Implementing and configuring NFS on Windows Server 2003 R2

Tech Note #5 in the "Interop Components in Windows" series

By Rodney Ruddock (Interop Systems)

Overview

With Windows Server 2003 R2 several of the components that were previously part of Windows Services for UNIX (SFU) became part of the base operating system distribution. This includes the Network File System (NFS) components. There have been changes to these components since the release of SFU version 3.5.

With Windows Server2003 R2 the NFS components no longer contain support for PCNFS and Gateway for NFS. The resource overhead with Gateway for NFS was fairly high and it was deemed much better for the client machines to connect as full NFS clients. The gained speed and lower resource use with NFS Client make this decision very clear. Since more Windows systems are able to run full NFS Clients rather than PCNFS, a similar decision was made for PCNFS support.

There is also new functionality added that will continue to be used in future Windows Server releases. One of these new bits of functionality is the addition of Unix user ID information within Active Directory (AD). Based on RFC 2307 this information can be used by NFS clients and servers for correctly mapping Windows IDs to and from UNIX IDs. It can be used for NIS support as well. The Username Mapping (UNM) available with SFU continues to be available with Windows Server 2003 R2 to support IT sites as they transition to using the new AD functionality. It should be noted that starting with Windows Server 2008 (Longhorn) UNM will no longer be supported.

These changes mean that administrators need to do some planning for the longer term to be prepared for later releases of Windows Server. Server 2003 R2 can be viewed as a “transition release” because UNM and RFC 2307 in AD are supported. The planning involves not only servers, but also clients. Client machines running NFS Client from SFU 3.5 are capable of using UNM, but cannot use the newer 2307/AD capability for ID mapping. This applies to any Windows client release prior to Windows Vista, e.g. Windows XP. Windows Vista comes with NFS Client capabilities that can use both UNM and 2307/AD functionality. Windows Server 2003 R2 is thus capable of supporting both the old UNM and the newer 2307/AD ID mapping. But from Server 2008 and onward the client machines will need to be Windows Vista as a minimum.

Selecting Component Installation

The first of several tasks is to install all of the needed components (NFS Server and any supporting components). Which supporting components you will need depends on what support is required for the NFS Client machines in particular.

If your client systems are releases of Windows prior to Windows Vista then you will need to use UNM. Those earlier systems will be running SFU 3.5’s NFS Client which only works with UNM.

If you have a completely new array of just Windows Vista machines then the recommendation is to use the newer RFC 2307 functionality in AD. The will mean fewer changes and transitions in your next upgrade cycle.

For definition purposes here is a brief explanation of what identity mapping is and why it is required. Modern Windows systems have unique identifiers for users and groups; these identifiers are different than with Unix systems. Unix UIDs and GIDs are only guaranteed to be unique on a per machine basis. A global management system, such as LDAP or NIS, can be used by Unix machines to enact a network-wide regime. In contrast the Windows identifiers are virtually unique amongst all Windows systems with the use of a SID (Security IDentifier). A SID and a UID/GID naturally do not match.

