



Application Note

## Using DirectControl with SFU NFS

*Using Centrify's DirectControl with Microsoft's Windows Services for UNIX NFS Server*

Published: October 4, 2005

---

### Introduction

The goal of this application note is to build a solution to solve the scenario where you need to share directories on a Windows server out to UNIX, Linux and Mac clients using the UNIX NFS file sharing protocol. For this solution, you are looking to use a secure, central, Active Directory based identity store for UNIX user and group information. Access control for the shared files needs to be controlled using the user and group credentials that are stored in Active Directory.

Centrify DirectControl provides Active Directory based identity, access control and policy services for UNIX, Linux and Mac systems. Microsoft's Windows Services for UNIX (SFU) product provides Windows to UNIX interoperability solutions including an NFS Server. Since the SFU NFS Server needs to be able to resolve usernames and groups and the only central directory service that it supports for doing name resolution is a Network Information Service (NIS) Server, a solution needs to be found for tying an NIS Server into the Active Directory directory service. Fortunately there are at least two solutions for this requirement: the NIS Service that is included with SFU and the NIS Server that is included with DirectControl.

This Application Notes explores methods for solving this need and includes information on how to set up Services for UNIX and DirectControl so that these two solutions share the same Active Directory based identity space for resolving user and group information.

## Contents

<b>1</b>	<b>Installation .....</b>	<b>3</b>
1.1	Preparation.....	3
1.1.1	Method #1: Use the SFU NIS server and the DirectControl SFU Zones feature.....	3
1.1.2	Method #2: Use the DirectControl NIS server with SFU User Name Mapping.....	3
1.1.3	Deciding which method is right for you.....	3
1.2	Installing the DirectControl software .....	4
1.3	Installing the Services for UNIX software .....	4
<b>2</b>	<b>Basic Configuration for Method #1.....</b>	<b>5</b>
2.1	Setting up SFU on Windows .....	5
2.2	Setting up DirectControl on Windows.....	7
2.3	Setting up the SFU NFS Server component on Windows .....	8
2.4	Setting up DirectControl components on UNIX .....	8
2.5	Mounting the NFS share from UNIX.....	9
<b>3</b>	<b>Basic Configuration for Method #2 .....</b>	<b>9</b>
3.1	Setting up DirectControl on Windows.....	9
3.2	Setting up DirectControl components on UNIX .....	10
3.3	Setting up the SFU User Name Mapping component on Windows.....	12
3.4	Setting up the SFU NFS Server component on Windows .....	14
3.5	Mounting the NFS share from UNIX.....	15
<b>4</b>	<b>Summary .....</b>	<b>15</b>
4.1	Related Information and Application Notes .....	15
4.2	For more information .....	16
4.3	Legal Notices .....	16

## 1 Installation

### 1.1 Preparation

There are at least two methods for accomplishing the task of sharing the same user identity store between DirectControl and Services for UNIX. Once either method is set up, the SFU NFS Server can be used to share Windows files to UNIX clients using the NFS protocol. The user information store for the NFS server will be the same information store that DirectControl uses for authenticating and authorizing UNIX users against their Active Directory credentials.

Before beginning the process of setting up or changing the setup of either product, it is worth exploring these two alternative methods.

#### 1.1.1 Method #1: Use the SFU NIS server and the DirectControl SFU Zones feature

This first method relies on using the SFU schema extensions for Active Directory as the storage mechanism for UNIX attributes of users and groups. The SFU NIS Server is configured to use this information and provide directory services for the SFU NFS Server. DirectControl is configured with a built-in feature which allows a Zone to be mapped to the UNIX attribute information that is stored in the SFU schema extensions.

#### 1.1.2 Method #2: Use the DirectControl NIS server with SFU User Name Mapping

The second method does not use the SFU NIS Server at all; therefore this component does not need to be installed. Instead, the DirectControl NIS Server, **adnisd**, is used and the SFU NFS Server is configured to use this service for resolving user and group information lookups. It is important to note that the user passwords are not exposed when user information is accessed from the DirectControl NIS Server. With this method, there is no requirement to extend the Active Directory schema with the SFU UNIX schema extensions and multiple Zones can be used in a single domain.

