

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
Overview of Required Configuration Tasks 4
Preconditions for setup5
Domain name conventions used for the example case5
Configuring the Oracle ZFS Storage Appliance to Access
Active Directory 6
Setting Up DNS Services
Setting up NTP Services
Joining the Active Directory Domain 10
Installing the IDMU Role Service on Windows Server
Active Directory
Exporting NIS Text Maps from the NIS Environment 17
Importing the NIS Text Maps to Services for UNIX 19
Migrating NIS Data to Active Directory Using the Migration
Wizard 19
Resolving Migration Conflicts – Using the Lavemill Example 28
Enabling Password Synchronization Between NIS and
Active Directory
Updating and Propagating NIS Maps
Reconfiguring the NIS Servers
Reconfiguring Oracle Linux NIS Servers and Clients
Reconfiguring Oracle Solaris NIS Servers and Clients
Configuring the Oracle ZFS Storage Appliance to Access NIS 39
Configuring the Oracle ZFS Storage Appliance IDMU Service 41

Verifying Directory Service Operation	43
Creating the Active Directory User	43
Conclusion	48
References	49
URL	49

#### **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.

4

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 <code>oel-NISsvr</code> and the slave server is named <code>oel-NISslv</code>.

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 <code>lavemill.org</code> – 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.

Sun Storage Appliance Login: zfssa	+		A.
https://zfssa:215			<b>宣</b>
♦ Sun		100000	
ORACLE		zfssa	6 A A
	Username		
	Password		
		LOGIN	

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.

<u>u</u> #			Configuration	Maintena			us An	alytics
						DASHBOARD	SETTING \$	NOM
Usage	E RAID10 Storage	CPU	1 %uti	100	NFSv3	0 ops/sec		
e	90.1G Used 2.40T Avail Compression: 1x Deduc: 1x	In Same	-	animal				
-		7d 24h	60 m		75 241	000		
	Memory 24.7G Cache 1.20G Unused	Network	1K bytes/sec	-#20K	NFSv4	Q ops/sec		**
0	a 33 fM Mgmt 376M Other 4 92G Kernel							
Consisor		74. 24m	60m		78 248	00m		
Services	A 1000	Disk	67 ops/sec	8628	SMB	0 ops/sec		
SMB HTTP	FTP  NOMP				311			
Replication	Shadow				1.			
G TETP	Antivirus	78 248	60m		78 244	80m		
@ NI5	W LEAP	111.000			122			
DNS	D Map     PMP	ISC SI	0 ops/sec	-30	Ind FIP	0 bytés/sec		:19
NTP	C Phone							
Dyn Routing	Taga Chuip							
© Syslog. SSH	<ul> <li>Syá ID</li> </ul>	7d 24h	00 <i>m</i>		7d 24h	-40		
Hardware	Up 184d 21 29	RECENT ALERTS						
CPU	University Nemory	2013-4-2 18:03:07	Finished replicating FCLUN Began replicating FCLUNR	REPTEST to appli FPTEST to appliant	ance ale-7210-2			
· Disks	Cards.	2013-4-2 17 03:07	Finished replicating FCLUN	REPTEST to appli	ance 'aie-7210-2'			
Fans	PSU	2013-4-2 17:03	Began replicating FCLUNR	EPTEST to appliar	nce 'aie-7210-2'			

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.

