An Oracle Technical White Paper

October 2013

How to Configure IDMU on the Oracle® ZFS Storage Appliance

A step-by-step guide to configure the Oracle® ZFS Storage Appliance to use IDMU for identity mapping between Active Directory (Windows) and Network Information Services (NIS) (UNIX) identities.

Executive Overview

The Oracle® ZFS Storage Appliance identity mapping service manages users of both Active Directory and Network Information Services (NIS) by associating their Microsoft Windows and UNIX identities. This allows shares to be exported and accessed by clients using either the Server Message Block (SMB) or Network File System (NFS) protocol.

The Oracle ZFS Storage Appliance identity mapping service can use Microsoft Identity Management for UNIX (IDMU) to create correlations between Windows and UNIX identities on the appliance. This document explains this IDMU mapping approach.

For the purposes of this document, an initial configuration of existing NIS servers and clients and Active Directory servers and clients, each existing in isolation, is assumed, as seen in figure 1's basic architecture. The introduction of an Oracle ZFS Storage Appliance to this infrastructure allows files to be shared with consistent permissions between the Windows and UNIX environments.

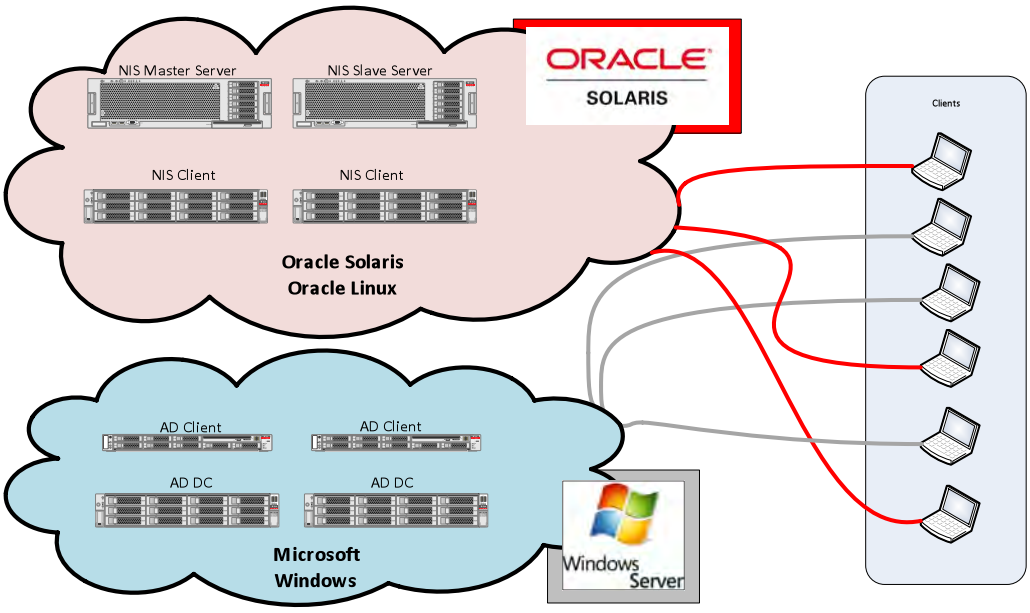

Figure 1. Basic architecture example for isolated server/clients

Figure 1 shows that the Microsoft Windows and Oracle Solaris and Oracle Linux environments exist in isolation. Files cannot be shared easily between the two environments or accessed simultaneously by both environments.

The addition of an Oracle ZFS Storage Appliance provides a bridge between the two environments, with files shared simultaneously and with consistent access permissions between each environment, as shown in figure 2.

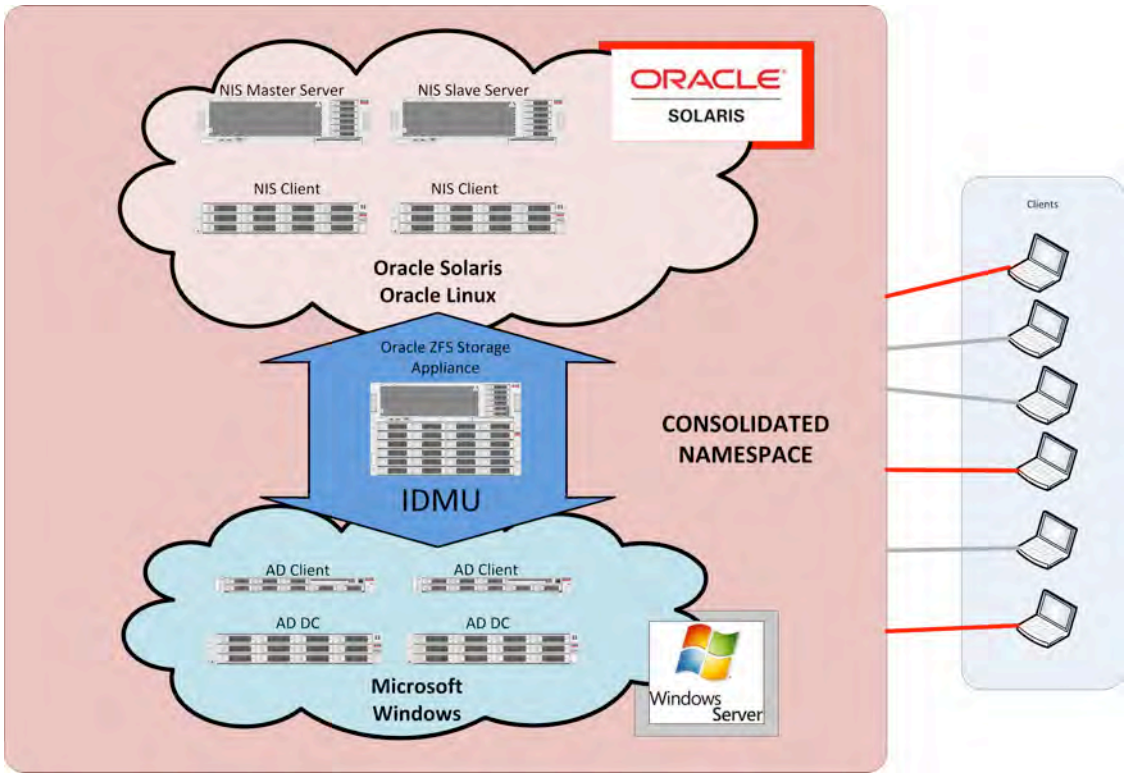

Figure 2. Oracle ZFS Storage Appliance bridging environments

Overview of Required Configuration Tasks

The following steps are executed in order to configure the Oracle ZFS Storage Appliance to enable directory access to both Active Directory and NIS environments and also to configure the Windows Server environment to provide services to both Active Directory and Network Information Services (NIS) clients.

1. Configure the Oracle ZFS Storage Appliance to access Active Directory.
2. Install Windows Server Identity Management for UNIX.
3. Export the NIS text maps from the NIS environment.
4. Import the NIS text maps to the Windows Server Identity Management for UNIX.
5. Enable and configure the Oracle ZFS Storage Appliance IDMU service.
6. Configure the Oracle ZFS Storage Appliance to access NIS.

7. Configure the NIS clients to access the Windows Server Identity Management for UNIX.
8. Reconfigure the NIS servers.

Preconditions for setup

The setup instructions in this document are based on the assumption that the following conditions are already met:

- The Oracle ZFS Storage Appliance has a proper network configuration and is able to route to NIS and Active Directory servers.
- A storage pool has been created on the Oracle ZFS Storage Appliance.
- The root passwords of the NIS servers and clients are known.
- A Windows domain administrator account username and password is known.
- Any Network Time Protocol (NTP) server keys are known.

Domain name conventions used for the example case

In the following pages, the example shown is from a fictitious company called Lavemill. Lavemill has two DNS servers at 192.168.1.5 and 192.168.1.6. The NIS servers provide for Oracle Solaris and Oracle Linux servers and are themselves Oracle Linux servers. The master NIS server is called `oel-NISsvr` and the slave server is named `oel-NISslv`.

The NIS domain is `nis.lavemill.org`.

The AD domain is `ad.lavemill.org`.

The DNS domain (`lavemill.org`) has the appropriate delegations for the AD servers to provide DNS servers at `ad.lavemill.org`.

The NIS servers also provide NTP services to the network to allow for clock synchronization.

These domain names are fictitious and are used to avoid ambiguity. In practice, the AD domain would probably be `lavemill.org` – as would the NIS domain.

Configuring the Oracle ZFS Storage Appliance to Access Active Directory

This section describes the settings required to configure the Oracle ZFS Storage Appliance to access the Active Directory services. The three steps are:

1. Setting up the DNS Services
2. Setting up the NTP Services
3. Joining the Active Directory Domain

Setting Up DNS Services

In order to locate the Active Directory service servers, the Oracle ZFS Storage Appliance DNS Service must be configured to refer to the DNS records provided by the Active Directory servers.

To set up the Oracle ZFS Storage Appliance DNS Service, open a web browser and in the URL field, enter `https://` followed by either the hostname of the Oracle ZFS Storage Appliance or the IP address, and then the port number 215. Figure 3 shows an example of the URL path.

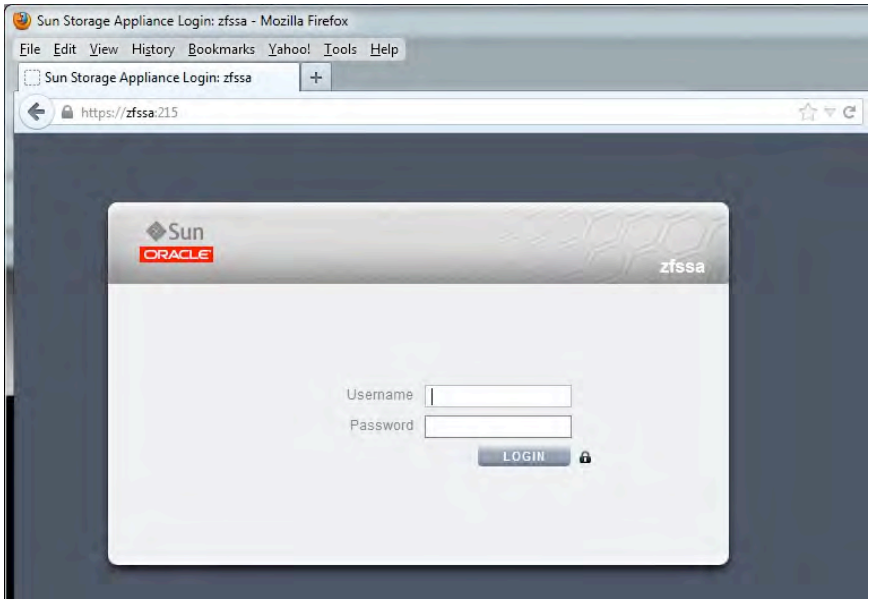

Figure 3. Creating the URL path to log into the Oracle ZFS Storage Appliance Browser User Interface

1. Enter the Oracle ZFS Storage Appliance administrator **Username** and **Password** and select **LOGIN.**

Once successfully logged in, you should see a screen similar to the following.

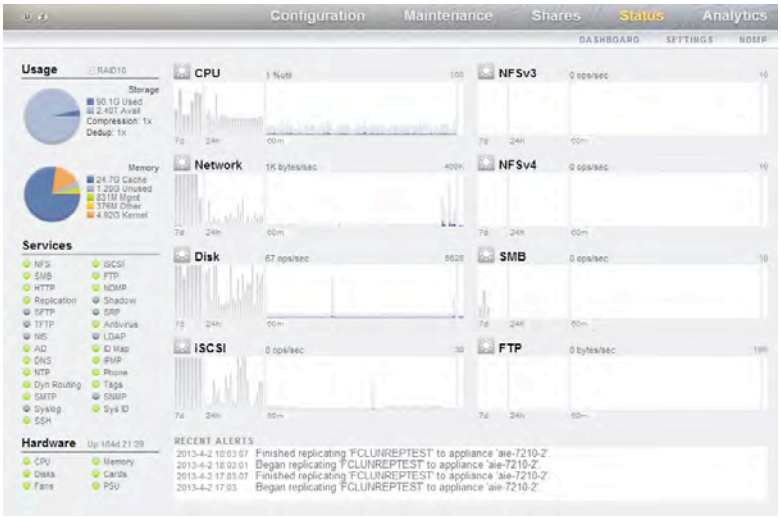

Figure 4. Status Page in the Oracle ZFS Storage Appliance BUI

2. Select **Configuration / Services,** and **DNS** under System Settings, as shown in figure 5.

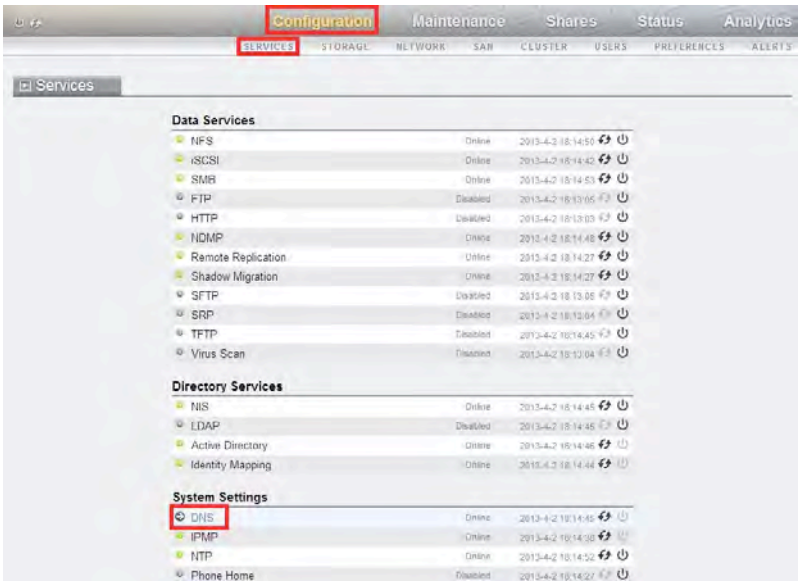

Figure 5. Selecting DNS settings in the BUI

3. Enter the **DNS Domain** name and at least one **DNS Server** IP address as in the example shown. To add additional DNS Server IP addresses, click on the ⊕ icon. Click **APPLY** to continue.

Figure 6. Adding DNS Domain Server details

The DNS Server details should now be complete.

Setting up NTP Services

Active Directory uses Kerberos for its authentication. Because Kerberos is sensitive to clock variations between servers and clients, it is highly advisable to implement the time synchronization service Network Time Protocol (NTP).

Because of the important nature of clock synchronization in authentication and authorization, it is possible to have the NTP servers only respond to commands that contain valid authorization keys.

Use the following steps to ensure clock synchronization.

