second step is to setup the DirectControl LDAP Proxy server onto a UNIX or Linux machine in the local network. Consult pages 387-389 of the Centrify DirectControl Administrator's Guide for instructions on installation (http://www.centrify.com/downloads/products/documentation/suite2013/centrify-unix-adminguide.pdf).

The LDAP Proxy must be installed on a machine along with the Centrify DirectControl UNIX agent.

Once this is done, you must configure your NetApp server to use the DirectControl LDAP Proxy by starting a terminal session on your NetApp server and type in the following to view your current LDAP settings:

```
options ldap
```

To configure the NetApp server to use the RFC 2307 attributes through the LDAP Proxy, make the following changes using these *options ldap* commands:

```
options ldap.ADDomain ADDOMAIN
options ldap.enable on
options ldap.base DC=addomain,DC=com
options ldap.servers ldapproxy.addomain.com
```

In this example, the Active Directory domain is "ADDOMAIN", there is no need to setup a user name or password as the connection to the DirectControl LDAP Proxy can be done using anonymous binding. The connection between Active Directory and DirectControl LDAP Proxy server is done using machine credential of the server. Optionally you can use SSL protocol if you want to use secure transaction by using LDAPS to connect your AD). The ldap.base information should be the default naming context of the Active Directory domain (in this example we assume the default naming context is DC=addomain,DC=com). Finally the ldap.servers option indicated the name of your DirectControl LDAP Proxy (you can define more than one for redundancy by separating names by comma or space).

If the Active Directory user names and UNIX user names are not the same, then you need to make the same changes to the mapping file mentioned previously.

Note:

a) *ldap.nssmap.attribute.userPassword needs to be mapped to something else - like "cn". This is because in most cases this attribute will be missing. If asked for specifically, it will fail.*

b) *b) ldap.rfc2307bis.enable must be off. Otherwise this will fail. This is because with this on, NetApp will ask for dn which is NOT a RFC2307 attribute.*

2.3 Mapping with Local Files

If there is no NIS server installed and you do not want to use RFC 2307, then you can define the UNIX user in the NetApp server's **\\mynetappserver\c$\etc\passwd** file.

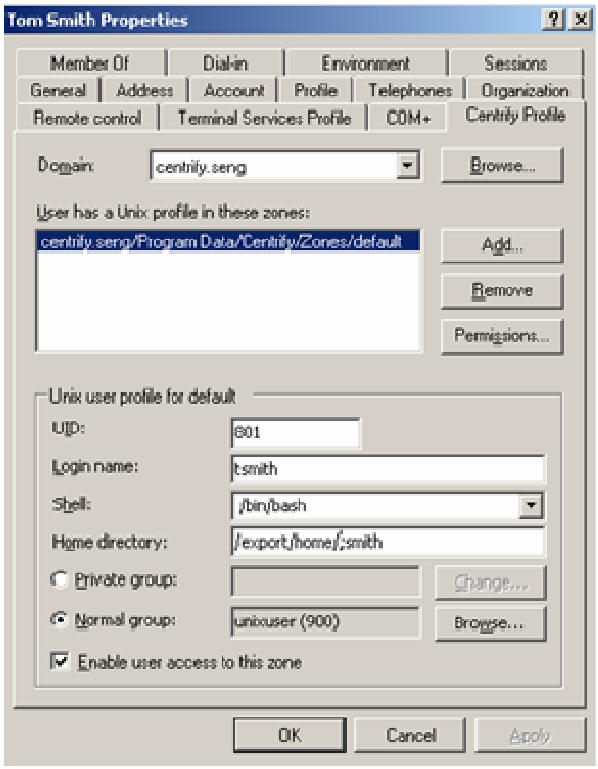
For example, if your Active Directory user "tom.smith" has a UNIX name of "tsmith", a UNIX UID of 801 and a primary UNIX GID of 900, you would add the following line to the **passwd** file.

```
tsmith::801:900::/:
```

Remember to put a blank line at the end of the file. Without it, the NetApp server may have difficulties.