6.5	Con	Iguration	Maintenance	e Shai		Status	Analytics
	SERVICES	STORAGE	NETWORK SAN	CLUSTER	USERS	PREFERENCE	S ALLEI
E Services							
	Data Services						
	NFS		Online	2013-4-2 18:1	4:50 49 0		
	- ISCSI		Online	2013-4-2 18-1	4:42 49 山		
	SMB SMB		Online	2013-4-2 18-1	453 FJ ()		
	e FIB		Disabled	2013-4-2181	3105 D U		
	P HTTP		Devald/ed	2013-4-2 18:1	3:03 () ()		
	NDMP		Dange	2013-1-2 18:1	1.48 49 0		
	Remote Replication		Unine	2013-4.2 18 1	4.27 49 0		
	Shadow Migration		Umine	2012-0-2 18:1	4.27 好 ()		
	9 SFTP		Deatled	2013-4-2-18-1	3.05 F# 😃		
	W SRP		Devided	2013-4-210,1	2:04 0 也		
	@ TFTP		Disabled	2013-4-2 18:1	4:45 F. U		
	Virus Scan		Disasted	2013-4-2 18-1	0.04 € U		
	Directory Services						
	NIS		Online	2013-4-2 18:1	4:45 49 0		
	C LDAP		Disabled	2013-4-2 18:1	4:45 C U		
	Active Directory		Ontrie	2013-4-2 18:1	4:46 42 1		
	<ul> <li>Identity Mapping</li> </ul>		Ohine	2012.4.2 18	a 44 69 (1)		
	System Settings						
	O DNS		Drine	2013-4-2101	1:45 63 ()		
	· IPMP		Online	2013-4-2 10/1	4:30 69 1		
	NTP		Dinting	2013-4-2 18:1	4:52 49 0		
	in Direct Henry		Whenterd	THE OWNER WATER	and the dis		

Figure 5. Selecting DNS settings in the BUI

8

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.

0.10	Conf	iguration	Mainte	nance	Shar	es	Status Ar	nalytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCES	ALERTS
🗉 Services 🔍 🔍 DN	NS						Properties	Logs
G Back to Services	🚯 🕛 2013-4-3 10:15:30 Online						REVERT	APPLY
Domain Name Service DNS is used to map host names such as oracle com to their corresponding IP addresses. DNS is always enabled on your appliance, and can be configured manually or based on your current DHCP settings. In addition, you may elect to attempt hostname resolution using other directory services (if configured).		Allow IPv4 Allow IPv6	DNS Do DNS Sen I non-DNS resol 6 non-DNS resol	main lave ver(s) 🟵 o ution 📄 ution 📄	mill.org 192.168.1.6 192.168.1.6	5	3	
See Also Help: DNS Wikipedia: DNS								



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.

9

)er	Conngalation	maintenance	endles	Analyti
	SERVICES STORAGE	NETWORK SAN	CLUSTER USERS	PREFERENCES ALER
Services				
	Data Services			
	NFS	Online	2013-4-2 18:22:22 🔂 🛈	
	iSCSI	Online	2013-4-2 18:14:42 5 0	
	SMB	Online	2013-4-2 18:14:53 🔂 🛈	
	· FTP	Disabled	2013-4-2 18:13:05 🕩 😃	
	• HTTP	Disabled	2013-4-2 18:13:03 🕫 😃	
	NDMP	Online	2013-4-2 18:14:48 🗲 🔱	
	Remote Replication	Online	2013-4-2 18:14:27 🗲 🕛	
	Shadow Migration	Online	2013-4-2 18:14:27 🗲 🙂	
	SFTP	Disabled	2013-4-2 18:13:05 🖅 😃	
	• SRP	Disabled	2013-4-2 18:13:04 🕬 😃	
	TFTP	Disabled	2013-4-2 18:14:45 🕩 😃	
	Virus Scan	Disabled	2013-4-2 18:13:04 🥬 😃	
	Directory Services			
	NIS	Online	2013-4-2 18:22:22 🔂 🛈	
	C LDAP	Disabled	2013-4-2 18:22:22 🕬 😃	
	Active Directory	Online	2013-4-2 18:14:46 🗲 🛈	
	Identity Mapping	Online	2013-4-2 18:14:44 🗲 🕛	
	System Settings			
	DNS	Online	2013-4-2 18:22:22 🔂 🕛	
	IPMP	Online	2013-4-2 18:14:38 🔂 🕖	
	© NTP	Online	2013-4-2 18:14:52 59 0	

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.

0 \$	Cont	iguration	Mainte	enance	Shai	res	Status	Anal	ytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	ÜSERS	PREFERENC	CES A	LERTS
🗈 Services 🔷 NT	Р						Prope	rties	Logs
G Back to Services	€ U 2013-4-2 19:43:00 Online	2					REVERT	API	PLY
Network Time Protocol Configure the network time	NTP Settings			Clo	ck				
protocol. If you choose to leave the NTP service disabled, you may manually set the time and data to	Discover NTP server via r	nulticast addres	IS:			Server Time	2013-4-3 09:35:5	58	
match your time according to your web browser.	Manually specify NTP se	rver(s):				Client Time	2013-4-3 09:35:4	SY	WC.
See Also Help: NTP	SERVER	AUTH KEY	-						
NTP Project Wikipedia: NTP	192.168.1.5	<none></none>							
			-						
	CNTP Authentication I	Keys		_					
	No NTP authentication Click the O button abo	keys have beer ve to add authe	n established ntication keys.						