1. In the BUI, select **Configuration / Services / NTP** as seen in figure 7.

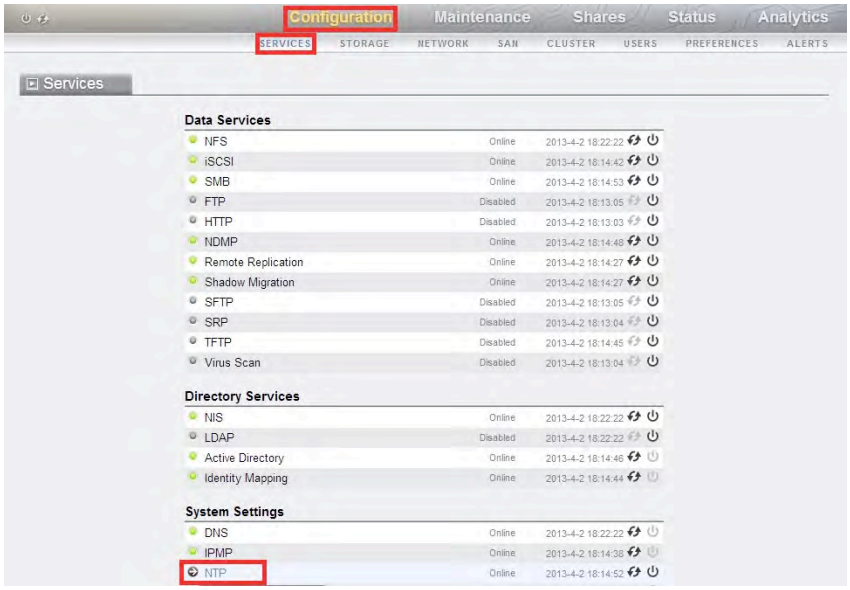

Figure 7. Configuring NTP service in the Oracle ZFS Storage Appliance BUI

2. Select either multicast address discovery or manual NTP server selection as seen in figure 8.

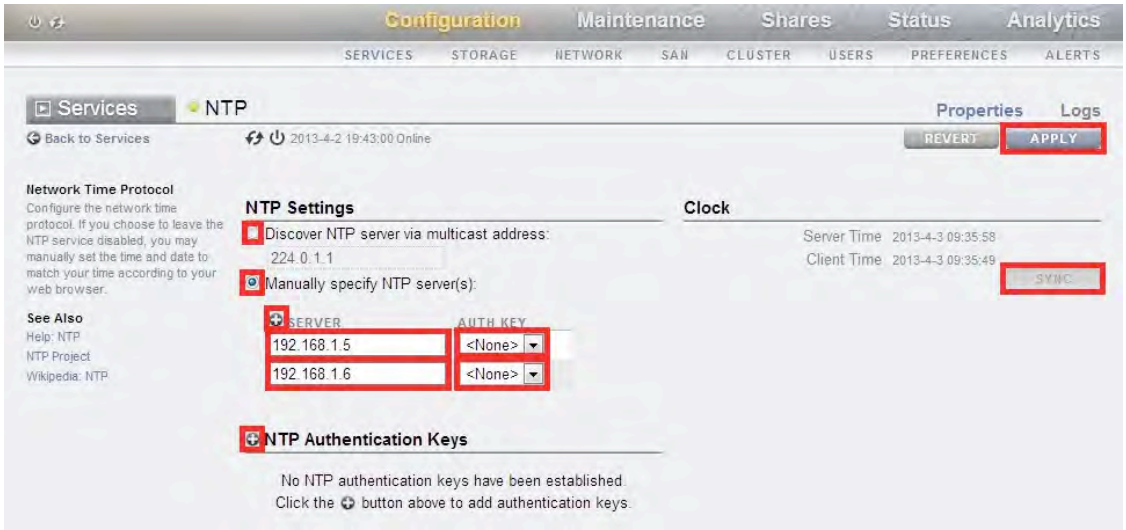

Figure 8. Providing NTP configuration details

3. [Optional] Enter any appropriate NTP authentication keys by clicking the ⊕ icon next to the key definitions.
4. If choosing manual server selection, enter at least one NTP server IP address in the NTP **SERVER** field and optionally select the **AUTH KEY** from the drop-down menu.

   Enter additional NTP server IP addresses by clicking the ⊕ next to the **SERVER** label.
5. Click **APPLY** to continue.

NTP synchronization can take a number of minutes to complete as it uses small adjustments to increase or decrease the rate of time passing as appropriate. You can perform immediate time sync by pressing the **SYNC** button under the Clock section of the BUI NTP settings field.

Joining the Active Directory Domain

Once the DNS and NTP configuration has been set, the next step is to join the Oracle ZFS Storage Appliance to the Active Directory domain. This will allow the Oracle ZFS Storage Appliance to resolve AD user and group names properly when share permissions are altered from Windows clients.

To join the AD domain, use the following steps:

1. Select **Configuration / Services / Active Directory** as shown in figure 9.

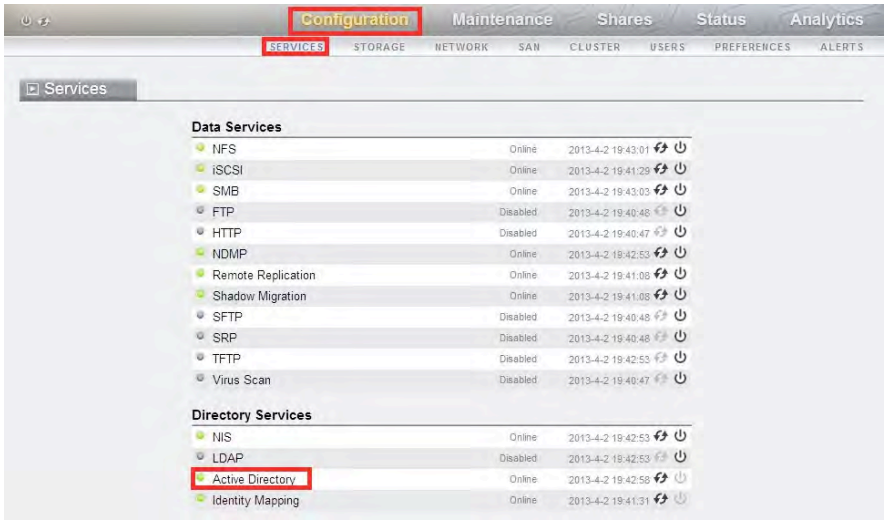

Figure 9. Navigating to Configuration / Services / Active Directory in the BUI

2. Click **JOIN DOMAIN** as shown in figure 10.

Figure 10. Initiating the AD join

3. In the **Join Domain** dialog box, enter the name of the Active Directory domain to be joined, the username of the **Administrative User**, the **Administrative Password** and (optionally) any **Additional DNS Search Path(s)** to be included. This additional search path option allows specified subdomain delegations to be searched, but it is not required in the example seen in figure 11. Click **APPLY** to join using the entered settings.

Figure 11. Join Domain window

The Active Directory summary screen, shown in the following figure, should reflect that the domain is successfully joined.

Figure 12. Successful AD Join

Installing the IDMU Role Service on Windows Server Active Directory

In order to provide the required mapping service from Active Directory to NIS, it is necessary to install an Active Directory role service on the AD domain controller. This installation not only provides the mapping but also enables password synchronization between Active Directory and NIS and configures the domain controller as an NIS master server.

As with all Role Service configuration, perform the addition of Identity Management for UNIX from within the Windows Server Manager application.

1. Start the Server Manager and select **Go to Active Directory Domain Services** from the AD Domain Services panel as shown in figure 13.

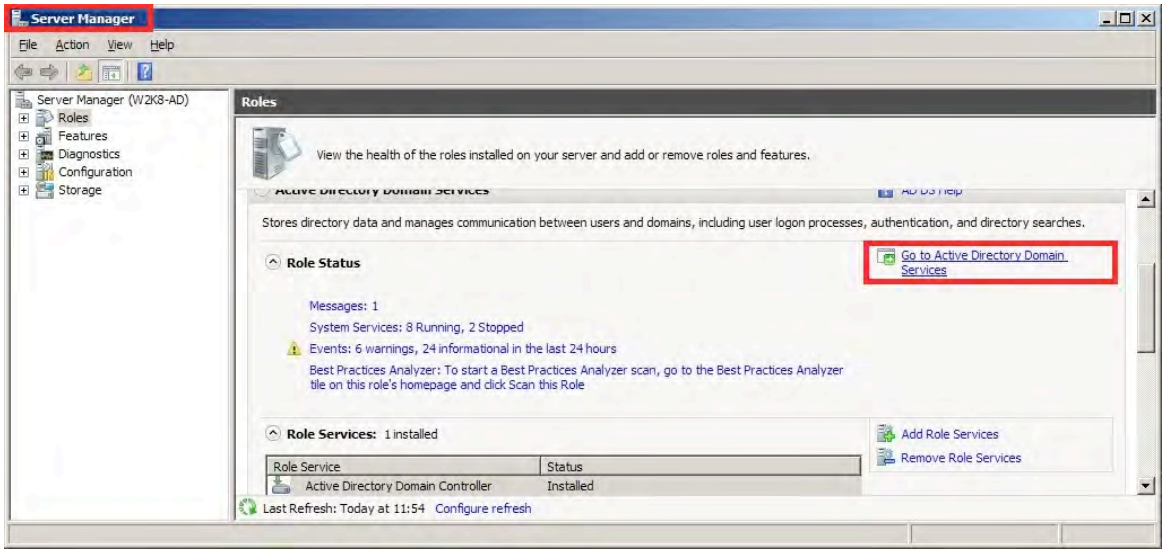

Figure 13. Role Service configuration under Server Manager, selecting AD Domain Services

2. Check to see if **Identity Management for UNIX** is installed. If it is already installed, skip to the next section.

If not, click **Add Role Services** as shown in figure 14 and continue with the remainder of this section.

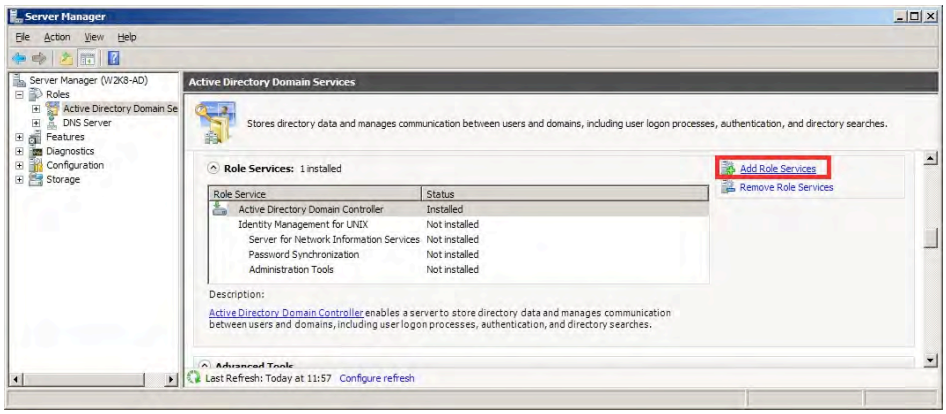

Figure 14. Selecting Add Role Services

3. In the Select Role Services dialog window, click the box next to **Identity Management for UNIX**. Ensure that Server for Network Information Services, Password Synchronization and Administration Tools are all selected as shown in figure 15 and click Next to save and continue.

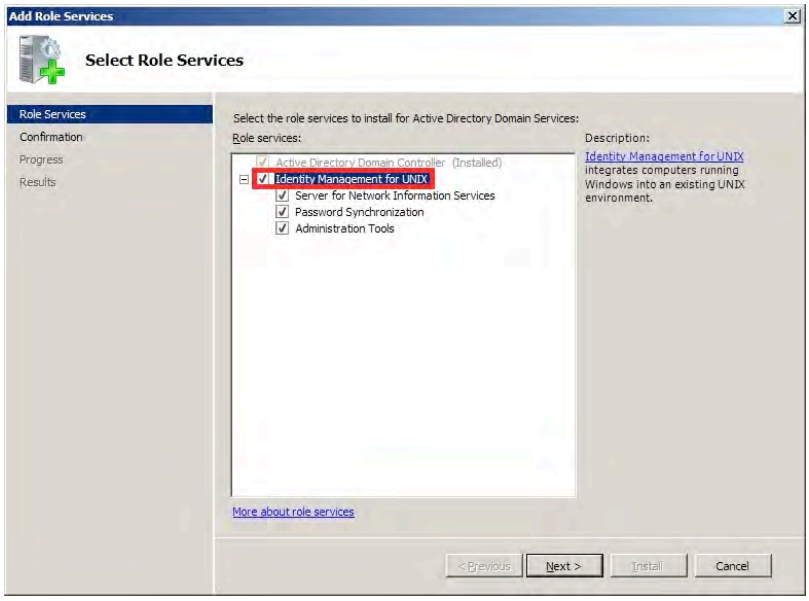

Figure 15. Configuring settings in Select Role Services

4. At the **Confirm Installation Selections** dialog, verify that the operation is correct and click **Install** to continue as shown in figure 16.

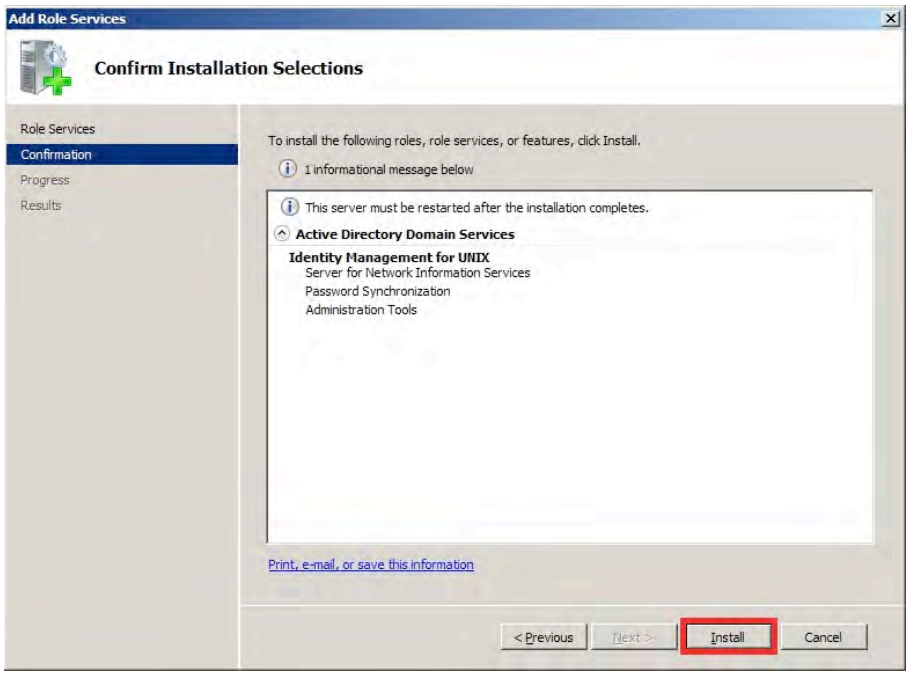

Figure 16. Confirm Installation Selections window

5. Windows Server will now install the relevant role services and will display the **Installation Results** dialog window, as seen in figure 17.