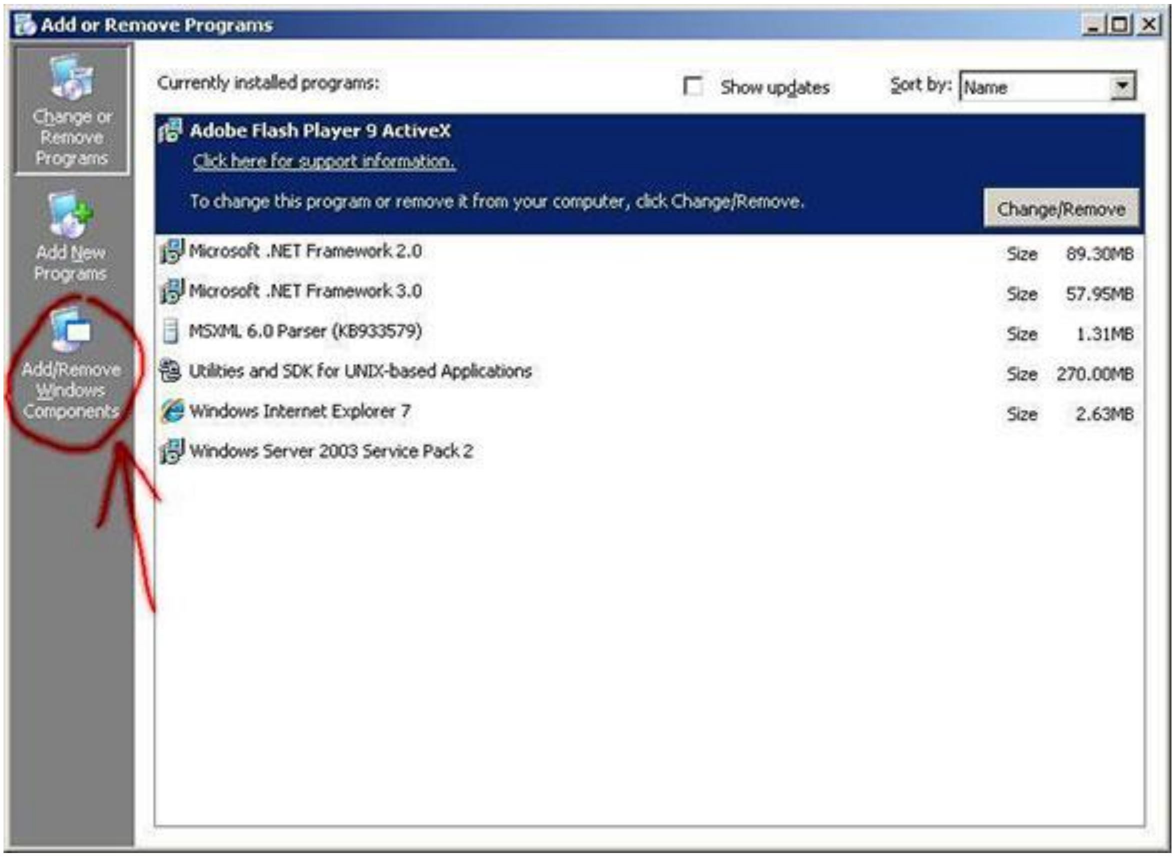
To create common ground for identification between the two systems, identity management on Microsoft Windows has been extended to provide UIDs and GIDs for users and groups respectively. Initially with SFU an implementation of NIS in conjunction with a User Name Mapping server allowed for the common ground between Windows and Unix systems. Starting with Windows Server 2003 R2 and continuing with Windows Server 2008 the information to map SIDs to UIDs and GIDs becomes part of AD's implementation of RFC 2307.

With a Unix UID and GID stored in either or both UNM and AD on a per user basis, an easy mapping between Windows SIDs and Unix UIDs/GIDs is achievable. Now a Windows computer and a Unix computer can communicate user identification using common credentials. This leads to NFS communications between Windows and Unix computers.

Installing NFS Server and friends

Note: It is assumed that you have already installed Active Directory and DNS with the correct configuration.

Open the Control Panel and then start the Add/Remove Programs utility. After it has started select from the left panel "Add/Remove Windows Components."

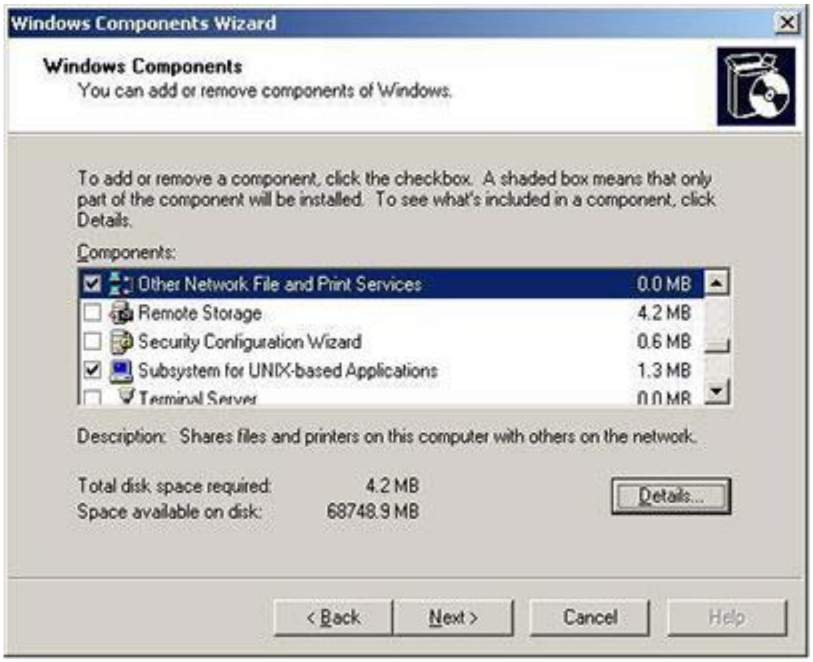

Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
□ Show updates
Sort by: Name
Change/Remove

Adobe Flash Player 9 ActiveX
Click here for support information.
To change this program or remove it from your computer, click Change/Remove.