Figure 8. Providing NTP configuration details

- 3. [Optional] Enter any appropriate NTP authentication keys by clicking the 😳 icon next to the key definitions.
- 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 <sup>O</sup> 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.

0 2	Configuration	Maintenance	Shares	Status	Analytics
IS	SERVICES STORAGE	NETWORK SAN	CLUSTER USERS	PREFERENCES	ALERTS
Services					
Data Service	s				
NFS		Onliné	2013-4-2 19:43:01 🗲 🙂		
iscsi		Online	2013-4-2 19:41:29 🗲 🔱		
SMB		Online	2013-4-2 19:43:03 🗲 🕛		
© FTP		Disabled	2013-4-2 19:40:48 🐨 😃		
♥ HTTP		Disabled	2013-4-2 19:40:47 🔂 😃		
NDMP		Online	2013-4-2 19:42:53 🗲 🙂		
🔍 🌳 Remote Rep	plication	Online	2013-4-2 19:41:08 🗲 🙂		
Shadow Mig	gration	Online	2013-4-2 19:41:08 🗲 🔱		
SFTP		Disabled	2013-4-2 19:40:48 🕬 😃		
© SRP		Disabled	2013-4-2 19:40:48 🗇 😃		
TFTP		Disabled	2013-4-2 19:42:53 🔂 😃		
Virus Scan		Disabled	2013-4-2 19:40:47 👘 😃		
Directory Ser	rvices				
NIS		Online	2013-4-2 19:42:53 🗲 🙂	1	
© LDAP		Disabled	2013-4-2 19:42:53 🔂 😃		
Active Direction	tory	Online	2013-4-2 19:42:58 🚯 🔱		
Identity Map	pping	Online	2013-4-2 19:41:31 🗲 🖑		

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

2. Click	JOIN DOMAI	N as si	nown in	i figu	re 10.			
<u>U</u> #	Com	iguration	Mainte	nance	Shar	es	Status Ar	nalytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCES	ALERTS
E Services • Ad	ctive Directory						Status	Logs
G Back to Services	砂 (Ú) 2013-4-3 10:10:32 Disabl	ed						
Active Directory Name Service Configure communication with a Microsoft Active Directory Server. Active Directory servers authenticate Windows users and share files over the SMB protocol	Mode: Workgroup Workgroup: Lavemill JOIN DOMAIN JOIN WO	RKGROUP						
See Also Help: Active Directory Microsoft Active Directory Technology Center Wikipedia: Active Directory								

. . **c**. 4.0

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.

Join Domain	CANCEL	APPLY
To join a domain, enter the Active Directory do the administrative password below.	omain, an administrative user	s name, and
Active Directory Domain:	ad.lavemill.org	
Administrative User:	andrew	
Administrative Password:		
Additional DNS Search Path:		

Figure 11. Join Domain window

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

0 \$		Cioni	iguration	Mainte	enance	Shar	es	Status A	nalytics
		SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCES	ALERTS
Services	Active Di	rectory						Status	Logs
G Back to Services	69 ()	2013-4-3 10:49:49 Online							
Active Directory Name	Service	-							
Microsoft Active Director	Server, Doma	Domain in: ad lavemill org							
authenticate Windows us	ers and Select	ed Domain Controller	w2k8-ad.ad.lav	vemill.org (192.1	168.1.81)				
See Also	JOIN	DOMAIN JOIN WO	RKGROUP						
Help: Active Directory									
Microsoft Active Directory Technology Center	1								
Wikipedia: Active Director	V.								