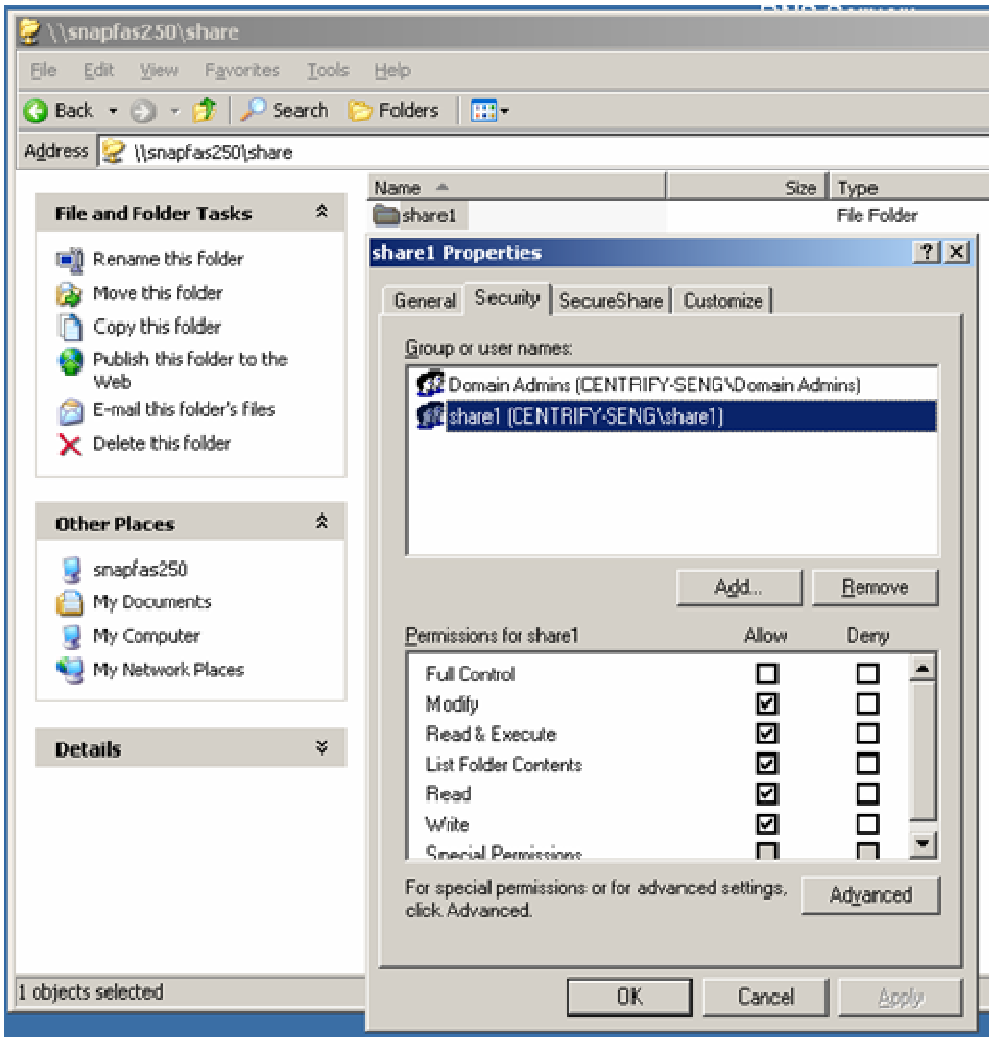
Note also that you do not have to set the user's UNIX home directory on this line. It is set in the Centrify user properties for the client to the NetApp server. If you want to use this share as a home directory, you can set the path in the Centrify profile "Home Directory" setting in Active Directory Users and Computers.

If the Active Directory user names and UNIX user names are not the same, then you need to make the same changes to the mapping file mentioned previously.

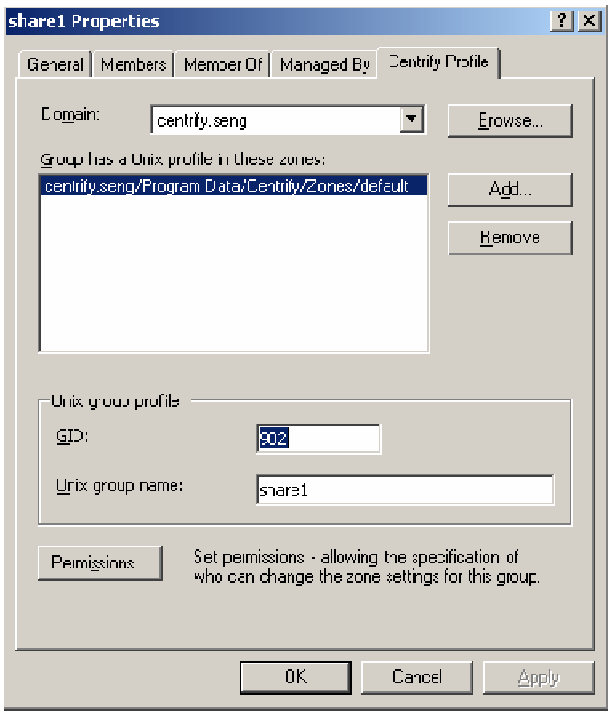


3 Controlling File Share Access with Active Directory Groups

The NetApp server can use group permissions to control access to shares and files. For example, you can use the Windows interface to create a new share on the NetApp server. Then, in the Security Properties for the share, assign an Active Directory group to have specific permissions for that share.



Only users in that Active Directory group will have the applied group permissions when accessing the share from a Windows computer. You can also UNIX-enable the group with the DirectControl Administrator Console or Groups Profile tab. This will allow an user who is both UNIX-enabled and a member of the Active Directory group to have access to the share from either a Windows machine or a UNIX machine.



4 Mounting NetApp Volumes from UNIX Machines

Once the configuration is complete using one of the three user mapping methods described above, you can then mount the NetApp volumes from your UNIX system using the standard *mount* command. For example:

```
mount  remoteserver:/home  /export/home
```

This command will mount the “home” share on “remoteserver” to the local **/export/home** mount point. You can also use standard *automount* tools to set up mounts that will automatically be established when needed. Centrify provides tools to manage and share this information to UNIX systems via NIS or through Group Policy based configuration. For further information, consult the DirectControl Administrators Guide and your UNIX documentation for more details.

5 Legal Notices

AN-005-2013-01-08