Microsoft .NET Framework 2.0	Size	89.30MB
Microsoft .NET Framework 3.0	Size	57.95MB
MSXML 6.0 Parser (KB933579)	Size	1.31MB
Utilities and SDK for UNIX-based Applications	Size	270.00MB
Windows Internet Explorer 7	Size	2.63MB
Windows Server 2003 Service Pack 2		

This will open a new panel. A list of components will be presented. Those components that already have a checkmark in the box at their left are already installed. Scroll down until you find the entry for 'Other Network File and

Print Services.’ (Why NFS is lumped in with Print Services is unknown, but this arrangement does change with the next Server release.)



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

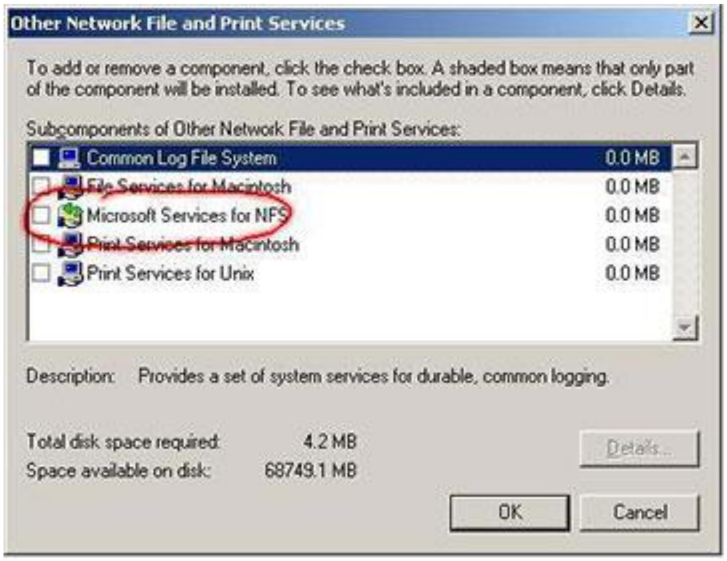
Components:

☑	Other Network File and Print Services	0.0 MB
□	Remote Storage	4.2 MB
□	Security Configuration Wizard	0.6 MB
☑	Subsystem for UNIX-based Applications	1.3 MB
□	Terminal Server	0.0 MB

Description: Shares files and printers on this computer with others on the network.

Total disk space required: 4.2 MB
Space available on disk: 68748.9 MB

Now select the Details button. A new window will open titled “Other Network File and Print Services.”



Other Network File and Print Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

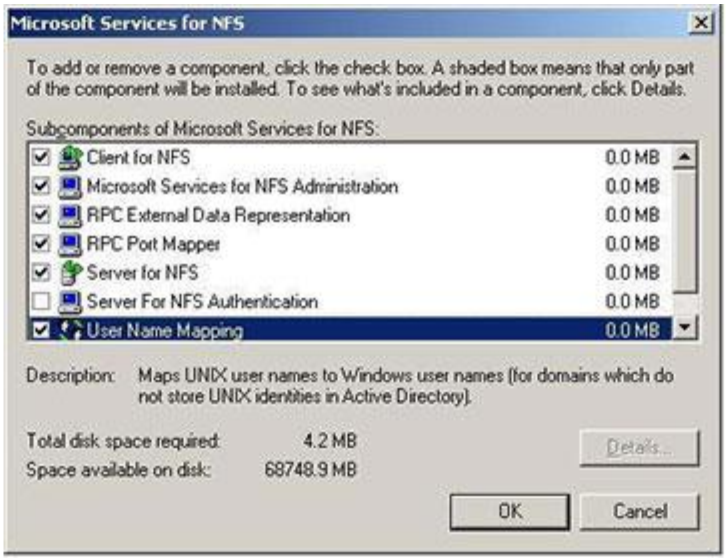
Subcomponents of Other Network File and Print Services:

□	Common Log File System	0.0 MB
□	~~File Services for Macintosh~~	0.0 MB
□	Microsoft Services for NFS	0.0 MB
□	~~Print Services for Macintosh~~	0.0 MB
□	Print Services for Unix	0.0 MB

Description: Provides a set of system services for durable, common logging.

Total disk space required: 4.2 MB
Space available on disk: 68749.1 MB

From this Window choose “Microsoft Services for NFS” and choose Details again. Yet another window will open, showing all of the available components related to NFS, titled ‘Microsoft Services for NFS.’