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.

et a real and				
File Action Alex Helb				
Þ 🗢 🖄 📅 🚹				
Server Manager (W2K8-AD)	Active Directory Domain Services			
Active Directory Domain Se	Stores directory data and manages comm	unication between users and domains, including user logon proce	esses, authentication, and directory searches.	2
me Diagnostics     Monopuration     Storage	Role Services: 1 installed		Add Role Services	-
	Role Service	Status	Remove Role Services	
	Active Directory Domain Controller	Installed		
	Identity Management for UNIX	Not installed		
	Server for Network Information Services	Not installed		
	Password Synchronization	Not installed		
	Administration Tools	Not installed		
	Description: <u>Active Directory Domain Controller</u> enables a ser between users and domains, including user logo	rver to store directory data and manages communication n processes, authentication, and directory searches.		
	Advanced Toole			-

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

 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.

ole Services onfirmation	Select the role services to install for Active Directory Domain Servic Role services:	es: Description:
Progress Results	✓       Active Directory Domain Controller (Installed)         ✓       ✓         ✓       Benetic Management for UNIX         ✓       Service for Network Information Services         ✓       Password Synchronization         ✓       Administration Tools	Identiv Masagement for UNX integrates computers running Windows into an existing UNIX environment.
	More about role services	

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.

Add Role Services		×
Confirm Ins	stallation Selections	
Role Services Confirmation Progress Results	To install the following roles, role services, or features, dick Install. <ul> <li></li></ul>	
	Print, e-mail, or save this information           < Previous         Install	Cancel

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.

Add Role Services	Results	×
Role Services Confirmation	One or more of the following roles, role services, or features require you to restart: $\hat{\bf \Omega}$ 1 warning message below	
Results	Active Directory Domain Services	
	Print, e-mail, or save the installation report	
	< Brevious Tylext > Close Ganc	리

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.

Add Rol	e Services
0	Do you want to restart now?
	This server must be restarted to finish the installation process. You cannot add or remove other roles, role services, or features until the server is restarted.
	Yes No

Figure 18. Permission to reboot

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

Resume Configuration Wizard		<u>×</u>
Installation Re	esults	
Resuming Configuration Progress	The following roles, role services, or features were	e installed successfully:
Results	Active Directory Domain Services	Installation succeeded
	The following role services were installed: Identity Hanagement for UHIX Server for Network Information Services Password Synchronization Administration Tools	
	Print, e-mail, or save the installation report	
	< <u>B</u> re	vigus Hext Cligse Cancel

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.

Role Services: 5 installed		Add Role Services
ole Service	Status	Remove Role Services
Active Directory Domain Controller	Installed	
Judentity Management for UNIX	Installed	
Server for Network Information Services	Installed	
Password Synchronization	Installed	
Administration Tools	Installed	

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.

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

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.

Microsoft Identity Management fo	r UNIX			_ 🗆 ×
<u>File Action View H</u> elp				
(+ +) 🖄 🖬 🔒 🖬 🖬				
🛄 Microsoft Identity Management for UN	Name		Actions	
Password Synchronization     Server For NIS	ad ad		Server For NIS	-
E ad			Map Updates	
			Stop Service	
			Start Service	
			Start NIS Data Migration Wiz	ard
			Check for Updates Now	_
			View	•
			Refresh	
			Export List	
			Properties	
			Help	
			The second second	

Figure 22. Microsoft Identity Management for UNIX console

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

NIS Data Migration Wizard	And and a second se	×
Before Yo	u Begin	
Before You Begin Specify NIS Source Domain Administrator Authentication NIS Map Selection NIS Map Source Files Destination Domain Manage Migration Conflicts Test Migration and Logging Completing the NIS Data Migration Log Migration Log Migration Completed	Welcome to the Network Information Service (NIS) Data Migration Wizard. This wizard helps you migrate NIS map data from an NIS server running a UNIX-based operating system to a Windows-based Active Directory domain controller running Server for NIS. To migrate NIS maps, you must have access to UNIX-based NIS map source files. To continue, click Next. <u>Previous</u> <u>Next&gt;</u> Finish	Cancel

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.

NIS Data Migration Wizard	and the second design of the s	×
Specify NI	S Source Domain	
Before You Begin Specify NIS Source Domain Administrator Authentication NIS Map Selection NIS Map Source Files Destination Domain Manage Migration Conflicts Test Migration and Logging Completing the NIS Data Migration Wizard	To migrate NIS maps from a UNIX-based NIS domain to a Windows-based Active Directory domain controller, provide the name of the UNIX-based NIS domain that is the source of the map data. Type the name of the UNIX-based NIS source domain. NIS source gomain name:	
Migration Completed	< <u>Previous</u> Prriish Cancel	

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.