#### 1.1.3 Deciding which method is right for you

The first method can be more appropriate if you are already using the SFU NIS Server, the SFU Active Directory schema extensions and you are able work with a single “Zone” for all UNIX users and groups. Since SFU only allows users to be members on one NIS domain, the method may not be appropriate if you want to use the powerful multi-zone features of DirectControl. Also, if you plan on using the new UNIX schema that will be

included in Windows Server 2003 R2, and will not be using DirectControl Zones, then this method will work for you. DirectControl 2.1 and later includes new support for looking up user and group information using the DirectControl NIS Server. If you are running an earlier version of DirectControl then you must use the first method as these new features were not included in earlier versions of the product.

If you are planning on building a multi-zone infrastructure and need the ability to restrict access to NFS shares across different Zones of users then using the second method makes the most sense. It is possible to set up a DirectControl NIS Server for each Zone and have full and separate control over each group of users, groups, systems and NFS shares. Also, if your organization has a restriction on extending the schema of production Active Directory servers then the second method is most appropriate since this method does not require any schema extensions within Active Directory.

If you are still uncertain as to which method will be most appropriate for your organization, it is recommended you use the second method since this method offers the most flexibility with the least amount of disruption.

## 1.2 Installing the DirectControl software

Proceed with installing the DirectControl software on both Windows and on your UNIX, Linux and Mac systems as appropriate. See the DirectControl Administrator's Guide for complete information on installing the product. You can create a default Zone, although the configuration section below will provide more information on how to set up your Zones, depending on which method you use.

If you are planning on using method #2, then you will need to install the Centrif DirectControl NIS Server on at least one UNIX or Linux machine in the Zone. Again, see the DirectControl Administrator's Guide for more information on how to install this component.

## 1.3 Installing the Services for UNIX software

Proceed with installing Microsoft's Services for UNIX product. This product is available as a free download from [microsoft.com](http://microsoft.com). See the [Microsoft Services for UNIX home page](#) for information on downloading and installing the software.

As a minimum, for an NFS Server solution, you will need to install the following components:

- NFS: Server for NFS
- Service for NIS (only required if you plan to use method #1)
- Authentication tools for NFS: User Name Mapping

- Authentication tools for NFS: Server for NFS Authentication

When prompted for a User Name Mapping Server during installation, select Remote User Name Mapping Server and enter “localhost” as the server name. This is the easiest way to install the product and these settings can always be changed later.

If you are installing the Service for NIS, it is important to note that the install process will extend your Active Directory schema. You will need to be a member of the “Schema Admins” group to complete the schema modification. This schema change is also irreversible. If this is an issue for you, then you should not install this component and instead follow the [configuration directions below for Method #2](#).

For complete information on installing Services for UNIX see the documentation that comes with the product. Before, proceeding to the next section, make sure you have access to the standard administrator documentation that comes with DirectControl and SFU.

---

## 2 Basic Configuration for Method #1

The following steps should be used as a guideline for configuring DirectControl and Services for UNIX to enable setting up an NFS Server on Windows leveraging a shared directory with UNIX attributes using the SFU NIS Server.

### 2.1 Setting up SFU on Windows

On the Windows server make sure that SFU NFS Server, User Name Mapping, the NFS authentication server and the SFU NIS Server have been installed. Note that the NIS Server needs to be installed on an Active Directory domain controller. You do not need to install the Password Synchronization service. If you open the properties for a user in the Active Directory Users and Computers MMC, you should see a tab for “UNIX Attributes”. If DirectControl is already installed, you will also see a tab called “Centrify Profile”. Now proceed with the following steps:

1. Make sure that the “Server for NFS”, “Server for NIS” and “User Name Mapping” services are running on the Windows system.
2. Once SFU is installed, run the Services for UNIX Administration MMC and select the “Server for NIS” line and open the tree to display the domain. The domain name should automatically appear. The name of the domain should be the same as the short name for the Active Directory domain. For example, if the Active Directory domain name was “centrify.com” then the NIS domain name will be “centrify”. Note this NIS domain name as you will need this name later.
3. Select the NIS domain name in the left pane and confirm that the right pane has valid information for your server. This information is automatically generated for the NIS server running on this machine.