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Microsoft Services for NFS:

☑	Client for NFS	0.0 MB
☑	Microsoft Services for NFS Administration	0.0 MB
☑	RPC External Data Representation	0.0 MB
☑	RPC Port Mapper	0.0 MB
☑	Server for NFS	0.0 MB
☐	Server For NFS Authentication	0.0 MB
☑	User Name Mapping	0.0 MB

Description: Maps UNIX user names to Windows user names (for domains which do not store UNIX identities in Active Directory).

Total disk space required: 4.2 MB

Space available on disk: 68748.9 MB

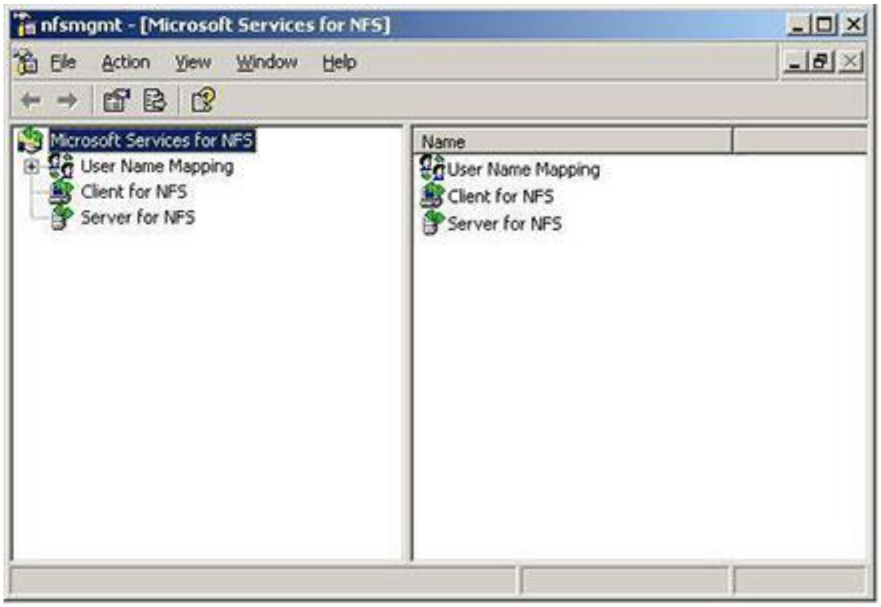
In the 'Microsoft Services for NFS' window you will select all of the components that you need to support your local configuration. You should check all of the available selection boxes in a typical situation because all of these components will be needed. If you are not going to use UNM because all of your client machines are now Windows Vista then you won't need to select User Name Mapping. Once all of the choices are made, click on OK (several times) to begin the installation/activation.

Configuring NFS Server

On Windows Server 2003 R2 the NFS Server can be configured to use UNM or AD/2307. Details on configuring UNM and AD/2307 follow this section.

Configuring NFS Server for UNM

Open the Services for NFS console. This can be started from the Start Menu then Administrative Tools then Microsoft Services for Network File System.



In the left panel select “Microsoft Services for NFS” and then right-click to pop up the action menu. Choose the Properties entry. A new window will open labeled ‘Properties.’ Make sure that the box beside “Active Directory Lookup” is not checked otherwise AD/2307 will be used. In this window enter either the domain name of the machine or the IP address of the machine that the UNM server is running on. Since this is most likely the machine you are starting NFS Server on, this is a good default choice. Any NFS Clients that communicate with this NFS Server should have the same UNM Server. This can prevent confusion if two different UNM Servers have slightly different information. Click OK to close the window.

Now right-click on the entry “User Name Mapping” – it is a sub-item of the “Microsoft Services for NFS” entry in the left panel – to get a popup menu. From this

popup menu select “Properties.” A new window will open titled “User Name Mapping Properties.” You will see two tabs: “UNIX User Source” and “Simple Mapping.” On the Unix User Source tab you can select between “Use Network Information Service (NIS)” or “Use Password and Group files.” (NIS is often grouped under the section “Identity Management,” which also includes Password Synchronization, when you are looking for on-line help or other articles).

When “Use Network Information Service (NIS)” is selected then an NIS server is used to get the UID and GID information to initialize the mapping. With this information two types of mapping can happen: simple and advanced.

When “Use Password and Group files” is selected you can then specify the path to the password file and the group file. These two files will be used to set the information for mapping UIDs and GIDs to users and groups respectively. Both the password and group files must be kept on a filesystem (disk) local to the machine. There can only be one of each file. If you have multiple password and/or group files then it is up to you to manually merge these files together and insure that each file has unique IDs for each entry. With this information two types of mapping can happen: again, simple and advanced.