NIS Data Migration Wizard	X
Administra	tor Authentication
Before You Begin Specify NIS Source Domain Administrator Authentication	To migrate map data to Server for NIS, you must log on as an Active Directory Domain Services Administrator:
NIS Map Selection NIS Map Source Files Destination Domain Manage Migration Conflicts Test Migration and Logging Completing the NIS Data Migration Wizard Migration Log Migration Completed	Specify how you want to log on:         I am logged on as an administrator         I want to log on as the following uger:         Liser name (domain\user name):         Password:
	< <u>P</u> revious <u>N</u> ext> Finish Cancel

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.

NIS Data Migration Wizard			×
NIS Map S	election		
Before You Begin Specify NIS Source Domain Administrator Authentication NIS Map Selection NIS Map Source Files Destination Domain Manana Ministration Conflicts	You can migrate the NIS maps using n To migrate a map, select a map in the map, select a map in the Maps to migr non-standard NIS map to migrate, click and click Edit/View	tap source files. Available NIS maps list, and then click Ad ate list, and then click Remove. To create k New. To view or edit a non-standard ma	ld. To remove a a new p, select the map
Test Migration and Logging Completing the NIS Data Migration Wizard Migration Log Migration Completed	Available NIS maps: netid netmasks passwd protocols protocols protocols services shadow ypservers	Add >         group           < Bemove	ate:
	< <u>Pr</u>	evious <u>N</u> ext> Finish	Cancel

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:.

NIS Data Migration Wizard		×
📕 NIS Map S	ource Files	
Before You Begin Specify NIS Source Domain Administrator Authentication NIS Map Selection	You can migrate the NIS maps using map source files. Provide the location of the UNIX-based NIS map source files. You can either copy the files to a local directory or enter the path name if the files are stored elsewhere on the network.	
NIS Map Source Files		
Destination Domain	and the second	
Manage Migration Conflicts	NIS map source files location: e:\	
Test Migration and Logging		
Completing the NIS Data Migration Wizard		
Migration Log		
Migration Completed		
	< <u>P</u> revious <u>N</u> ext> Finish Cance	8

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.

NIS Data Migration Wizard	
Destination	Domain
Before You Begin Specify NIS Source Domain Administrator Authentication NIS Map Selection	The destination domain is the NIS domain in AD DS to which maps are migrated. You can migrate maps into a new domain or merge maps into a previously migrated NIS domain:
Destination Domain	Migrate into an existing domain:
Manage Migration Conflicts	C Migrate into a new domain:
Completing the NIS Data Migration Wizard Migration Log Migration Completed	Container name Enter the name of an Active Directory Domain Services container for migration. To use the default container, click Next. AD DS container name:
	< Previous Next> Finish Cancel

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.

NIS Data Migration Wizard	×
Test Migra	tion and Logging
Before You Begin Specify NIS Source Domain	To perform a test of NIS data migration, without actually migrating data, select Do not migrate (log only).
Administrator Authentication NIS Map Selection	To perform an actual migration, and log all migration steps and conflicts, select Migrate and log.
NIS Map Source Files Destination Domain Manage Migration Conflicts	Do not migrate (og only)
Test Migration and Logging	
Completing the NIS Data Migration Wizard	Migration log file name:
Migration Log	C:\Windows\IDMU\nis\nis2ad.k Browse
Migration Completed	
	< Previous Next> Finish Cancel

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.

IS Data Migration Wizard			>
Completing	g the NIS Data Migration	Wizard	
Before You Begin Specify NIS Source Domain	Verify the migration settings that you ha	ave selected.	
Administrator Authentication	Your current selection:	and the second sec	
NIS Map Selection	<u>U</u> sername :		
NIS Map Source Files	<u>N</u> IS source domain :	nis.lavemill.org	
Destination Domain	Destination NIS domain :	ad	
Manage Migration Conflicts	Active Directory container name:		
Test Migration and Logging	NIS map source files location:	e:\	
Completing the NIS Data	NIS map selection:	passwd.group	
Migration Wizard	Log only or actual migration:	Trial	
Migration Log	Manage migration conflicts:	Preserve	
Migration Completed	Log file :	C:\Windows\IDMU\nis\nis.	
	Conflicts <u>fi</u> le :	C:\Windows\IDMU\nis\cor	
	To begin data migration, click Next.		
	< <u>P</u> n	evious <u>N</u> ext> Pinish	Cancel

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.