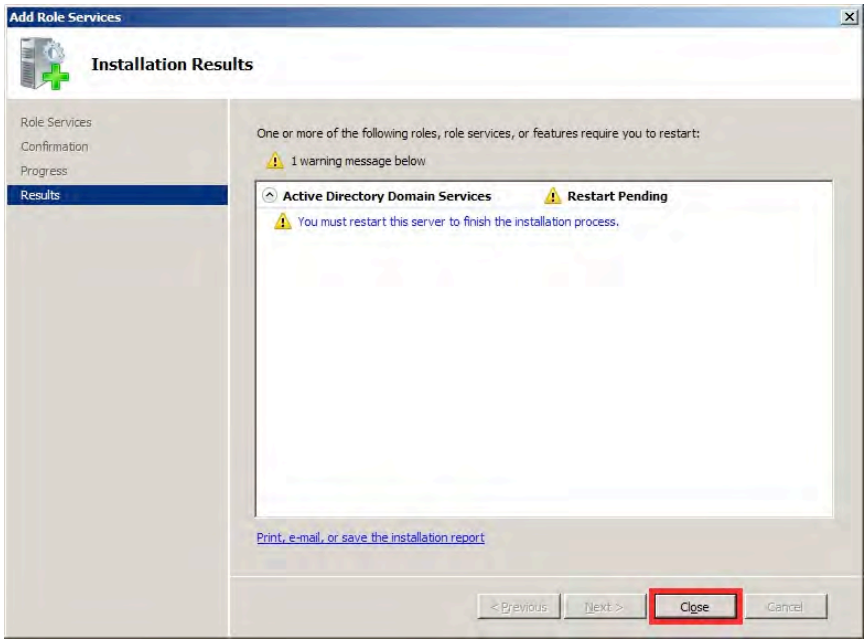

Figure 17. Installation Results window

Note: As displayed in figure 17 and depending on the services that were installed, it may be necessary to restart the Windows domain controller in order to complete the installation.

If the server reboot is required, user permission is first requested from the user. Local server administration policy should dictate when the server may or may not be rebooted.

If you choose not to reboot the Windows server, you will be unable to add or remove and roles, role service or features until the reboot has been completed.

Figure 18 shows an example of the reboot permission dialog window.

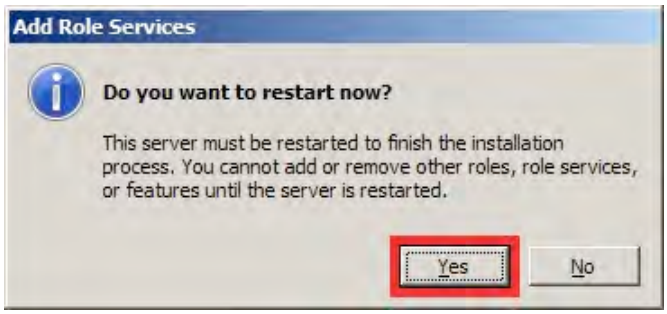

Figure 18. Permission to reboot

6. Once the reboot has been completed, a further **Installation Results** dialog window will be displayed.

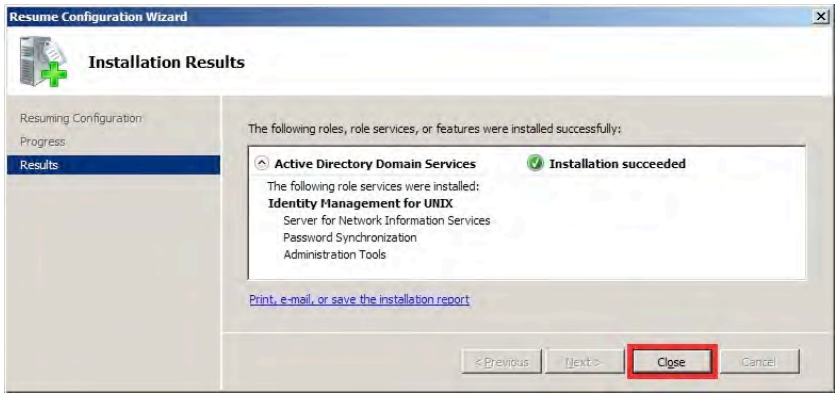

Figure 19. Installation Results summary window

7. The Server Manager screen previously shown in figure 14 should display the updated information with the Role Service status shown in the following figure.

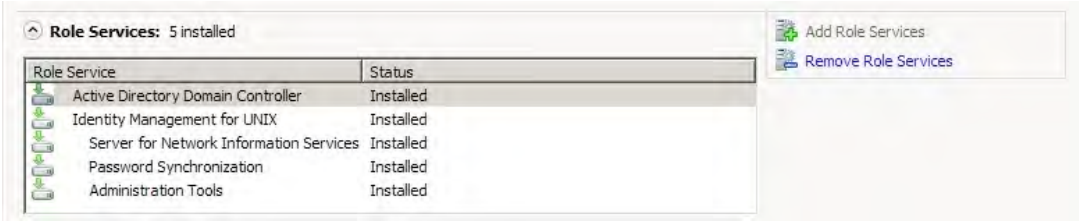

Figure 20. Role Service Summary window

Exporting NIS Text Maps from the NIS Environment

An advantage of using IDMU and Active Directory is that the Windows server then becomes a single directory source with password synchronization among the different types of views into the directory.

When IDMU was installed in the previous section, one of the options installed was **Server for Network Information Services**. Its purpose is to assign the Windows Active Directory domain controller to provide NIS services to the clients that use the services of the Oracle Solaris or Oracle Linux NIS servers.

To do this, the Windows server provides empty NIS maps that can be populated with information exported from the original servers. While populating these maps only requires a few simple steps, the resulting text files may need editing to allow for differences between NIS and Active Directory. Consider the following:

- NIS `passwd` and `group` maps do not share a namespace, which means that you can have a group with the same name as a user. This is common practice and is the default in many Linux implementations when the `useradd` command is used to create user directories and `passwd` file entries. Note that Linux implementations also create a group with the same name as the user being created.
- Active Directory has a shared namespace for security groups and user directory entries, which means that it is not possible to have a group and a user with the same name.
- Depending on the implementation of NIS, the `passwd` map may not contain the encrypted passwords for the users. These may be in the `shadow` map – in which case, this file will need to be migrated too.

Providing for the listed differences, exporting the NIS map information is easily accomplished. Use the following steps to export the `passwd` and `group` maps. Additional

maps may be required as defined by local administration policy. The steps required for these maps should be similar.

NOTE: Microsoft has a best practice guide for running Server for NIS under Windows Server 2008R2, listed in the References section at the end of this document.

1. Log on to one of the NIS clients or servers in a terminal session and become the root user.

```
andrew@laptop$ ssh andrew@oel-NISsvr
andrew@oel-nissvr's password:
Last login: Wed Apr  3 14:06:38 2013 from rasp1.lavemill.org
[andrew@oel-nissvr ~]$ su
 Password: XXXXXXXXXXXXXXXX
 [root@oel-nissvr andrew]# mkdir NISexport
 [root@oel-nissvr andrew]# cd NISexport
```

2. Export the NIS maps and edit to add or remove entries as appropriate to conform with local administration policy.

```
 [root@oel-nissvr andrew]# ypcat passwd > passwd
 [root@oel-nissvr andrew]# vi passwd
… Remove / add users as appropriate …
 [root@oel-nissvr andrew]# ypcat shadow > shadow
 [root@oel-nissvr andrew]# vi shadow
 … Remove / add users as appropriate …
 [root@oel-nissvr andrew]# ypcat group > group
 [root@oel-nissvr andrew]# vi group
 … Remove / add groups as appropriate …
```

3. Transfer the output files to the Windows server using USB Flash drive or the network, or by placing them on a share presented by the Oracle ZFS Storage Appliance. Once the files are accessible by the Windows server, they can then be imported into Windows Server for NIS as shown in the next section.

Importing the NIS Text Maps to Services for UNIX

Now that the prepared text files have been created, you can migrate the NIS data to an Active Directory domain. With Windows Server version 2008 R2, you can use either the NIS Data Migration Wizard or the command-line utility `nis2ad`.

When Windows servers are running Windows Server 2012, the NIS Data Migration Wizard is not available, so you must use the command-line utility `nis2ad`.

The continuing example reflects use of Windows Server 2008 R2.

Migrating NIS Data to Active Directory Using the Migration Wizard

To migrate the NIS data stored in the previously created and transported text files, use the following steps:

1. Start the Microsoft Identity Management for UNIX console by opening **Start > Microsoft Identity Management for UNIX > Microsoft Identity Management for UNIX** as shown in figure 21.

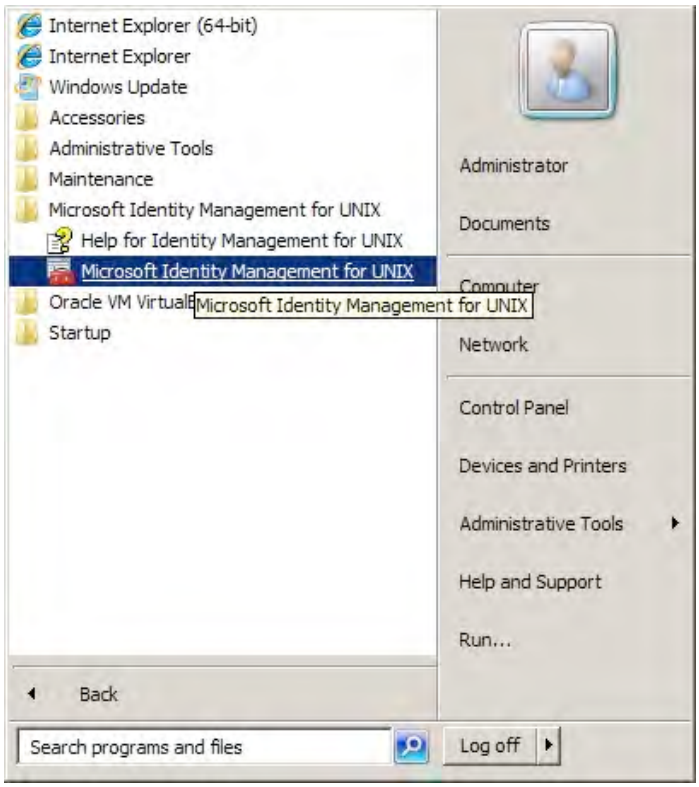

Figure 21. Selecting Microsoft Identity Management for UNIX in the Windows interface

2. When the IDMU console starts, select the entry **Server for NIS** from the leftmost navigation tree and then **Start NIS Data Migration Wizard** from the Actions panel as seen in figure 22.

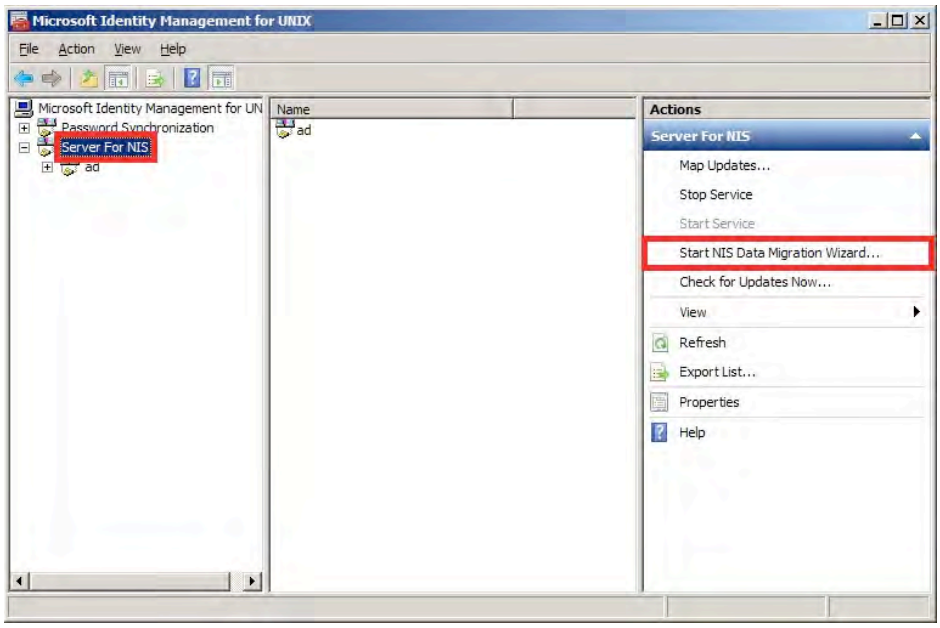

Figure 22. Microsoft Identity Management for UNIX console

3. The **NIS Data Migration Wizard** introduction dialog window is displayed. Click **Next** to continue.

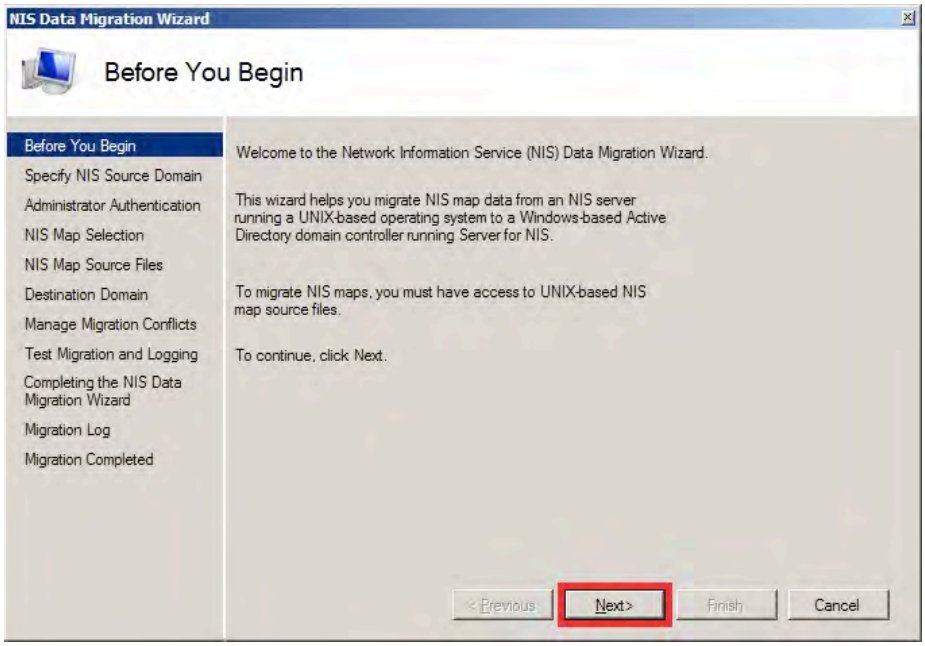

Figure 23. Introductory dialog window for NIS Data Migration Wizard

4. The wizard then prompts for the NIS source domain name. The name shown in figure 24 reflects the continued example from Lavemill. Click **Next** to continue.