Simple mapping can happen when the usernames in the password file are identical in spelling and the intended user already is in the Windows user database. This is true when you have specified using NIS or password/group files. Simple maps are the most straight-forward and easiest. If you have been manually administering your users and groups this way then lucky you! Switch to the second tab panel of this Window, “Simple Mapping.” Then check the box labeled “Use Simple maps.” If you have more than one Windows Domain and you are using the password and group files, you may need to select the correct one from the dropdown menu. However, with most networks with only one domain, the default is correct. If you are using NIS then on this tab panel you will need to add the correct NIS domain to get the ID information.

Now click the OK button to set the information.

Advanced mapping must be used when one or more of the usernames in the password file does not match the intended Windows user by either spelling or intended user. The next section deals with Advanced maps in more detail. With either NIS or password/group files you should make sure that the simple mapping is not selected in the User Name Mapping Properties window’s tab named Simple Mapping.

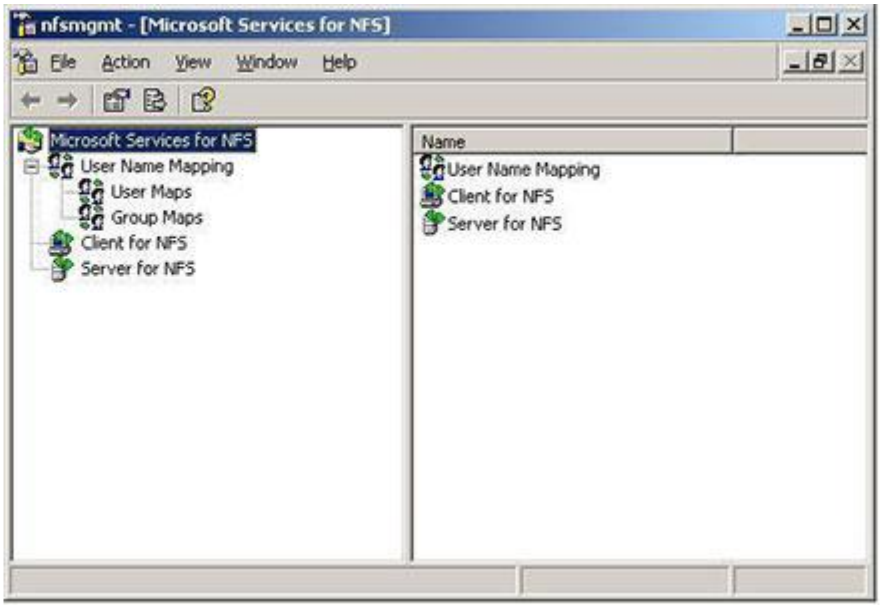
The interval at the bottom of the panel for synchronizing the data is self-explanatory. You can click the “Synchronize now” button to force an immediate synchronization.

Don’t reboot just yet. There is still more to do in the next section if you are using Advanced Mapping.