NIS Data Migration Wizard	No. of Concession, Name				×
Migration	Log				
Before You Begin Specify NIS Source Domain Administrator Authentication NIS Map Selection NIS Map Source Files Destination Domain Manage Migration Conflicts Test Migration and Logging Completing the NIS Data Migration Wizard Migration Log Migration Completed	Migration log complei clicking on Next Log file: Conflicts file:	ted . You have selected to C:\Windows\IDMU\nis\ [Ves\IDMU\nis\conflicts.]	o log only. If you wish, y ni	ou could migrate by	y Ones

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.

Active Directory Users and Comput	Name	Type	Description
Saved Queries	Administrator	User	Built-in account for admini
🟥 ad.lavemill.org	Allowed RODC Password Replica	Security Group - Domain	Members in this group can
🕀 🧾 Builtin	🔏 Andrew Ness	User	
Computers	Cert Publishers	Security Group - Domain	Members of this group are
Domain Controllers	RODC Password Replicat	Security Group - Domain	Members in this group can
ForeignSecurityPrincipals	A DnsAdmins	Security Group - Domain	DNS Administrators Group
Managed Service Accounts	A DnsUpdateProxy	Security Group - Global	DNS clients who are permi
OSETS	R Domain Admins	Security Group - Global	Designated administrators
	R Domain Computers	Security Group - Global	All workstations and serve
	R Domain Controllers	Security Group - Global	All domain controllers in th
	😣 Domain Guests	Security Group - Global	All domain guests
	🙈 Domain Users	Security Group - Global	All domain users
	Admins	Security Group - Universal	Designated administrators
	🗟 Enterprise Read-only Domain Co	Security Group - Universal	Members of this group are
	Sroup Policy Creator Owners	Security Group - Global	Members in this group can
	🚴 Guest	User	Built-in account for guest
	RAS and IAS Servers	Security Group - Domain	Servers in this group can
	Read-only Domain Controllers	Security Group - Global	Members of this group are
	😣 Schema Admins	Security Group - Universal	Designated administrators
	St colucere	Security Group - Global	

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.

Active Directory Users and Com	puters		
File Action View Help			
🔄 🔿   🚈 📅 🖌 🕌 🖬	s   🛛 🖬 🔧 🐮 🛅	7 2 %	
Active Directory Users and Comput	Name	Туре	Description
🗉 🧾 Saved Queries	Administrator	User	Built-in account for admini
🖃 🏥 ad.lavemill.org	ainsley	User	and the second se
🕀 🔛 Builtin	Allowed RODC Passw	Security Group - Domain	Members in this group can
<ul> <li></li></ul>	🚴 Andrew Ness	User	
	🗟 Cert Publishers	Security Group - Domain	Members of this group are
	achioe -	User	
Managed Service Accounts	Connor	User	
Users	Rode Rode Passwo	Security Group - Domain	Members in this group can
	A DrisAdmins	Security Group - Domain	DNS Administrators Group
	& DnsUpdateProxy	Security Group - Global	DNS clients who are permi
	Somain Admins	Security Group - Global	Designated administrators
	Reputers	Security Group - Global	All workstations and servers
	& Domain Controllers	Security Group - Global	All domain controllers in th
	A Domain Guests	Security Group - Global	All domain guests
	Somain Users	Security Group - Global	All domain users
	angineers .	Security Group - Global	
	Renterprise Admins	Security Group - Universal	Designated administrators
	😹 Enterprise Read-only	Security Group - Universal	Members of this group are
	Sroup Policy Creator	Security Group - Global	Members in this group can
	🖁 Guest	User	Built-in account for guest
	amedical .	Security Group - Global	
	RAS and IAS Servers	Security Group - Domain	Servers in this group can
	Read-only Domain Co	Security Group - Global	Members of this group are
	Schema Admins	Security Group - Universal	Designated administrators
	Solusers	Security Group - Global	
	& students	Security Group - Global	
	& vboxsf	Security Group - Global	
	and the second s		
		1	