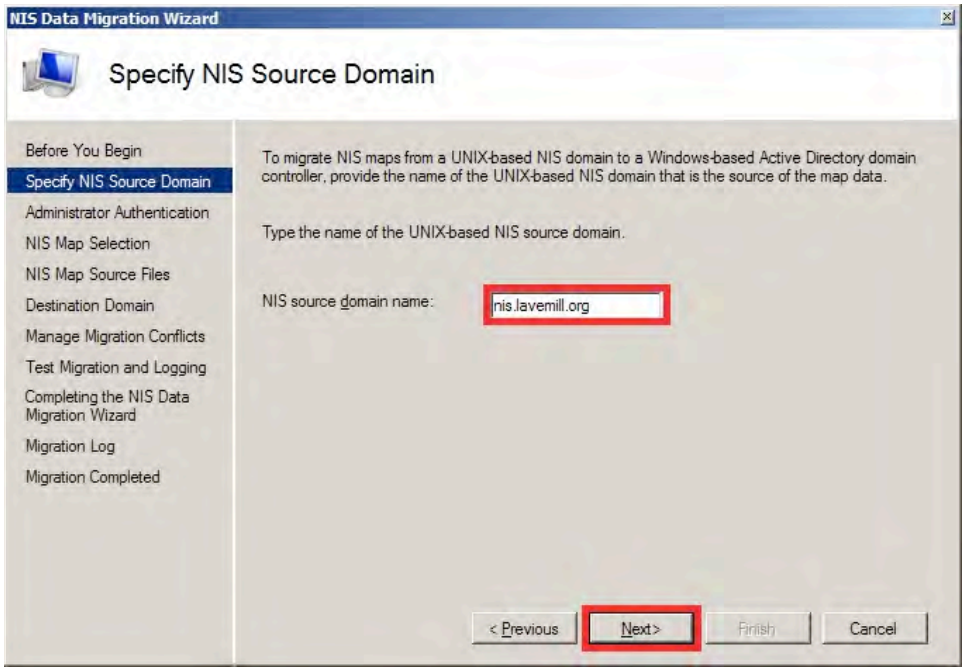

Figure 24. Specifying the NIS source domain name

5. The Wizard then allows you to log on to the Active Directory domain as an administrative user by selecting the radio button shown in figure 25.

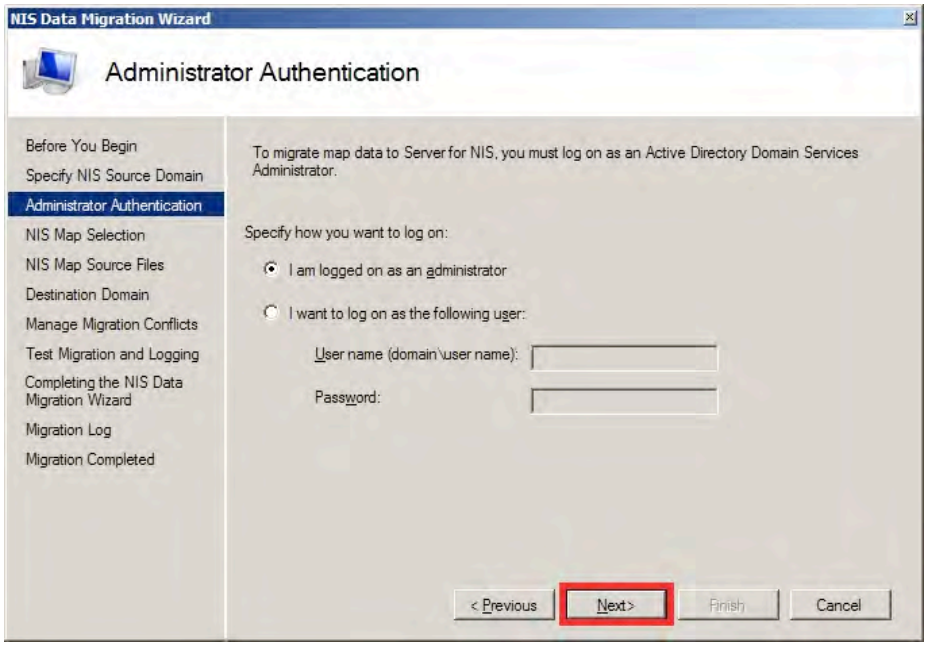

Figure 25. Logging on as an administrator in Administrator Authentication

If necessary, select the “I want to log on…” radio button and enter the **User name** and the **Password.**

In either case, Click **Next** to continue once the appropriate entries have been completed.

6. The Wizard then prompts for which NIS maps to migrate. Select each applicable map name in the **Available NIS maps** list and click **Add>**, ensuring that all the required maps appear in the **Maps to migrate** list. Click **Next** to continue.

Note: Remember that the shadow map may also be required, as previously discussed.

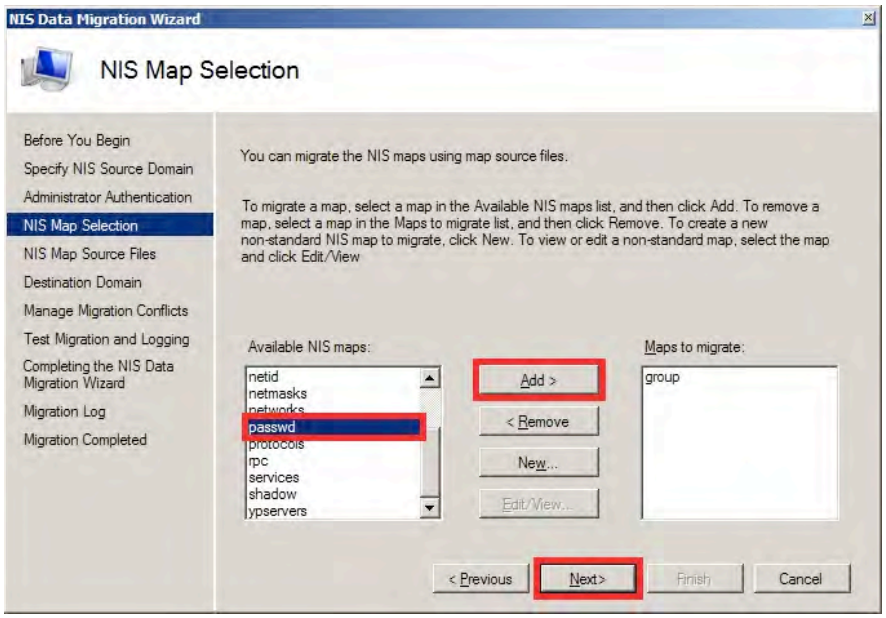

Figure 26. NIS Map Selection window

7. The Wizard next prompts for the location of the NIS map files. Enter the appropriate directory and click **Next>** to continue.

Figure 27 shows, under NIS Map Source Files, that the files have been copied to a USB flash drive from the NIS server, and the inserted drive appears in the Windows Active Directory domain controller as drive e:.

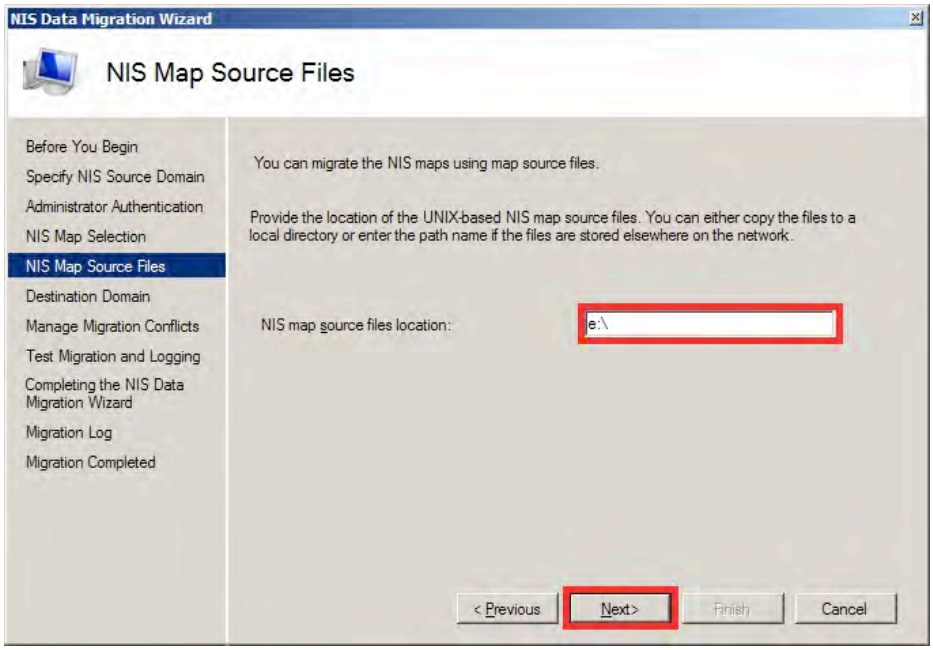

Figure 27. NIS Map Source Files window

8. The Wizard prompts for the Destination NIS Domain for the NIS maps, which may be migrated into a new domain or merged into an existing NIS domain. The NIS domain being prompted for is the one that the Windows server will control rather than the source domain.

Select the appropriate radio button for either the existing domain (which was created when Microsoft Identity Management for UNIX was installed and has the same name as the first part of the AD domain name – that is, up to the first period. In the example, the Active Directory is `ad.lavemill.org` so the IDMU-controlled domain created upon installation is `ad`.

The Wizard offers the opportunity to specify an Active Directory Domain Services (DS) container to hold the migrated data. If no container name is entered in the **AD DS container name** field, the default container is used.

The default values will be used with the following example screen settings. Clicking **Next>** continues the data migration setup process.

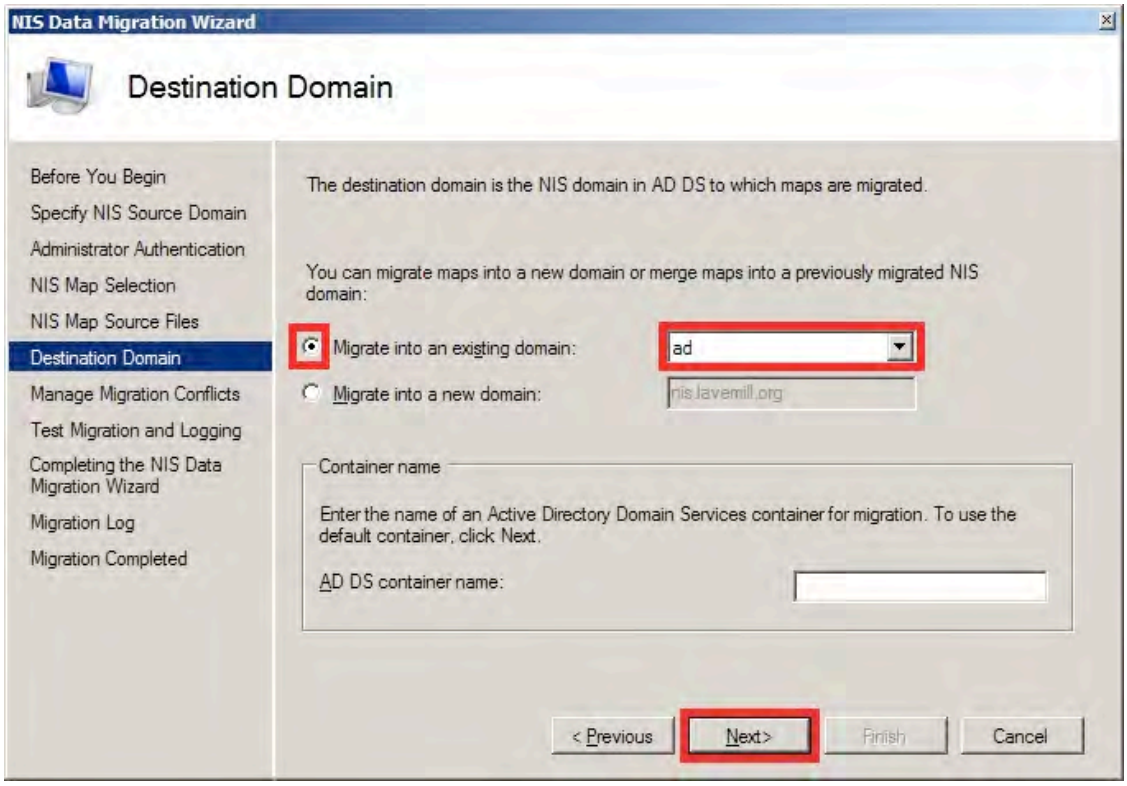

Figure 28. Choosing the default domain container in the Destination Domain screen

9. The Wizard then presents the options for conflict management. A conflict can arise when an entry exists with the same key as one the Wizard is attempting to add. This can happen if a user already exists in Active Directory as well as the NIS maps. It can also happen when a group name conflicts with an existing username, as previously discussed.

There are three options for a conflict:

- Overwrite the Windows Active Directory account information with NIS data.
- Rename the Windows AD account – if two objects of different types have the same name, Server for NIS changes the names of both objects before migrating data.
- Preserve the Windows AD account information.

Choosing the correct option for conflict resolution depends on local policy and knowledge of the data being migrated. For example, if there are a small number of conflicting entries, it may be easier to preserve the Windows AD account information and manually add the respective UNIX User IDs (UIDs) or Group IDs (GIDs) after the migration process. In this case, select the last option's radio button.

Next, the log of the migration conflicts can be saved in a directory other than the default `c:\windows\IDMU\nis\conflicts.log` and this can be entered in the **Record conflicts in this file** field.

In the example, the last option is chosen and **Next** is selected to save the settings and continue.

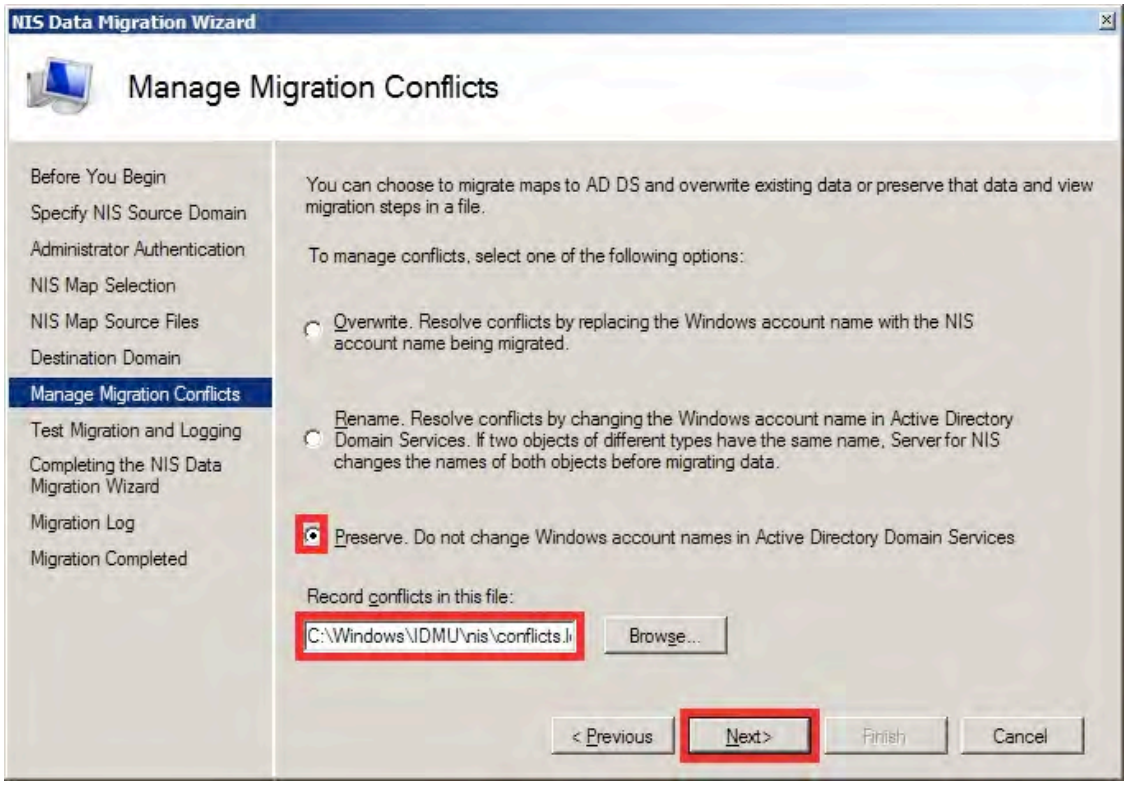

Figure 29. Choosing the default directory location in the Manage Migration Conflicts window

The Migration Wizard offers the opportunity to perform a dry-run test by reporting potential problems it may find. Not all errors may be captured using this method; conflicts caused by data migrated earlier in the same process may exist. For example, a user and group may share the same name in NIS, but since the users are not migrated during the dry-run test, there is no conflict detected until the migration is actually run.