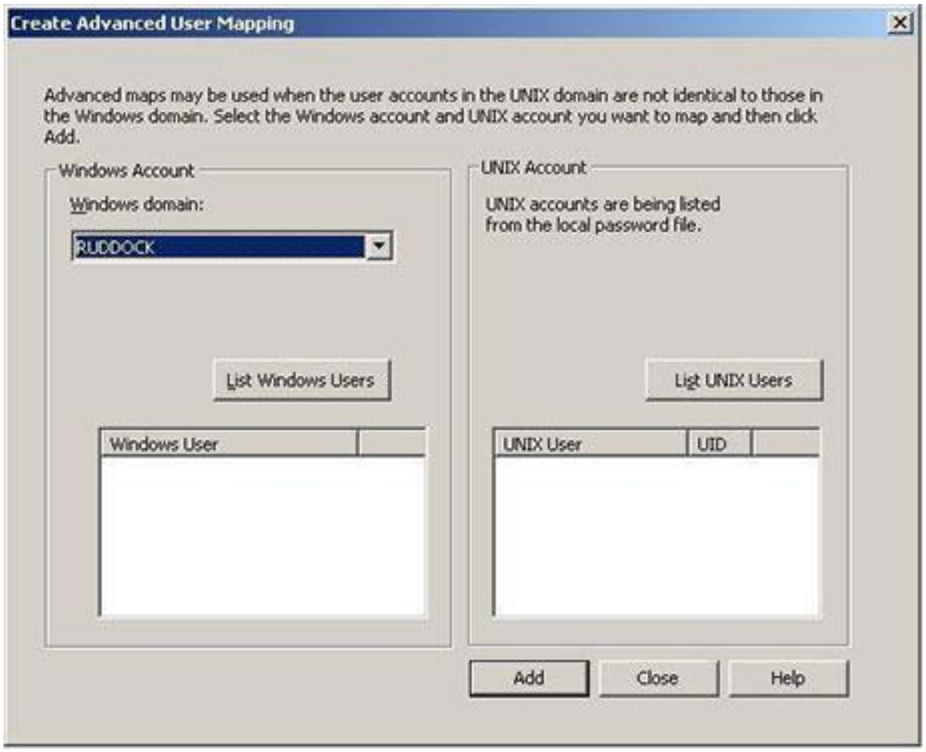
Creating Maps

The user and group maps instruct UNM which Windows user or group is to match to which UID or GID. Thus when a remote machine makes, for example, an NFS request using a UID and GID it can be mapped to a Windows account with a SID so that correct file access permissions are used. There is a third map that controls which hosts are allowed to have or not have access. Again, you must be the Administrator or a member of the Administrators group to make changes to these maps.

In the window for managing Microsoft Service for Network File System, in the left panel expand User Name Mapping by clicking on the plus sign (“+”). This should expand to show two sub-entries: User Maps and Group Maps. With little surprise the method for setting Advanced Maps for users and groups is virtually identical.



To create an Advanced Map for users right click on the “User Maps” entry to get the popup menu and select “Create Map.” A new window will open titled “Create Advanced User Mapping.”



Advanced maps may be used when the user accounts in the UNIX domain are not identical to those in the Windows domain. Select the Windows account and UNIX account you want to map and then click Add.

Windows domain: RUDDOCK

UNIX accounts are being listed from the local password file.

You will see two sections on screen. The left side is for listing Windows users and the right side is for listing Unix users. Click the appropriate button to get a list of the Windows and Unix users. Select the Windows user on the left side (with a mouse click) and then select the Unix user in the right side that are to map to each other. Then select "Add" to set the mapping. Repeat these steps for as many maps as you need to do. You can have many Windows users mapping to one Unix account, but this should be highly discouraged for security reasons.

Creating an Advanced Map for groups is so similar to creating an Advanced Map for users you should already understand and need no further instruction.

The final map to be concerned with is the ".maphosts" file. This file sets the criteria for allowing or denying access from remote host machines. The syntax is similar to NIS syntax. Each line in the file specifies one hostname. If a line has no modifiers then the current default is used; initially this is "+". This is the same as if the "+" modifier was added at the end of the line. If the "-" modifier is specified at the end of the line then this host id is denied access. A modifier on a line by itself indicates accepting (+) or denying (-) all hosts not already specified on lines above. An example file is:

```
Rootbeer +
Cola -
Orange
+
```

In this example the host rootbeer is allowed access while cola is denied access. The host orange is denied access since the last modifier given was a "-". The final line, just a "+" indicates that all other hosts are allowed access.

You should not have any hosts or modifier listed after a line that has only a "+" or "-" because these lines will be ignored.

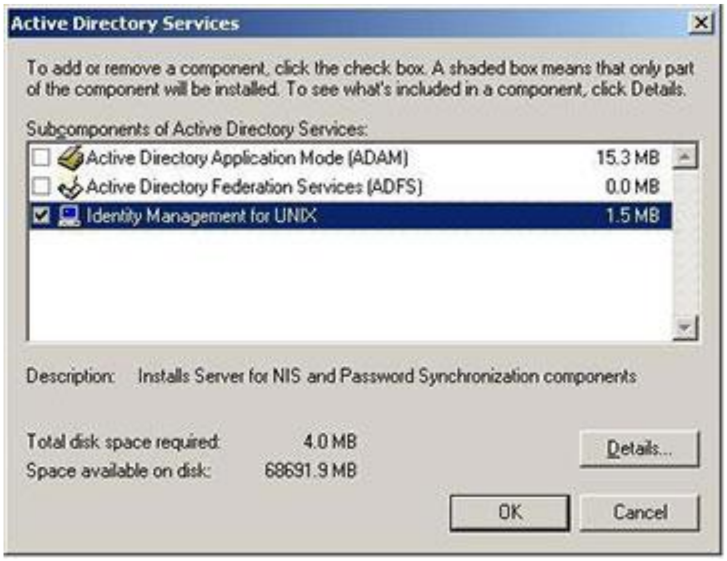
The ".maphosts" file is located in the %WINDIR%/msnfs directory. It can be edited with either a Windows or Interix editor.