4. Now select the “User Name Mapping” line in the left pane.
5. In the configuration pane on the right, select NIS as the method and change the refresh interval to something more frequent, especially while testing. Hit “Synchronize Now” and hit “Apply”.
6. At this point, NIS is set up but there are no users in the NIS domain. Open the Active Directory Users and Computers MMC.
7. Create a new global security group. For this example use “unixuser”. Click OK and then open the properties for the new group. It is also possible to use an existing Active Directory group if you prefer.
8. On the group Properties page, select the UNIX attributes tab. In the NIS Domain field, enable the group with the available domain. In this example, it will be “centrify”. A GID is automatically generated. You can override this GID if you prefer. Click “OK”.
9. Now open the properties for an existing Active Directory user you wish to enable in the NIS domain. Select the “UNIX Attributes” tab. In the NIS Domain field, enable the user with the available domain. In this example, it will be “centrify”. A UID is automatically generated or chose your own UID. Check that the other settings such as “Login Shell” are set correctly. Make sure the user’s “Primary Group” is set to the new UNIX-enabled group that you just created. In this example, set it to “unixuser”. Click “OK”.
10. Repeat steps 7-9 for the users and groups that need to be UNIX enabled.
11. You should also create Active Directory accounts for the UNIX “root” group and “root” user. Create the root group first and call it “root”, UNIX enable it and give it a GID of 0 (zero).
12. Create the root user account and call it “root\_sfu”. UNIX enable this account and give it a UID of 0 (zero) and make sure the “Primary group” is “root”.
13. Return to the Services for UNIX Administration MMC and select “User Name Mapping” in the left pane.
14. Select the Maps tab, check “Simple maps”.
15. You will be prompted for information about the NIS domain. Use the domain name that was displayed by the “Server for NIS” manager for the “NIS domain name” (e.g. centrify) and leave the NIS server name blank. Click OK.
16. Now select “Show User Maps”.
17. Click on “List Windows Users”. You should see your Windows domain users displayed.

18. Fill in the NIS Domain name (e.g. centrify) and then click “List UNIX Users”. You should see a list of the users and their UIDs that were enabled as UNIX users.
19. In order to map the root user correctly, select the AD user name for the root account in the left list (e.g. root\_sfu) and then select the UNIX user named “root” in the right list.
20. Click on the Add button and confirm the mapping of this special account.
21. Since simple maps are enabled, users should be automatically mapped to each other. You can check the “Display simple maps in Mapped users list” to check this. You can also create advanced mapping for accounts that have different AD and UNIX names.
22. You also might need to create some advanced maps for groups. Select “Show Group Maps”.
23. Enter the NIS Domain name again and list both the Windows and UNIX groups.
24. Check the box “Display simple maps in Mapped group list”. Make sure the AD root group has been automatically mapped to the UNIX root group. If it has not or if you have used different names, select the AD and UNIX names for the root group account and click “Add”.
25. Do the same for any other groups that aren’t automatically mapped via simple maps.
26. Hit “Apply” in the top right corner and go back to the Configuration tab and hit “Synchronize Now”
27. At this point, the NIS mapping should complete and will manage itself as you add and delete users in AD and SFU since simple maps will map the user accounts.

**Note:** SFU allows you to map multiple AD accounts to a single UNIX account, so it is recommended that you map the AD Administrator account to the UNIX root account as well. That way if a directory or file is owned by Administrator, it will show up as owned by root when viewed through an NFS share. However, if Administrator is logged in and creates a directory or file, it defaults to being owned by the AD group “Administrators” not the user “Administrator”. SFU does not support mapping an AD group name to a UNIX user name so you’ll probably need to double check file ownerships when Windows Administrator users create files in a directory that is NFS shared.

## 2.2 Setting up DirectControl on Windows

Follow these configuration steps to set up DirectControl on Windows:

1. Open the DirectControl Administrator Console.

2. Create a new Zone. For this example, we will use the name “sfu-zone”.
3. Hit Next and select “SFU zone” since we want to map the DirectControl users with the existing SFU NIS domain users.
4. Hit Next and input the correct Windows domain and NIS domain from the lists provided. Click Finish.
5. If you open the properties for the new SFU Zone, you will see that the UNIX enabled users and groups already appear as DirectControl members of the Zone.

## 2.3 Setting up the SFU NFS Server component on Windows

Most of the default settings for the “Server for NFS” can be used without change. These can be viewed in the Services for UNIX Administration MMC. To set up a test NFS share on Windows, do the following:

1. Open the Windows Explorer and create a Folder, for example C:\test-nfs.
2. Right click and select Properties for this new folder.
3. Select the “NFS Sharing” tab, and check “Share this folder”.
4. Hit “Permissions” to access the “NFS Share Permissions” page. Change the default settings for “Type of access” to “Read-Write” and check “Allow root access”.
5. Hit “OK” twice.
6. You’ll need to make sure that the directory being shared is owned by a user that is UNIX mapped (e.g. root) otherwise when you try and mount the share from UNIX, the username will show up as a number. Also, make sure the Permissions on the directory are set appropriately since UNIX enabled AD users will need access to the share from UNIX systems.
7. This directory is now shared using the NFS protocol.