It is advisable to perform the dry-run migration to determine the scale of any conflicts. Do so by clicking the **Do not migrate (log only)** radio box.

You can change the migration file location and name at this point if you wish to alter it from the default of `c:\windows\IDMU\nis\nis2ad.log`.

The example in figure 30 shows the dry-run test's selection.

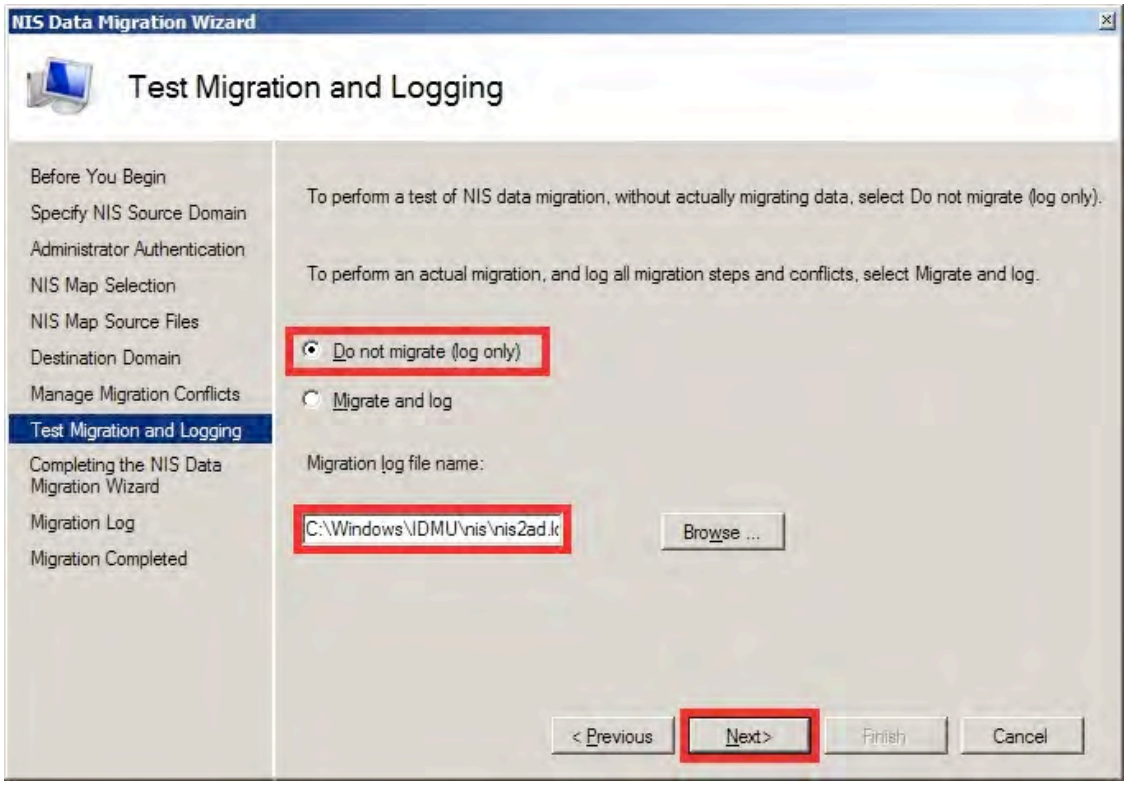

Figure 30. Selecting a test run in Test Migration and Logging

10. The next screen, shown in the following figure, provides a summary of the NIS Data Migration operation before executing either the dry-run test or actual mode. Click **Next>** to run.

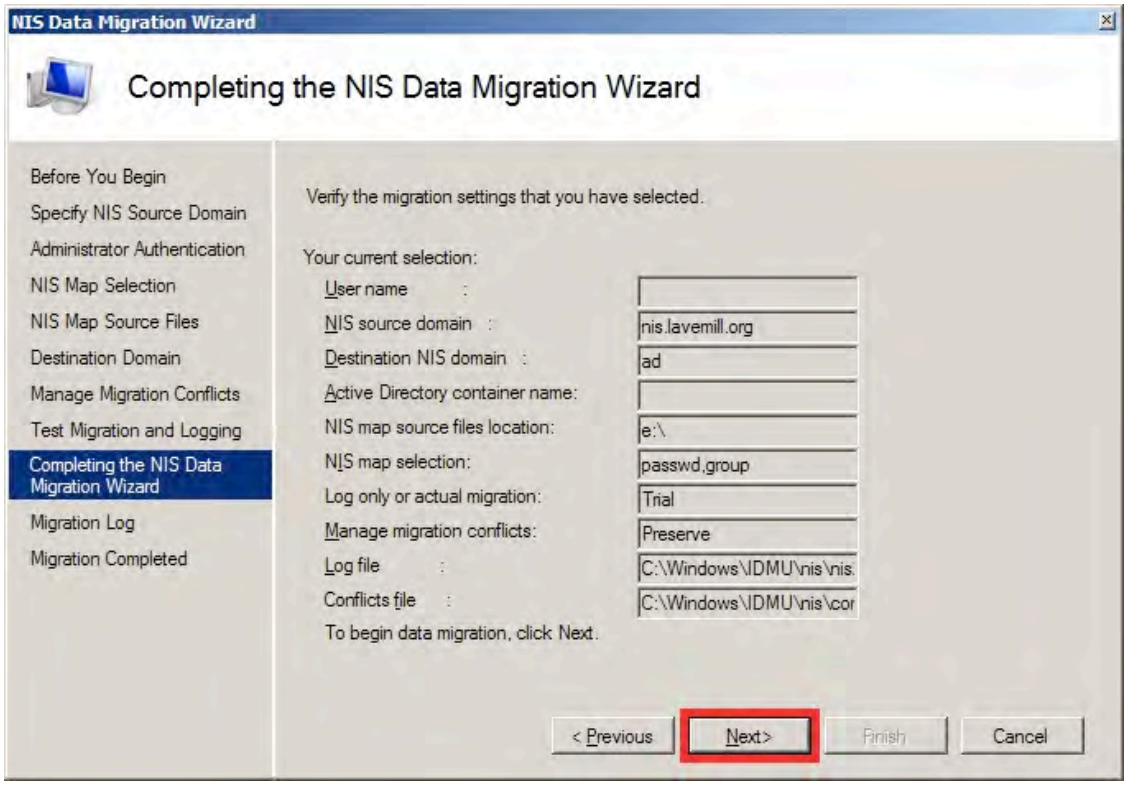

Figure 31. Summary details in the Completing the NIS Data Migration Wizard window

Should any errors / conflicts occur for any of the maps, a warning will be displayed for each map in conflict. To proceed, click **OK** for each warning.

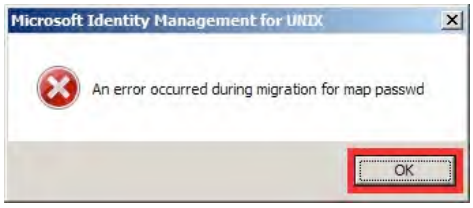

Figure 32. Conflict warning message in the Migration Wizard

11. Once all the maps have been processed, the migration and conflict logs can be viewed to determine what needs to be changed or ignored in order for the migration to complete.

If the option for the dry-run was taken, it is possible to actually perform the operation by clicking **Next>** to continue.

Figure 33 shows an example of the Migration Log screen.

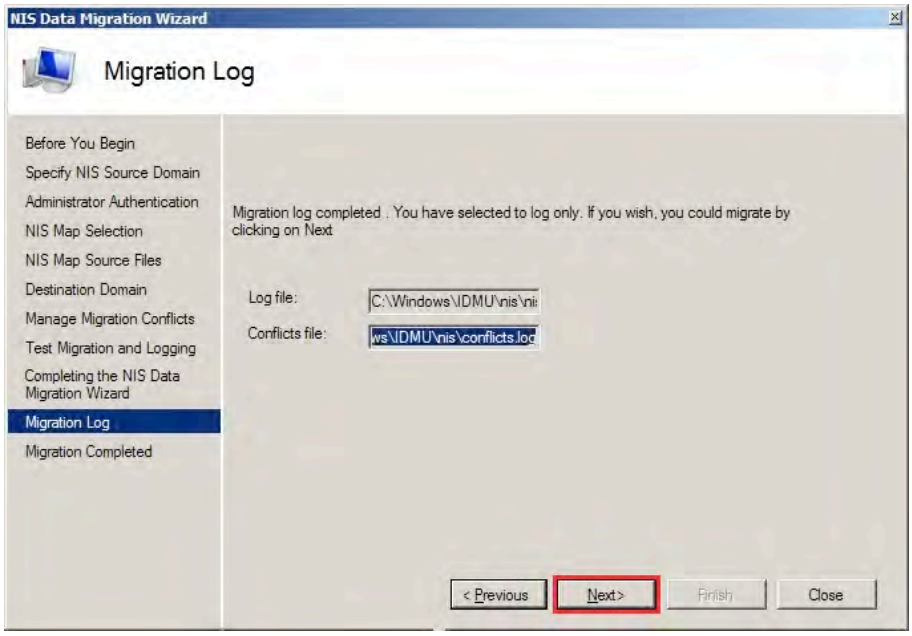

Figure 33. Migration Log screen showing location of conflicts log

Resolving Migration Conflicts – Using the Lavemill Example

Figure 34 shows Lavemill's Active Directory domain containing the users and security groups, prior to any migration.

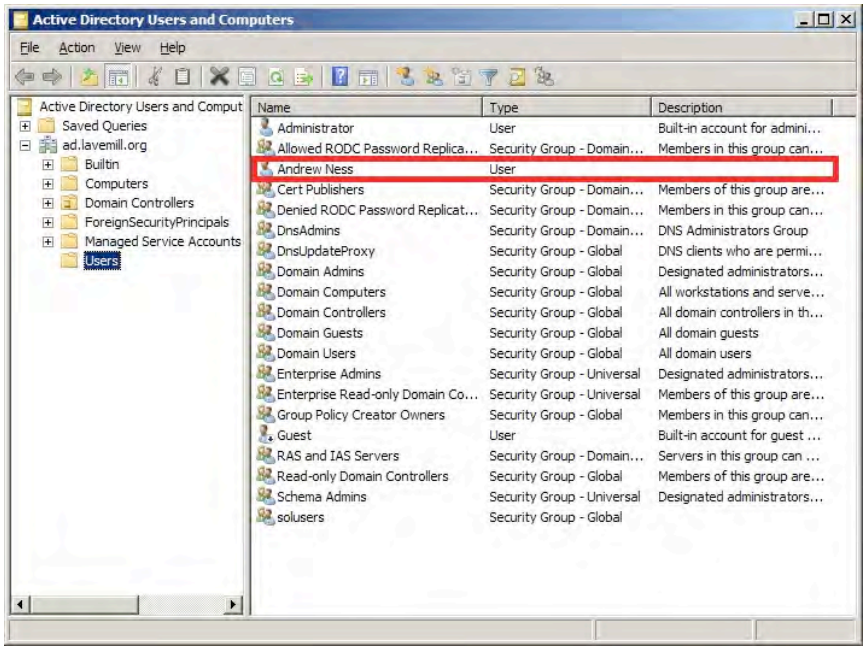

Figure 34. Pre-Migration Users and Groups

There is currently only one user – Andrew Ness, whose Windows login name is `andrew`. Andrew is a Windows domain administrator who also has Oracle Solaris and Oracle Linux accounts which are held in the NIS domain `nis.lavemill.org`.

The NIS maps also contain other users who can be seen in the following NIS `passwd` map.

```
ainsley:$1$1jdc2i8c$:80593:80593:Ainsley:/export/home/ainsley:/bin/bash
andrew:.NuBO0fGs:80592:10000:Andrew:/export/home/andrew:/bin/bash
chloe:$1$yZvjviDA /LLl.:80594:80594:Chloe:/export/home/chloe:/bin/bash
connor:$1$WjaK09.:80595:80595:Connor:/export/home/connor:/bin/bash
```

The NIS group map contains the following entries:

```
engineers:!:501:andrew
medical:!:502:ainsley
students:!:503:chloe,connor
solusers:!:10000:
andrew:!:80592:andrew
ainsley:!:80593:ainsley
chloe:!:80594:chloe
connor:!:80595:connor
```

The NIS migration has been attempted with just the `passwd` and `group` maps. Figure 35 shows the resultant log file for the conflicts.

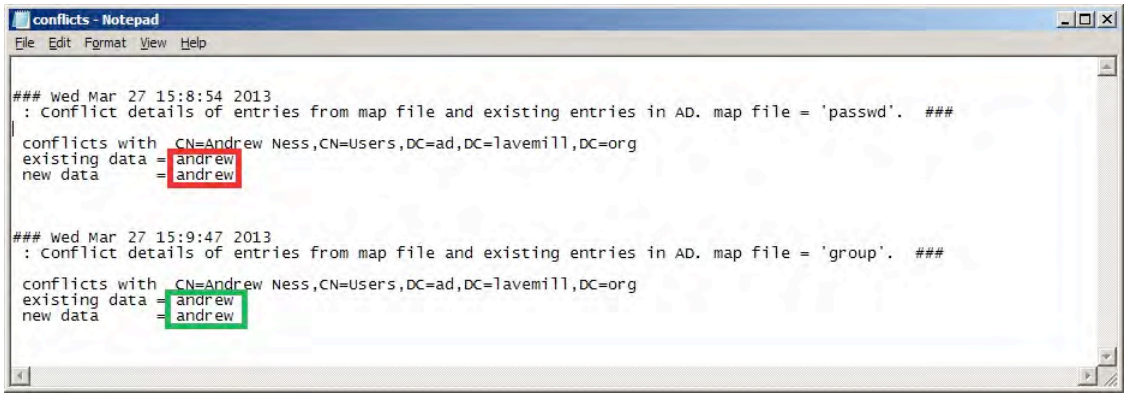

Figure 35. Dry-run conflicts log for Lavemill migration

The conflict log has shown that all the users except `andrew` (highlighted in the upper box in figure 35) and all the groups except `andrew` (highlighted in the lower box) were created properly.

The migration is then run in earnest without modifying the NIS text files in any way due to the low number of conflicts – it is easier to modify the AD record for `andrew` manually. The conflicts file is checked once again because the Migration Wizard has produced the migration warning message (shown in figure 32). Figure 36 shows that the number of conflicts has increased.