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 -

drew Ness Pr	operties	?
Dial-in Remote General   Addre Personal V	Environment   control   Remote Deskto ess   Account   Profile   Telephones   ( irtual Desktop   COM+	Sessions p Services Profile Organization   Member Of UNIX Attributes
To enable acc NIS domain th	ess to this user for UNIX clients, you will h is user belongs to.	nave to specify the
<u>N</u> IS Domain:	ad	
<u>u</u> id:	80592	
Login Shell:	/bin/bash	
<u>H</u> ome Directory:	/export/home/andrew	
Primary group name/GID:	engineers	<b>•</b>
	OK Cancel	Apply Help

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.

eneral Configuration	1
Direction of passwo	ord synchronization
These password syr individual computers	nchronization settings override any settings for s participating in password synchronization.
Windows to U	INIX
UNIX to Wind	ows
Port configuration	
Password Synchro changes.	onization monitors this port for password
Port number:	6677
Before changing the running a firewall p that the firewall allo previous port num	he default port number on a computer that is program, check your firewall settings to verify pows the new port number but blocks the per.
Encryption and dec	ryption key
If you change the e also configure UNIX	ncryption key, or generate a new key, you must {-based computers to use the new key.
Key:	ABCDZ#efgh\$12345
	Generate <u>k</u> ey

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.

Synchronization retries Specify the number of sync	hronization retries if s	ynchronization fails.
Number of retries:	3	
Interval between <u>r</u> etries:	120	seconds
Results of synchronization steps in synchronization ref check box.	are logged automatic: ries, select the Enable	ally. To log intermediate e extensive logging
Results of synchronization steps in synchronization ref check box.	are logged automatic: ries, select the Enable ng rectory) password syr	ally. To log intermediate e extensive logging
Results of synchronization steps in synchronization ref check box. Enable extensive loggir Windows to NIS (Active D Select Enable to automati to UNIX direction for all N Active Directory Domain S	are logged automatic: rise, select the Enable ng rectory) password syn cally synchronize pas: S accounts that have jervices.	ally. To log intermediate e extensive logging inchronization swords in the Windows e been migrated to

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.

Vindows to NIS (Active Dir	ectory) Password Synchronizat	ion
To protect the security of use NIS password synchronizatio that you allow Password Syn controllers in the forest that a SP1 or later releases.	er account passwords when Windows in is enabled, it is strongly recommend chronization to identify all domain are not running Windows Server 2003	s to led
Do you want Password Sync	hronization to perform this check?	
	Yes No	

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.
- Right click on the Server for NIS entry and select Properties as shown in figure 44.

File Action View Help			
🔄 🔿 🖄 📅 🗟 👔			
Server Manager (W2K3-AD)  Roles  Active Directory Domain Services  Active Directory Domain Services  Microsoft Identity Management for UNIX  Comparison  Server For VIS  (Comparison  (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Comparison (Compari		Server For NIS	Actions
		Name	Server For NIS
		Gal ad	Map Updates Stop Service Start Service
Active Directo Stop Service     Active Directo Start Service     Dis Server Start NIS Data Migrat     Dis Server Check for Updates No	Stop Service Start Service Start NIS Data Migration Check for Updates Now	Wizard	Start NIS Data Migrati Check for Updates No View
m Diagnostics     Configuration	View	•	Refresh
🗉 🚰 Storage	Refresh		Export List
	Export List		Properties
	Properties		Help
	Help		The second se

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.

and the second of			
Map update interv			
Server for NIS peri domains for which to NIS subordinate	odically checks for update it is the master, and then p servers.	es to maps in all NIS propagates updated i	naps
Valid values for int for days, from 0 thr minutes, from 0 thr	ervals are whole numbers i ough 99999; for hours, froi ough 59.	in the following range m 0 through 23; and	es: for
Check for updat	es every:		
Days: 0	Hours:	Minutes: 00	
		_	-

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:

 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.