## 2.4 Setting up DirectControl components on UNIX

1. Chose a UNIX or Linux system, log in as root and join this system to the Zone “sfu-zone”. For example, if you were in the centrifly.com domain, you would issue the command:  

```
adjoin -z sfu-zone centrifly.com
```
2. Try logging in as an Active Directory user to make sure DirectControl is functioning correctly.

## 2.5 Mounting the NFS share from UNIX

On the UNIX box, you can now mount the Windows file share that has been shared out via NFS. For example, execute the following command as the root user, where “ws2k3” is the name of the Windows server that has the NFS share:

```
mkdir /test
chmod 777 /test
mount -t nfs ws2k3:/test-nfs /test
```

Once the Windows file share is mounted on UNIX via NFS, all DirectControl users should automatically have access to it (assuming the share and directory permissions are set to allow access) and files that get created by various users will be stamped correctly with them as the owner. Back on the Windows server, the files also show up correctly with the right ownership.

---

## 3 Basic Configuration for Method #2

The following steps should be used as a guideline for configuring DirectControl and Services for UNIX to enable setting up an NFS Server on Windows leveraging a shared directory with UNIX attributes using the DirectControl NIS Server. This method does not require that the SFU NIS Server be installed. It also does not use the SFU Zones feature within DirectControl but instead uses the native multi-zone capability that is built into the product. Again, this method does not require any changes to the schema on the Active Directory servers.

### 3.1 Setting up DirectControl on Windows

Follow these configuration steps to set up DirectControl on Windows:

1. Open the DirectControl Administrator Console.
2. If you have not already created a DirectControl Zone for your UNIX users, do so now. This Zone can use any Zone name including using the default Zone. If you have already created a Zone, then an existing Zone can be used in these steps. For this exercise, we will use the Zone name of “nfs-zone”.
3. Create a new Active Directory global security group called “root”.
4. Add the new “root” group to the zone “nfs-zone”. When prompted for a GID, enter “0” (zero) and make sure the UNIX Group Name is “root”. Note that the Active Directory name does not have to be “root” however the UNIX Group Name should be “root”.
5. Create a new Active Directory user called “root\_nfs-zone”.
6. Add the new user “root\_nfs-zone” to the zone “nfs-zone”. When prompted for the “UNIX User Profile”, change the UID to “0” (zero), the Login name to “root” and

set the Primary Group to the Normal Group called “root”. These steps are required to correctly map the special root user account and enable root to be able to mount NFS file systems from UNIX.

## 3.2 Setting up DirectControl components on UNIX

1. Chose a UNIX or Linux system, log in as root and join this system to the Zone “nfs-zone”. For example, if you were in the centrifly.com domain, you would issue the command:

```
adjoin -z nfs-zone centrifly.com
```

2. Install the DirectControl NIS Server on this UNIX or Linux system. See the DirectControl Administrator’s Guide section titled “Using the DirectControl Information Service for NIS requests” for information on installing this service.
3. Edit the file /etc/centriflydc/centriflydc.conf.
4. Make sure there is a line in this file allowing access to the Windows machines where the SFU NFS Server will be run. If you are using a secure internal network, then you have the option of allowing NIS requests from all machines in the network. For example, if the Windows Server machines are all in the IP network 192.168.111.0 then the line in the centriflydc.conf file should read:

```
nisd.securenets: 192.168.111.0/255.255.255.0
```

5. It is recommended that while you are testing the solution, you update the following settings in the centriflydc.conf file:

```
adclient.cache.expires: 60  
nisd.update.interval: 60
```

Change those settings back to something less frequent once everything is stable.

6. Edit the file /etc/hosts.allow.
7. Add lines for the Windows machines that will be running NFS servers. For example, if you want to allow access to all NFS servers in the local IP network that are part of the centrifly.com domain, then add the line:

```
ALL: .centrifly.com
```

For more information on how to configure the hosts.allow file, see the UNIX MAN page HOST\_ACCESS(5). It is important that the hosts.allow and hosts.deny files are in sync with the controls set up with the “nisd.securenets” setting in /etc/centriflydc/centriflydc.conf.

8. Make sure that **adclient** is running and that DirectControl is functioning correctly.
9. Insure that RPC is running. Usually it is running by default. The result of running:

```
rpcinfo -p localhost
```

should be an RPC table, not "can't contact portmapper".