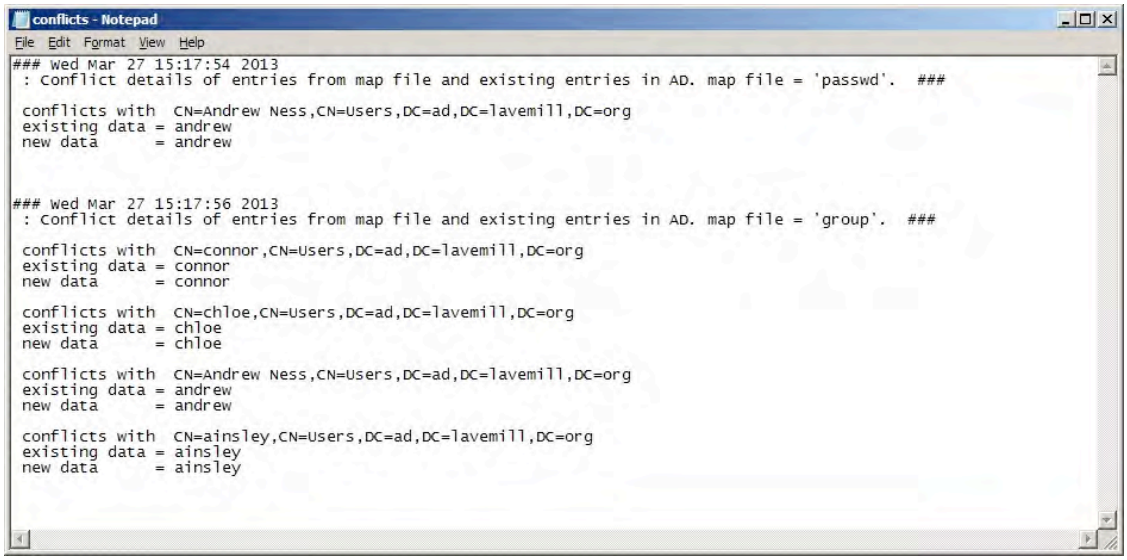

Figure 36. Lavemill migration conflicts log

Not surprisingly, the conflict log shows the same "`andrew`" conflict for the `passwd` map that displayed previously.

However, the `group` map migration now shows four conflicts instead of the one shown during the dry-run test.

These conflicts are due to the clash of namespaces for `group` and `passwd` maps. As the source was an Oracle Linux instance, a group named the same as the user name was created automatically. This conflicts because of the AD single namespace for security groups and users previously mentioned.

These conflicts did not arise during the dry-run test as the users had not existed when the `group` map merge dry-run was attempted, and the `passwd` map merge had also been a dry-run.

The resulting Active Directory changes are then reflected in the AD User and Computers console as shown in figure 37.

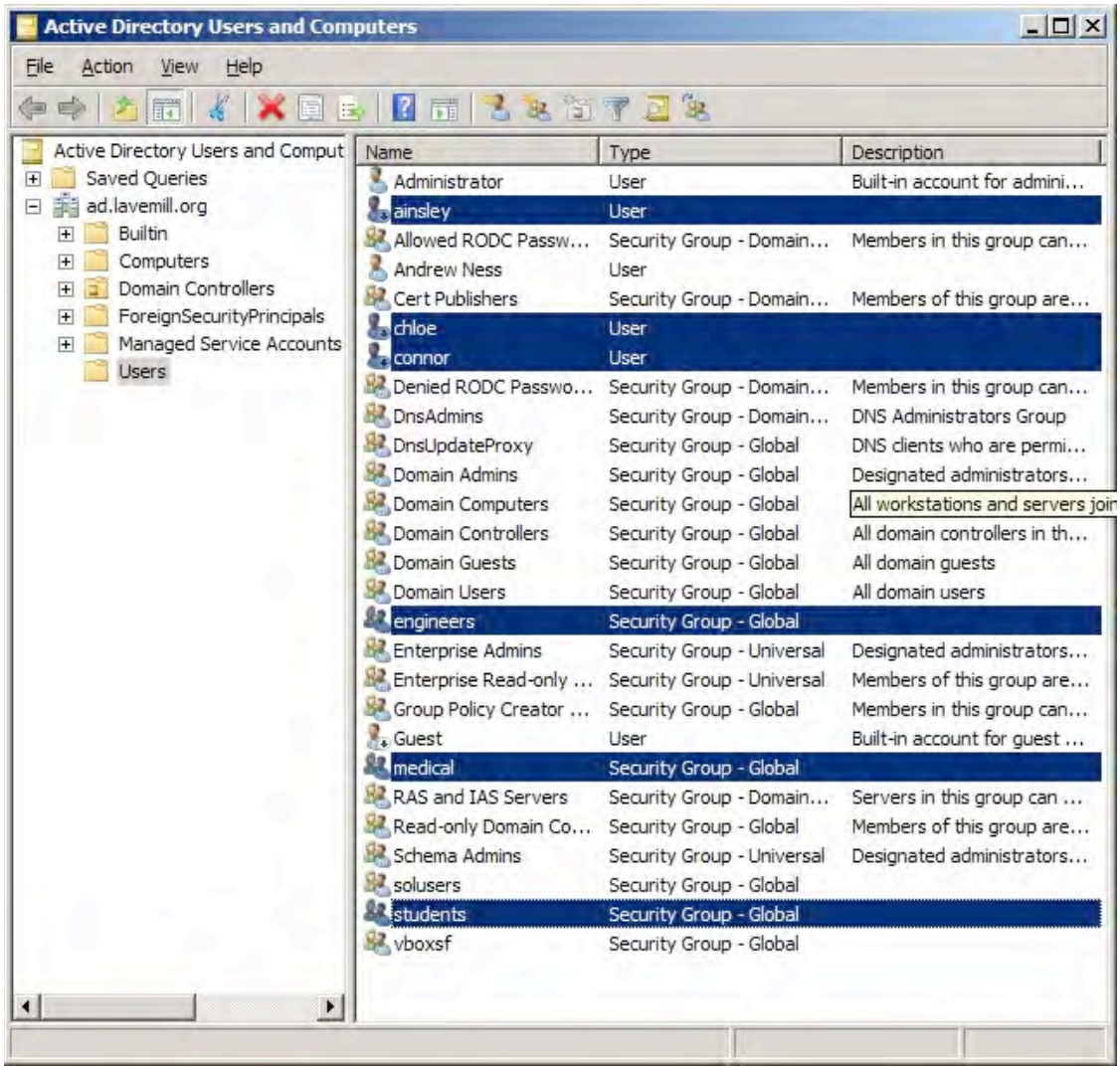

Figure 37. NIS Maps merged

All the newly created accounts are automatically disabled when created and must be enabled manually. This is done in the **Active Directory Users and Computers** console by selecting the **UNIX Attributes** panel as shown in figure 38. This is shown by the small down arrow icon in the bottom right of the user icon -

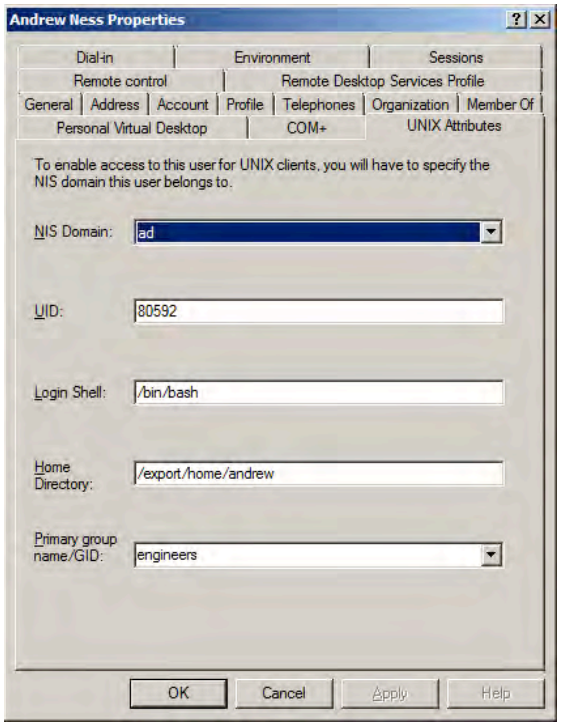

Figure 38. Active Directory user properties

Enabling Password Synchronization Between NIS and Active Directory

By default, password synchronization between NIS and AD is not enabled under Microsoft Identity Management for UNIX. To allow for a consolidated namespace, you must enable this feature using the following method:

1. Log on to the Windows Active Directory domain controller as a domain administration user and open the Server Manager if it does not automatically start.
2. Expand **Roles > Active Directory Domain Services > Microsoft Identity Management for UNIX** in the navigation panel on the left.
3. Right-click the Password Synchronization entry from the middle panel and select Properties.

   The Server Manager can be seen in figure 39.

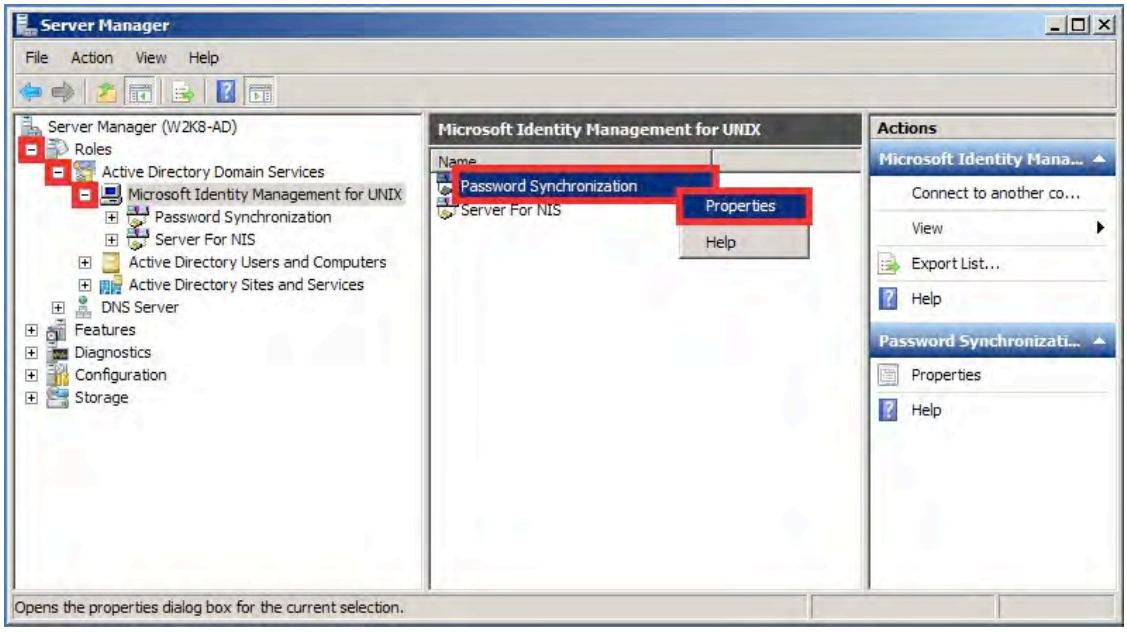

Figure 39. Selecting Password Synchronization and Properties in Server Manager

4. In the Password Synchronization Properties dialog, ensure both Windows to UNIX and UNIX to Windows entries are checked as shown in figure 40.

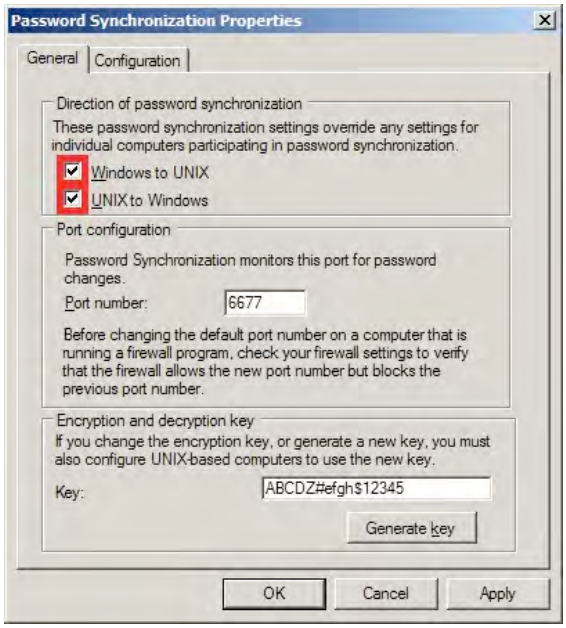

Figure 40. Password Synchronization Properties window

5. Click on the **Configuration** tab and ensure Windows to NIS (Active Directory) password synchronization is enabled as shown in the following figure.

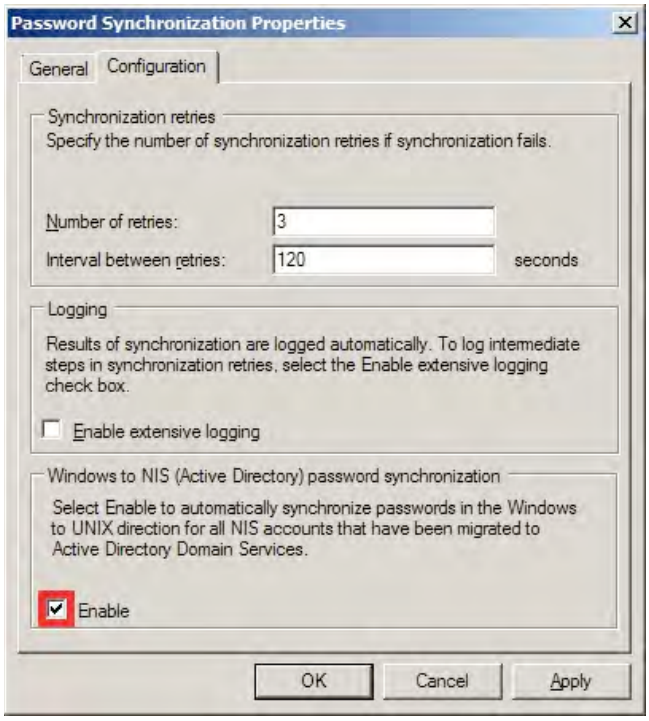

Figure 41. Enabling Windows to NIS synchronization

As soon as the synchronization is enabled, the dialog box shown in figure 42 is displayed, warning of domain controllers 'in the forest' that are running pre-Windows Server 2003 SP1. It is highly recommended that these domain controllers be identified as there are compatibility issues with earlier Active Directory DC configurations. Click **Yes** to allow the search.

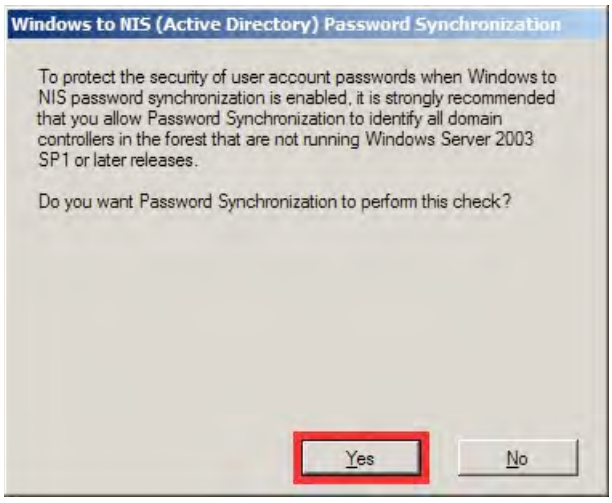

Figure 42. Enabling a pre-Windows 2003 SP1 domain controller search

Once the search to identify any servers running incompatible Windows operating systems is completed, the following message is shown. Should any incompatible domain controllers be identified, refer to the Microsoft web site for any resolution. Click **OK** to finish.