Now that User Name Mapping is finished you should restart the UNM Service. You can do this more than one way. One method is with the Microsoft Services for Network File System panel. Right click the User Name Mapping entry to get the popup menu. Now stop the service. Once the service has stopped then start the service again with the popup menu selection.

Configuring 2307/AD for Unix IDs

By default the ability to set Unix IDs in Active Directory is not activated. The Server for NIS needs to be installed and activated.

The first thing is to get NIS installed. Without it installed then the RFC 2307 part of AD cannot be used. From Add/Remove Programs select Add/Remove Windows Components. From the component window select "Active Directory Services" and then click the Details button. This will display the "Active Directory Services" window.



Active Directory Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Active Directory Services:

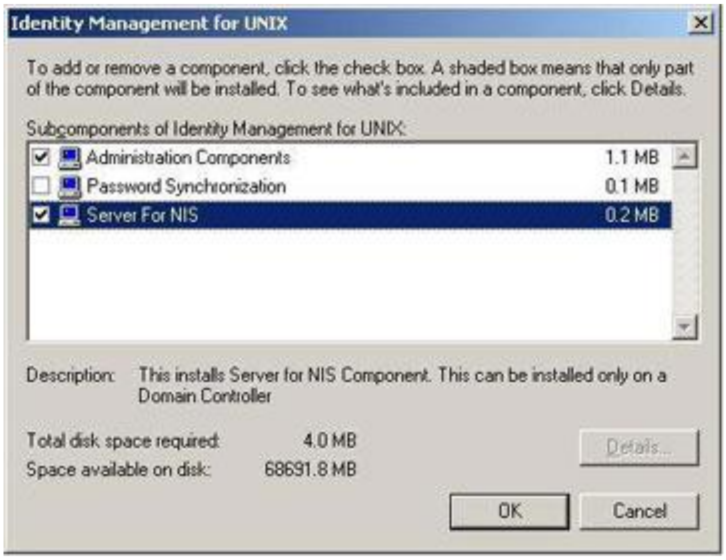
☐	Active Directory Application Mode (ADAM)	15.3 MB
☐	Active Directory Federation Services (ADFS)	0.0 MB
☑	Identity Management for UNIX	1.5 MB

Description: Installs Server for NIS and Password Synchronization components

Total disk space required: 4.0 MB

Space available on disk: 68691.9 MB

In the next window select "Identity Management for UNIX" and click the Details button again. Another window will open. Select "Server for NIS" and check the box associated with it. When you do this the check box with "Administration Components" will be checked automatically. This is required.


Identity Management for UNIX

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Identity Management for UNIX:

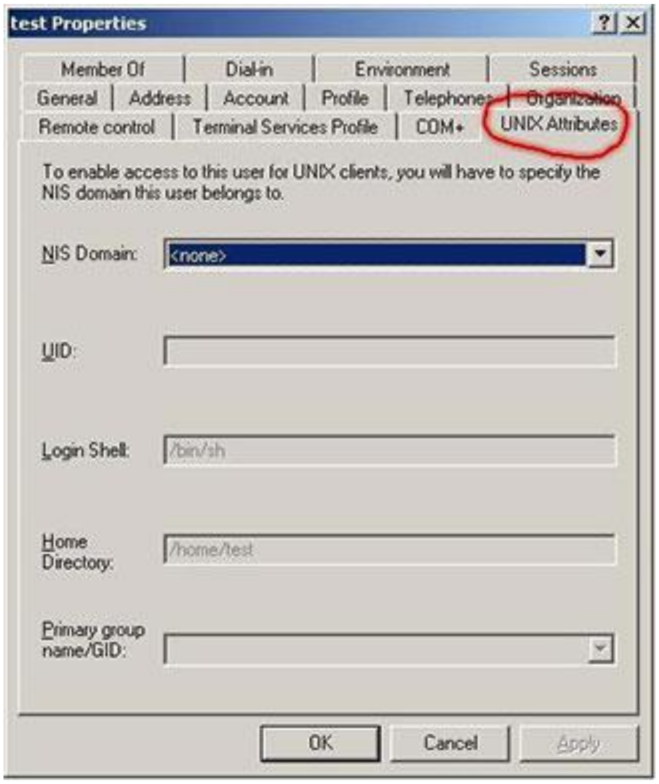
- ☑ Administration Components 1.1 MB
- □ Password Synchronization 0.1 MB
- ☑ Server For NIS 0.2 MB

Description: This installs Server for NIS Component. This can be installed only on a Domain Controller

Total disk space required: 4.0 MB
Space available on disk: 68691.8 MB

Now click OK in this window and click OK in the next window. You should be back at the components window now where you will select the Next button to start the installation. When it is done you will not be prompted to reboot. However, you must reboot to get the new 2307 information shown when you are looking at AD user information.