10. Start the DirectControl NIS Server by running:

On Linux type: `/sbin/service adnisd start`

On Solaris type: `/etc/init.d/adnisd start`

11. Try testing the NIS service by setting up a local NIS client on the UNIX machine where you installed **adnisd**, by doing the following:

a. On Linux,

i. Run:

`domainname nfs-zone`

Note this is the name of the Zone you joined, not the domain.

ii. Edit `/etc/yp.conf` to add the line "domain *zone-name* server *server*". This is not strictly necessary because the server can be discovered by broadcast but it is better to do this. The server may be "localhost". For our example, you would have:

`domain centri fy.com server localhost`

iii. Start **ypbind** with

`/sbin/service ypbind start`

b. On Solaris,

i. Run:

`domainname nfs-zone`

ii. If you want to bind to specific servers, run "ypinit -c" and enter the servers. If you choose to skip this step, the NIS server will be found with broadcast. **ypinit** must be used when the broadcast would not reach desired servers due to network topology (e.g. the router does not transmit broadcasts across subnets).

iii. Start **ypbind** with

`/usr/lib/netsvc/yp/ypbind`

iv. If you choose to use broadcast, you must start ypbind with the "-broadcast" option.

12. Perform these basic system verification tests:

c. Verify that **adnisd** is running with **ps**.

i. If it is not running, restart **adnisd**. If it refuses to stay running, check the log.

- d. Verify that **ypserv** is not running with **ps**.
  - i. If **ypserv** is running, kill it. Modify the system init files to insure that **ypserv** does not start on boot. Restart **adnisd**.

- e. Verify that **adnisd** has registered with RPC. To check this, run:  
`rpci nfo -p local host.`

You should see two entries in the RPC table for **ypserv**. For example:

```
100004      2      udp  668  ypserv
100004      2      tcp  670  ypserv
```

- i. If no table is displayed, restart the RPC services. If "ypserv" is not listed, restart **adnisd**.
- f. Verify connectivity from the UNIX machine to the Windows NFS server machine. If you cannot resolve names or cannot reach server check the network or DNS configuration. Fix it before proceeding.
- g. Useful utilities to run to make sure the NIS server is resolving information out of Active Directory include the following:
  - i. What is the name of my NIS server?  
`ypwhi ch`
  - ii. What maps are served by the NIS server?  
`ypwhi ch -m`
  - iii. What nicknames are defined for NIS maps?  
`ypwhi ch -x`
  - iv. Display contents of a map, including both keys and values:  
`ypcat -k map`

### 3.3 Setting up the SFU User Name Mapping component on Windows

1. On the Windows server make sure that SFU NFS Server, User Name Mapping and the NFS authentication server have been installed. Note that these services can be installed on either Windows XP or Windows Server. You do not need to install the SFU NIS Server or the Password Synchronization service.
2. Make sure that the "Server for NFS" and "User Name Mapping" services are running on the Windows system.
3. Once SFU is installed, run the Services for UNIX Administration MMC and select the "User Name Mapping" line in the left pane.
4. In the configuration pane on the right, select NIS as the method and change the refresh interval to something more frequent, especially while testing.

5. Select the “Maps” tab, check “Simple maps”.
6. You will be prompted for information about the NIS domain. Use the DirectControl Zone for the “NIS domain name” (e.g. nfs-zone) and use the UNIX server name where **adnisd** is running as the NIS server name. Click OK.
7. If **adnisd** is set up correctly, this previous step should succeed. If you get an error message, double check the configuration of the **adnisd** server environment. Common problems include network or DNS issues, or the UNIX machine is denying access due to the setup of the hosts.allow files.
8. Now select “Show User Maps”.
9. Click on “List Windows Users”. You should see your Windows domain users displayed.
10. Fill in the NIS Domain name (this is the same as the Centrify Zone name e.g. nfs-zone) and then click “List UNIX Users”. You should see a list of the users and their UIDs who are defined as members in the DirectControl Zone.
11. In order to map the root user correctly, select the AD user name for the root account in the left list (e.g. root\_nfs-zone) and then select the UNIX user named “root” in the right list.
12. Click on the Add button and confirm the mapping of this special account.
13. Since simple maps are enabled, users should be automatically mapped to each other. You can check the “Display simple maps in Mapped users list” to check this. You can also create advanced mapping for accounts that have different AD and UNIX names.
14. You also might need to create some advanced maps for groups. Select “Show Group Maps”.
15. Enter the NIS Domain name again and list both the Windows and UNIX groups.
16. Check the box “Display simple maps in Mapped users list”. Make sure the AD root group has been automatically mapped to the UNIX root group. If it has not or if you have used different names, select the AD and UNIX names for the root account and click “Add”.
17. Do the same for any other groups that aren’t automatically mapped via simple maps.
18. Hit “Apply” in the top right corner and go back to the Configuration tab and hit “Synchronize Now”
19. At this point, NIS mapping should complete and it will manage itself as you add and delete users in AD and DirectControl since simple maps will map the user