Figure 43. Compatibility check completed

Updating and Propagating NIS Maps

By default, the Windows Active Directory NIS server checks for updates to the NIS maps and, if necessary, propagates these changes to the other NIS servers. It is advisable to change the interval between these checks to match the expected volatility of the maps. The interval applies to all maps so the most volatile map – the map that requires the updates to be pushed to the other servers most frequently – should determine the interval value.

For instance, setting the update frequency at 1 hour would mean that any password update would take up to 1 hour to reach the other servers, which may be acceptable to any service level agreements in place.

Conversely, checking and updating the maps too frequently may cause an increased load on the Active Directory domain controllers, which could impact the performance of the Windows domain as a whole.

In practice, it is possible to force a map update to handle exceptional circumstances. In the example, the maps are small and not frequently updated, so 1 hour is acceptable.

To set the frequency, log on to the Windows Active Directory domain controller as a domain administrator and follow these steps:

1. Start the **Server Manager** and expand the Roles > Microsoft Identity Management for UNIX tree in the navigation panel.
2. Right click on the **Server for NIS** entry and select **Properties** as shown in figure 44.

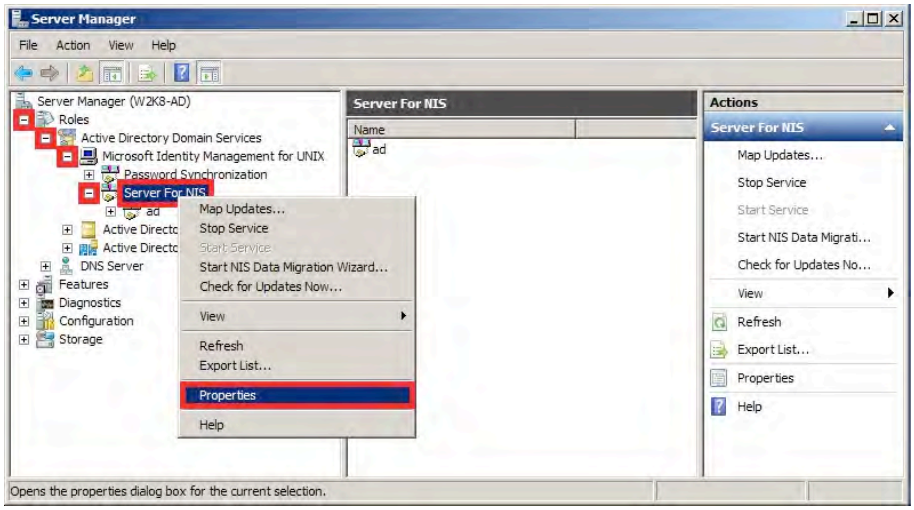

Figure 44. Selecting Server for NIS Properties

Enter the required frequency as Days, Hours and Minutes in the appropriate boxes, and click **OK** to finish.

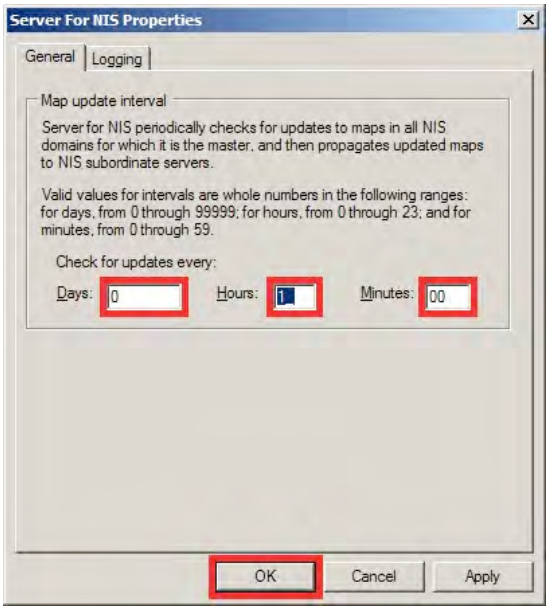

Figure 45. Setting propagation frequency for map updates in Server for NIS Properties window

Reconfiguring the NIS Servers

With the new NIS service in place, the now redundant NIS servers that originally served the authoritative NIS data can be made NIS slave servers of the Windows Server NIS

service. This allows for increased redundancy and minimal changes to the original NIS configuration.

The method for reconfiguring NIS servers depends on the operating environment of the NIS server. This section details how to reconfigure Oracle Linux and Oracle Solaris servers.

First, however, you need to register each subordinate NIS server with the Windows Server for NIS. To do this, use the following steps for each NIS server to be added:

1. Log on to the Windows Active Directory domain controller as a domain administrator user and start the **Server Manager**. Expand the **Roles > Microsoft Identity Management for UNIX > Server for NIS > *domainname* > NIS Servers** entry in the left navigation panel.

   Right-click on the NIS Servers entry and select '**Add NIS Server…**' as shown in figure 46.

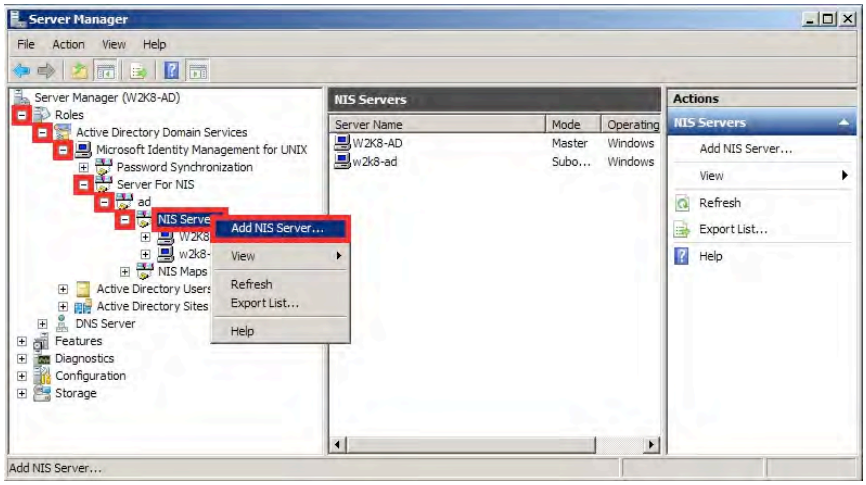

Figure 46. Adding the NIS server

2. Enter the name of the NIS server in the dialog box as shown in the following figure.

Figure 47. Providing the NIS server name

Click **OK** to complete the operation. The newly added NIS server should appear in the middle and navigation panes.

Reconfiguring Oracle Linux NIS Servers and Clients

The following commands are required on both Oracle Linux servers and clients when the AD domain name is different from the NIS domain name.

Log on to the Linux server in a terminal session and become root.

```
[andrew@oel-nissvr ~]$  su
Password: XXXXXXXXXXXX
[root@oel-nissvr ~]#  domainname ad
[root@oel-nissvr ~]#  vi /etc/yp.conf
/ change  domain nis.lavemill.org   server  192.168.1.92
/ to      domain ad                 server  192.168.1.81
[root@oel-nissvr ~]#  service ypbind restart
Shutting down NIS services:                                [  OK  ]
Turning on allow_ypbind SELinux boolean
Binding to the NIS domain:                                 [  OK  ]
Listening for an NIS domain server.ser.
[root@oel-nissvr ~]# service yppasswdd restart
Stopping YP passwd service:                                [  OK  ]
Starting YP passwd service:                                [  OK  ]
```

The following commands are only required on Oracle Linux NIS servers. It should be noted that Windows Services for UNIX NIS servers do not support `ypxfrd` (the high speed NIS map transfer utility).

```
[root@oel-nissvr ~]# service ypserv restart
Stopping YP server services:                               [  OK  ]
Starting YP server services:                               [  OK  ]
[root@oel-nissvr ~]# service ypxfrd restart
Stopping YP map server:                                    [  OK  ]
Starting YP map server:                                    [  OK  ]
[root@oel-nissvr ~]# ypwhich
w2k8-ad.lavemill.org
[root@oel-nissvr ~]# ypinit –s w2k8-ad
[… output deleted…]
```

The NIS servers will now present directory information from the Active Directory NIS implementation.

Reconfiguring Oracle Solaris NIS Servers and Clients

Log on to the NIS server or client as an administrative user:

```
admin@s11nisclient:~$ pfexec svccfg -s nis/domain
svc:/network/nis/domain> setprop config/domainname = ad
```

The next step specifies which NIS server to try when the NIS client starts. It is advisable to leave this at the original NIS server IP address(es) to avoid swamping the Windows Active Directory domain controller with NIS requests. In the following example, the originally assigned NIS server is the one specified.

```
svc:/network/nis/domain> setprop config/ypservers = 192.168.1.92
svc:/network/nis/domain> listprop config
config                      application
config/value_authorization astring     solaris.smf.value.name-
service.nis.domain
config/domainname          hostname    ad
config/ypservers           host        192.168.1.92
svc:/network/nis/domain> exit
admin@s11nisclient:~$ domainname
nis.lavemill.org
admin@s11nisclient:~$ pfexec svcadm refresh nis/domain
admin@s11nisclient:~$ domainname
ad
admin@s11nisclient:~$ exit
```

The now-redundant NIS servers can be repurposed as NIS slave servers by re-running the `ypinit` command.

```
admin@s11nissvr:~$ pfexec ypinit –s w2k12-ad
```

The NIS server will now be presenting the directory information from the Active Directory NIS implementation.

Configuring the Oracle ZFS Storage Appliance to Access NIS

The next step is to configure the Oracle ZFS Storage Appliance to access the new Windows-based NIS service. This step should also be taken if NIS is already configured and the new domain must be set.

1. Log on to the Oracle ZFS Storage Appliance BUI, as shown previously in figure 3, as an administrative user.

   Select **Configuration / Services / NIS** as shown in figure 48.

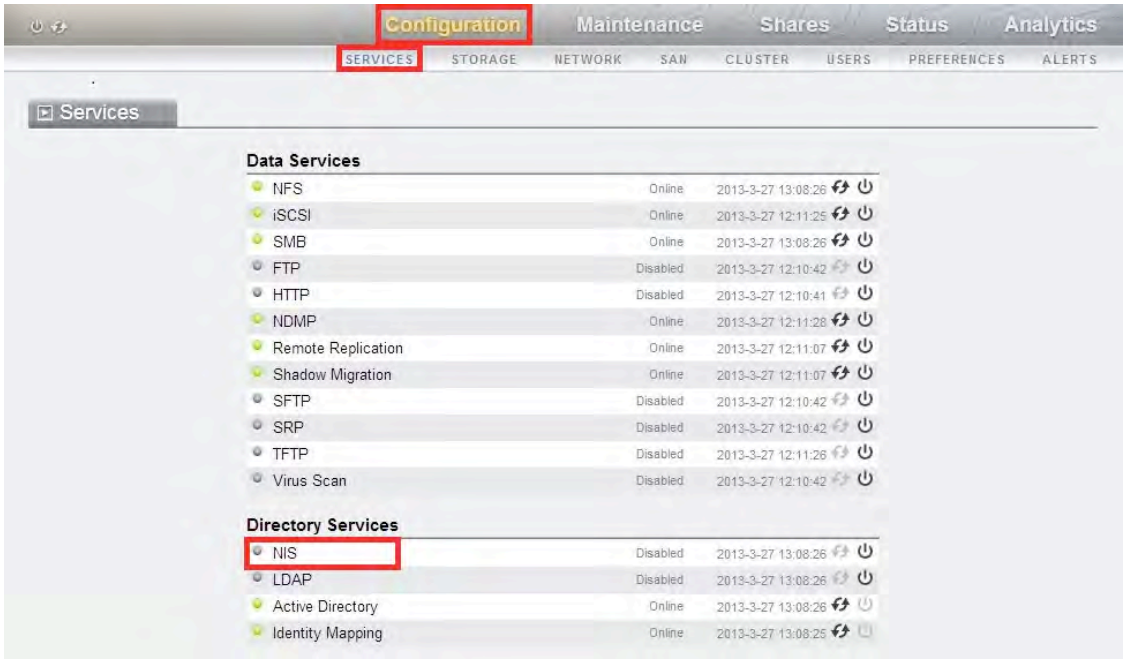

Figure 48. Configuration / Services / NIS in the Oracle ZFS Storage Appliance BUI

2. Enter the NIS **Domain** and select whether a server will be selected either explicitly or by broadcasting. Local administration policy should be the guide as to which option to choose.

   If explicit servers are to be defined, enter the IP address of each server in the bottom box. Add more servers to the list by clicking the ⊕ icon to the right of the server box. The example in figure 49 reflects the choice to broadcast for servers.

   Click **Apply** to continue.

Figure 49. NIS Domain and Server configuration

3. If the NIS service was disabled prior to executing these steps, the following warning and choices of action will be shown.

Figure 50. NIS Service warning

The Oracle ZFS Storage Appliance should now be able to access the NIS directory service.

Configuring the Oracle ZFS Storage Appliance IDMU Service

The Oracle ZFS Storage Appliance should now be able to access both Active Directory and NIS directory servers. Windows Server is now presenting consolidated data to both Active Directory and NIS.

In order to capture this mapping and to provide the consistent file and directory permissions necessary for the shares to be used concurrently by both Windows and Oracle Linux or Oracle Solaris environments, you must enable the IDMU service using the following steps:

1. Log on to Oracle ZFS Storage Appliance through the BUI as an administrative user. See figure 51 for an example.
2. Select **Configuration / Services / Identity Mapping**.