After the reboot, when you look at the Properties of a user in Active Directory, you will see a new tab labeled “UNIX Attributes.”


test Properties

To enable access to this user for UNIX clients, you will have to specify the NIS domain this user belongs to.

NIS Domain: <none>

UID:

Login Shell: /bin/sh

Home Directory: /home/test

Primary group name/GID:

The first thing to do is to select the NIS domain. Once this is done then the other selectable and settable items become active. There are default entries for UID, shell and home directory. The entry for the Primary Group is left empty. You can change these values to match your needs. For example, it is quite common to change the default shell to "/bin/csh" or "/bin/bash."

You can make these changes one user at a time through the AD GUI or through the command line utilities. With the command line utilities you can create a script to automate changes for a large group of users. An example of this would be changing the default shell for all users. This is a task that is slow, boring, tedious and error prone when using a GUI but quick and accurate with a script.

With Server for NIS installed you will want to set Services for NFS to use Active Directory. This will use the UNIX Attributes IDs for mapping identities. From the Microsoft Service for Network File System management console right click the

left panel entry "Microsoft Service for NFS" and select Properties. In the window that opens check the box beside "Active Directory Lookup." Then enter the name of the Active Directory domain in the box below.

You should reboot the system for this change to properly take effect.

Mapping of user and group IDs to and from NFS for Windows accounts will get the information from Active Directory now. The IDs used will be those specified on the UNIX Attributes panel of the User's or Group's property window.

Configuring NFS Server for AD/2307

With RFC 2307 Active Directory can store Unix IDs (user and group) on a per user basis. This allows for a mapping between Windows SID and Unix UIDs/GIDs. If you are going to have both UNM and AD/2307 working at the same time, please remember that it is important to keep both synchronized with the same information for security reasons.

Open the Microsoft Services for NFS console. This can be started from the Administrative Tools entry in the Start Menu.

In the left panel select "Services for NFS" and then right-click to pop up the action menu. Choose the Properties entry. A new window will open labeled 'Properties.' Have the box beside "Active Directory Domain Lookup" checked. Then enter either the domain name of the machine or the IP address of the machine that AD is running on for your Windows Domain. Then click OK.

You may need to reboot your machine for this change.

Sharing filesystems by NFS

Regardless of which choice is made for ID mapping you will need to adjust any firewall the system is using so that NFS clients can communicate with the server. You will need to ensure that the following ports are open before sharing any filesystem:

- UDP: 111, 1039, 1047, 1048 and 2049.
- TCP: 111, 1039, 1047, 1048 and 2049.

Once the ports can pass through the firewall then filesystems can be shared with the NFS Server. Within Windows Explorer select the filesystem to be shared by NFS. Then open a pop-up menu for the filesystem to be shared (right-click the mouse). From the popup menu select 'Sharing and Security' or 'Properties.' (It doesn't matter since both open the same window.) A new window will open with several tabs. Select the tab labeled 'NFS Sharing.' On this panel choose "Share this folder." Do set a name for this share so other systems can find it. If you have a secure enough network you may want to check the box for Allow Anonymous Access. If your anonymous ID is something other than “-2” you’ll need to change the default ID.

By default the filesystem shared by NFS is given read-only access with root access disallowed (quietly re-mapped to the anonymous ID). You can adjust this by clicking on the Permissions button to open a new window labeled “NFS Shared Permission.” Current permissions are listed. New permissions can be added and/or current permissions deleted and/or current permissions modified. You can set root access to "allowed" by selecting the checkbox in this window. How to do each is pretty much self-explanatory other than to note that “names” to add are machine names, not user or group names.

If there are any options you want to adjust you can do so now before selecting OK. Once you select OK then the filesystem should be available to an NFS Client.

It would be good to test that the filesystem is now available by attempting to mount it with an NFS Client on another machine. Using another machine will also verify that all network, firewall and access issues have been resolved. If access is a problem check that the client host has been listed with access allowed in the “.maphosts” file. This is the easiest to confirm before checking the firewall ports are open (on server and client) and verifying DNS information for the server and client can be found by each computer.

Summary

There are a lot of different items to install and configure just to get basic NFS Server support; however, the end result can be very productive in a heterogeneous operating system environment. Very few computer sites run solely one operating system these days. But interoperability amongst these systems is a must to avoid confusion and duplication of stored data. Of course security must be maintained as tightly as possible and the UNM and RFC 2307 support in Active Directory both help to ensure this.

Feel free to post a question in the Interop Community forums.