accounts. However, if you have private groups with DirectControl, you will need to manually map each new private group with SFU's User Name Mapper every time you add a user since the AD group name is "*private\_group\_name.group*" and the UNIX group name is just "*group*". For this reason, it makes more sense to use "Normal group" assignments instead of using a "Private group".

**Note:** SFU allows you to map multiple AD accounts to a single UNIX account, so it is recommended that you map the AD Administrator account to root as well. That way if a directory or file is owned by Administrator, it will show up as owned by root when viewed through an NFS share. However, if Administrator is logged in and creates a directory, it defaults to being owned by the AD group "Administrators" not the user "Administrator". SFU does not support mapping an AD group name to a UNIX user name so you'll probably need to double check file ownerships when Windows Administrator users create files in a directory that is NFS shared.

### 3.4 Setting up the SFU NFS Server component on Windows

Most of the default settings for the "Server for NFS" can be used without change. These can be viewed in the Services for UNIX Administration MMC. To set up a test NFS share on Windows, do the following:

1. Open the Windows Explorer and create a Folder, for example C:\test-nfs.
2. Right click and select Properties for this new folder.
3. Select the NFS Sharing tab, and check "Share this folder".
4. Hit "Permissions" to access the "NFS Share Permissions" page. Change the default settings for "Type of access" to "Read-Write" and check "Allow root access".
5. Hit "OK" twice.
6. You'll need to make sure that the directory being shared is owned by a user that is UNIX mapped (e.g. root) otherwise when you try and mount the share from UNIX, the username will show up as a number. Also, make sure the Permissions on the directory are set appropriately since UNIX enabled AD users will need access to the share from UNIX systems.
7. This directory is now shared using the NFS protocol.

### 3.5 Mounting the NFS share from UNIX

Back on the UNIX box, you can now mount the Windows file share that has been shared out via NFS. For example, execute the following command as the root user, where “ws2k3” is the name of the Windows server that has the NFS share:

```
mkdir /test
chmod 777 /test
mount -t nfs ws2k3:/test-nfs /test
```

Once the Windows file share is mounted on UNIX via NFS, all DirectControl users should automatically have access to it (assuming the share and directory permissions are set to allow access) and files that get created by various users will be stamped correctly with them as the owner. Back on the Windows server, the files also show up correctly with the right ownership.

---

## 4 Summary

Regardless of which method you use, the end result will be the same. The final solution will have the following features:

- UNIX users can be managed from Active Directory and can use their Active Directory username and password to log into UNIX. This capability is provided by DirectControl.
- UNIX authentication is managed securely using the Kerberos technology that is part of DirectControl and Active Directory.
- UNIX systems are securely joined to the Active Directory domain and can be controlled and managed centrally via DirectControl.
- Users can create file shares on Windows that can be shared out to UNIX systems using the NFS protocol. This capability is provided by Microsoft’s Services for UNIX.
- Consistency is maintained for user and group attributes on files across Windows and UNIX – regardless whether files are created or managed from UNIX or Windows. User identity attributes, such as UID, home directory and login shell, are now stored and managed in Active Directory.

### 4.1 Related Information and Application Notes

Numerous books are available for administrators that describe how to manage NIS and NFS. Some of these references include:

- O’Reilly’s [Managing NFS and NIS - Automounter](#)
- [SunService Tip Sheet for Sun NIS](#)

- [Sun's NIS FAQ](#)

Additional Services for UNIX information can be found on:

- [Introduction to Microsoft Windows Services for UNIX 3.5](#)
- [Windows Services for UNIX 3.5 White Paper](#)

## 4.2 For more information

For the latest product information on DirectControl, check out our web site at <http://www.centrify.com/products.asp>

## 4.3 Legal Notices

*Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.*

*Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2005 Centrify Corporation. All rights reserved.*

*Centrify and DirectControl are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*