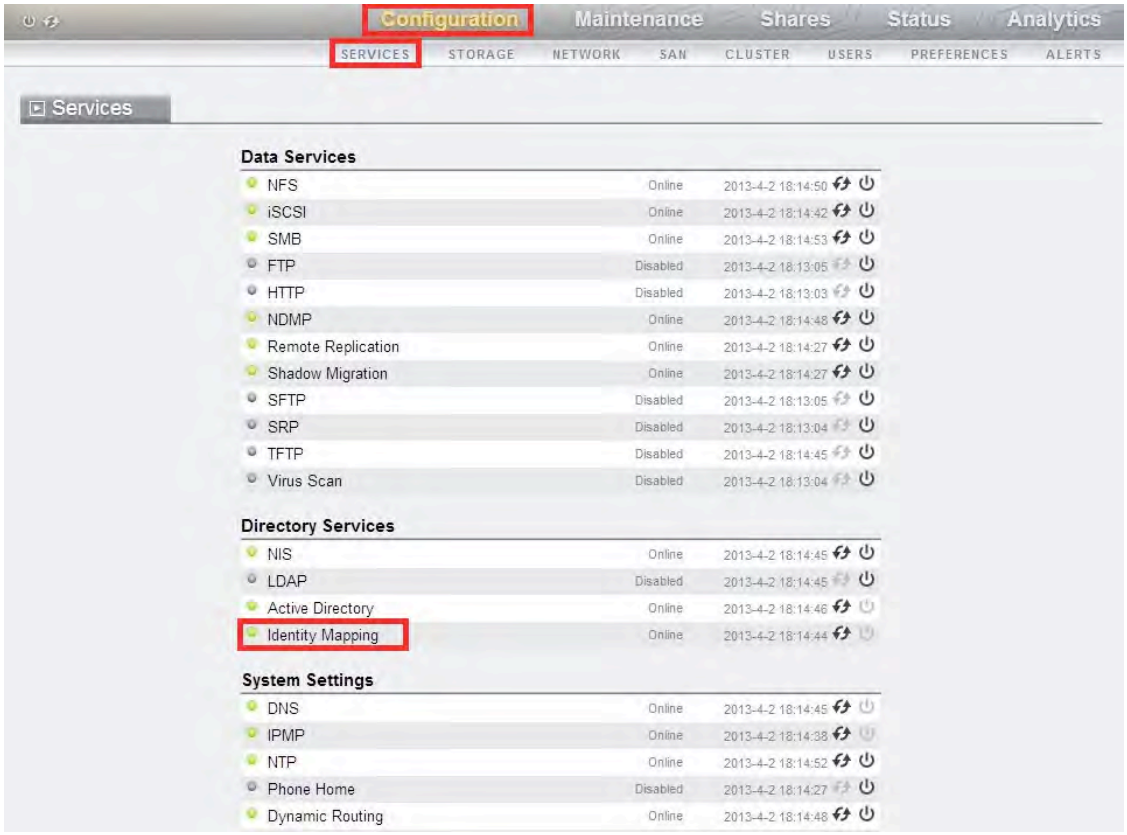

Figure 51. Navigating to Configuration / Services / Identity Mapping in the Oracle ZFS Storage Appliance BUI

3. Ensure that **Mapping mode** has the value **IDMU** selected as seen in figure 52.

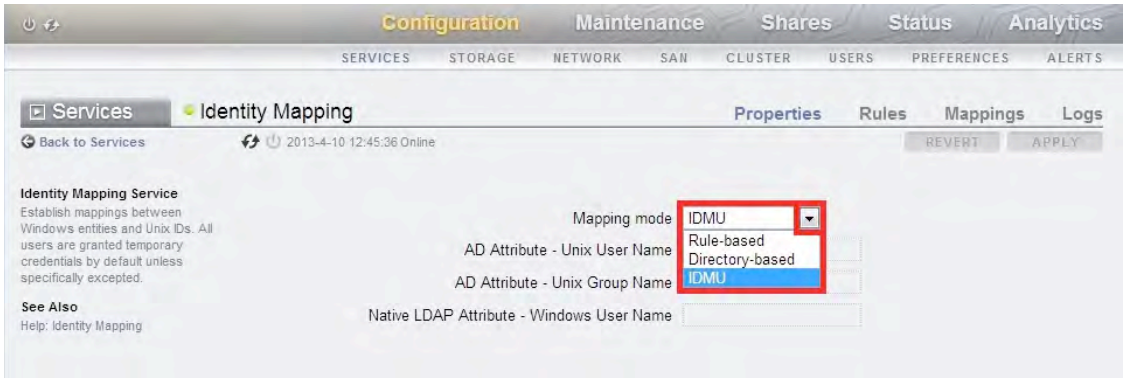

Figure 52. Selecting IDMU for Identity Mapping

Verifying Directory Service Operation

The final step in configuring IDMU is to verify that the consolidated directory service operates as expected. In order to do so, create a new user in Active Directory with the appropriate UNIX attributes set. Then create a share on the Oracle ZFS Storage Appliance and set restrictive permissions to allow only the owner to access any files or directories within the share.

The example will show testing in both Windows and Oracle Linux environments.

Creating the Active Directory User

To create the user in Active Directory, log on to a Windows server with a domain administrator account and follow these steps:

1. Open **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.

   Under Type, the User and Security Group view is shown by default. Click on the 'Add User' icon as shown in figure 53.

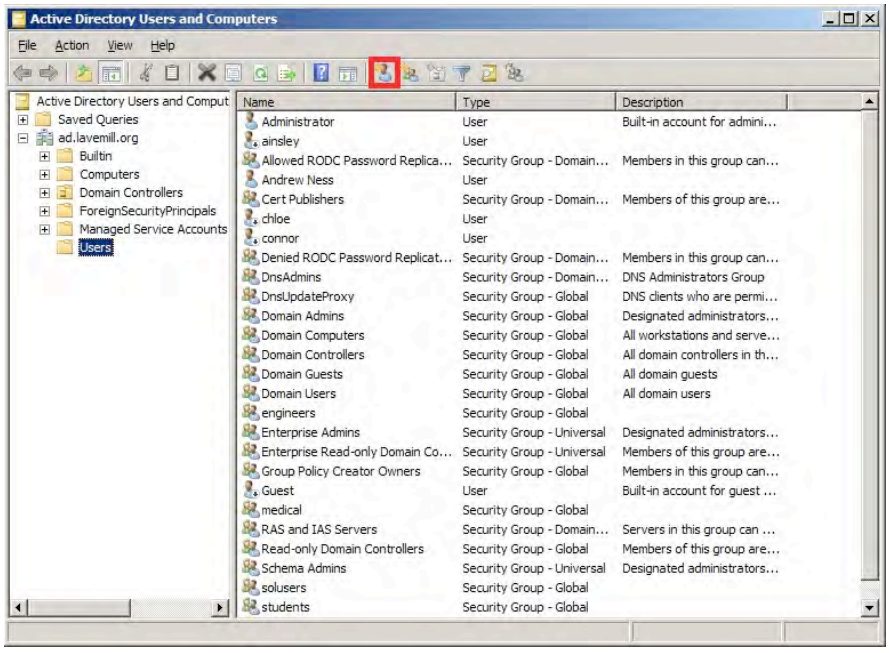

Figure 53. Windows Active Directory Users and Computers screen

2. Enter the appropriate details in the **New Object – User** dialog window as shown in the following figure and click **Next>** to continue.

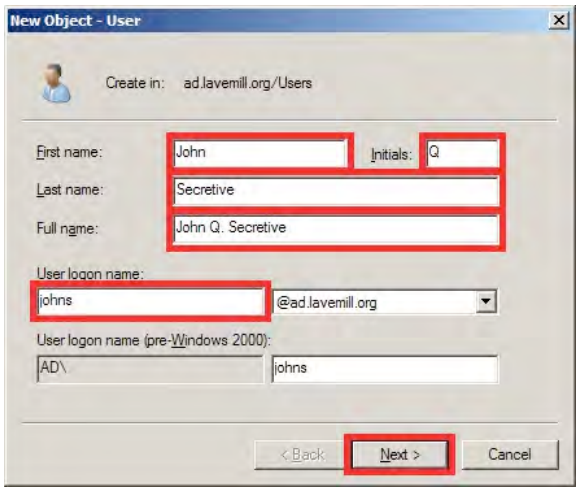

Figure 54. New Object - Username

3. Enter an appropriate password and re-enter in the **Confirm password:** field, then Click **Next>** to continue.

   NOTE: If the user will primarily be an Oracle Linux or Oracle Solaris user, you make sure that **User must change password at next logon** is deselected, since as there is no mechanism to force the password change on the Oracle Linux or Oracle Solaris environments.

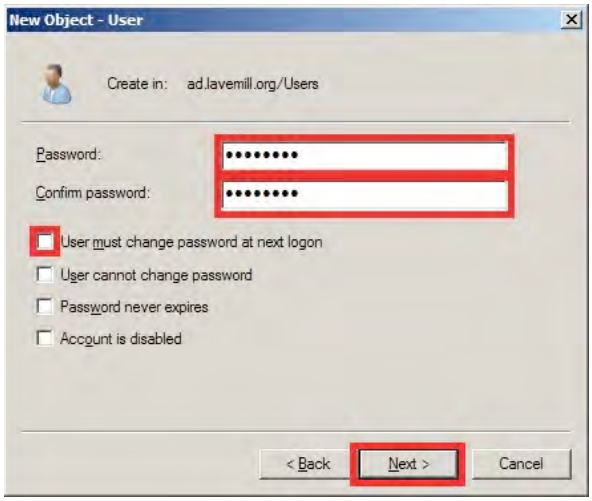

Figure 55. New Object - Password

4. A summary screen displays the requested operation's details. Click **Finish** to commit to the object's creation.

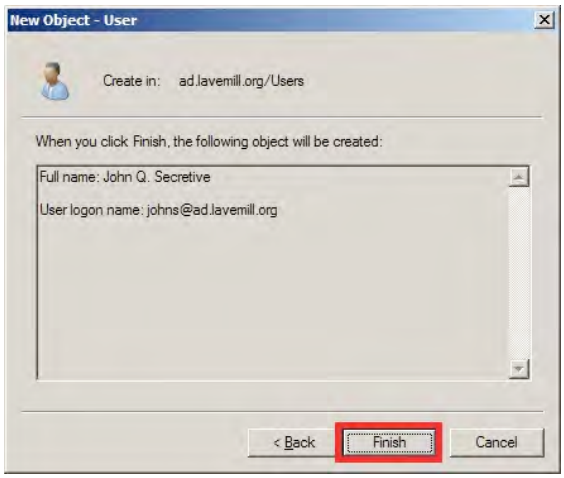

Figure 56. New Object - User Confirmation

5. The newly added user will then be displayed in the **Active Directory Users and Computers** screen.

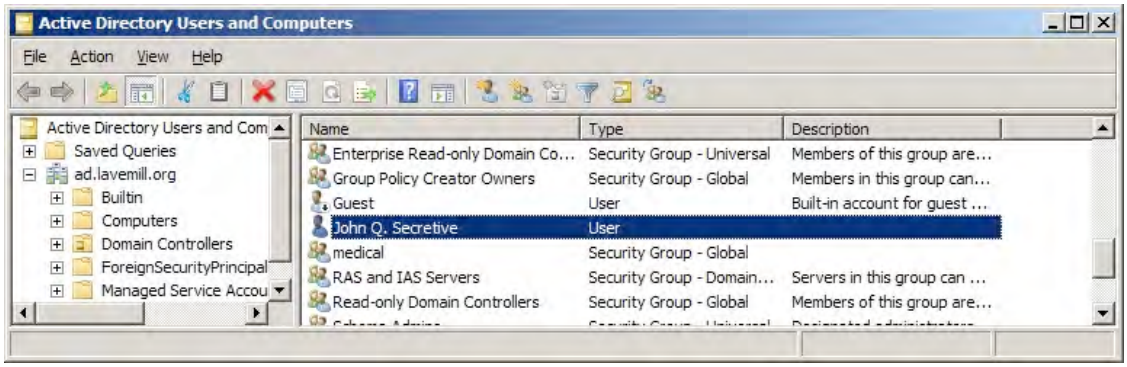

Figure 57. Newly added user shown in Active Directory

6. Double-clicking on the user name should bring up the properties for John Q. Secretive.

   Click on the **UNIX Attributes** tab and select the **NIS domain** from the drop-down menu box. When this has been selected, the **UID**, **Login shell**, **Home Directory** and default **Primary group name/GID** will be pre-filled. Check that these are suitable for your environment and, if not, modify as appropriate. The **UID** will be the last entered UID + 1. Click **Apply** to continue.

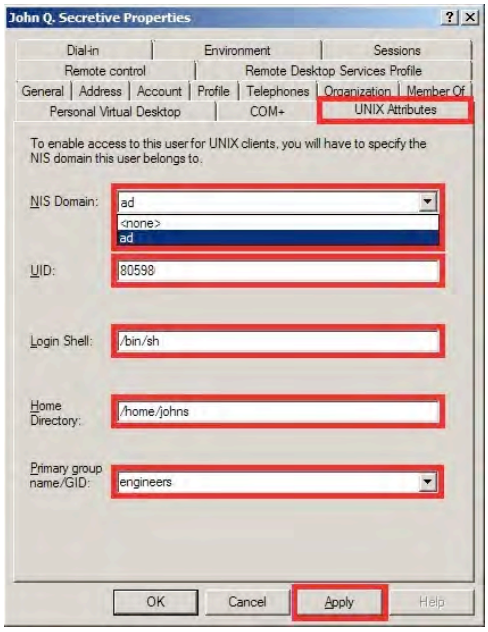

Figure 58. Auto-filled settings for UNIX Attributes

7. Depending on when the NIS map update propagation is due to happen, it may be necessary to force an update (for instance, if an urgent change is made that needs to be pushed out.

   Select **Start > All Programs > Microsoft Identity Management for UNIX > Microsoft Identity Management for UNIX**.

   Select **Server for NIS** from the left navigation panel with a right click and select **Check for Updates Now…** which will force a map update.

   Figure 59 highlights the screen navigation.

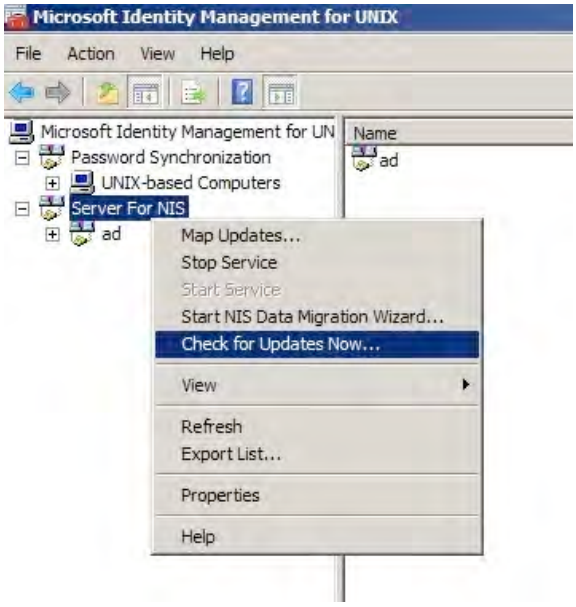

Figure 59. Forcing an NIS map update

When the map update has been initiated, the following dialog is displayed.

Figure 60. NIS map update initiated

The Event Viewer should be used to diagnose any problems. Refer to Microsoft Windows Server documentation for details regarding the Event Viewer.

Click **OK** to continue.

Conclusion

Enabling and configuring Identity Mapping for UNIX (IDMU) on the Oracle ZFS Storage Appliance and on Windows Server provides a simple, cost-effective way to provide a consolidated directory service for both Windows and UNIX-based environments. Furthermore, the Oracle ZFS Storage Appliance uses this information to provide a consistent view of permissions to shares that can be accessed concurrently by Windows and UNIX-based environments.

References	URL
"Microsoft Windows Server Best Practices for Server for NIS" Windows Server 2008R2 and Windows Server 2012	http://technet.microsoft.com/en-us/library/cc755243.aspx
Oracle ZFS Storage Appliance Documentation	http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html
Oracle ZFS Storage Appliance Product Pages	http://www.oracle.com/us/products/servers-storage/storage/nas/overview/index.html

How to Configure IDMU on the Oracle® ZFS Storage Appliance

October 2013, Version 1.1
Author: Andrew Ness

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together