Server Manager				
File Action View Help				
🧇 🔿 🙋 🖬 🛃 🖬				
Server Manager (W2K8-AD)		NIS Servers		Actions
- P Roles	nicae	Server Name	Mode Operat	ing NIS Servers 🔺
Microsoft Identity Mana	agement for UNIX	W2K8-AD	Master Windov Subo Windov	Add NIS Server
Password Synchron	ization			View 🕨
- 😁 ad				( Refresh
E NIS Serve	Add NIS Server			Export List
E J w2k8-	View	•		<table-cell> Help</table-cell>
Active Directory Users     Active Directory Sites	Refresh Export List			
A DNS Server     Features	Help			
m Diagnostics     m Diagnostics     m Configuration     Storage				
		•		<b>F</b>
Add NIS Server				

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: XXXXXXXXXXXXX
[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 <code>ypxfrd</code> (the high speed NIS map transfer utility).

[root@oel-nissvr ~]# service ypserv restart			
Stopping YP server services:	[	OK	]
Starting YP server services:	[	OK	]
<pre>[root@oel-nissvr ~]# service ypxfrd restart</pre>			
Stopping YP map server:	[	OK	]
Starting YP map server:	[	OK	]
[root@oel-nissvr ~]# <b>ypwhich</b>			
w2k8-ad.lavemill.org			
[root@oel-nissvr ~]# <b>ypinit -s w2k8-ad</b>			
[ 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
                                    192.168.1.92
config/ypservers
                         host
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.

) <b>\$</b>	Configuration	Maintenance	Shares	Status Analytic
	SERVICES STORAGE	NETWORK SAN	CLUSTER USERS	PREFERENCES ALER
Services				
	Data Services			
	NFS	Online	2013-3-27 13:08:26 🗲 🙂	
	iscsi	Online	2013-3-27 12:11:25 💔 🙂	
	SMB	Online	2013-3-27 13:08:26 🗲 🔱	
	• FTP	Disabled	2013-3-27 12:10:42 🗇 😃	
	● HTTP	Disabled	2013-3-27 12:10:41 🔂 🔱	
	NDMP	Online	2013-3-27 12:11:28 🔂 🛈	
	Remote Replication	Online	2013-3-27 12:11:07 🗲 🔱	
	Shadow Migration	Online	2013-3-27 12:11:07 🗲 🕛	
	• SFTP	Disabled	2013-3-27 12:10:42 🤣 🔱	
	• SRP	Disabled	2013-3-27 12:10:42 🗇 😃	
	TFTP	Disabled	2013-3-27 12:11:26 🕬 😃	
	Virus Scan	Disabled	2013-3-27 12:10:42 🖅 Ů	
	Directory Services			
	• NIS	Disabled	2013-3-27 13:08:26 🤧 😃	
	· LDAP	Disabled	2013-3-27 13:08:26 🔮 😃	
	Active Directory	Online	2013-3-27 13:08:26 🚺 🛈	
	Identity Mapping	Online	2013-3-27 13:08:25 🚺 🛄	

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.

0 \$		Coni	iguration	Mainte	nance	Shar	es	Status	Analytics
		SERVICES	STORAGE	NETWORK	SAN	CLUSTER	ÜSERS	PREFERENC	ES ALERTS
Services	NIS							Prope	rties Logs
G Back to Services	好也2	013-4-10 12:46:57 Onlin	ie					REVERT	APPLY
NIS Directory Service Recognize users and groups defined in a NIS directory. Once NIS service is configured, go to Configuration/Users to give user permission to log into the administrative interface.	the 's			Do Ser	main ad ver(s)	earch using bi lse listed serve	roadcast ers	0.0	
See Also Help: NIS Wikipedia: NIS									

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.

VIS Directory Service	
This service is currently disable service with the new values, or	d. Do you want to apply your changes and enable the leave it disabled?

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.

0 13	Configuration	Maintenance	Shares	Status A	nalytics
	SERVICES STORAGE	NETWORK SAN	CLUSTER USERS	PREFERENCES	ALERT
Services					
	Data Services				
	• NFS	Online	2013-4-2 18:14:50 🗲 🙂		
	iscsi	Online	2013-4-2 18:14:42 🗲 🕛		
	SMB	Online	2013-4-2 18:14:53 🗲 🙂		
	FTP	Disabled	2013-4-2 18:13:05		
	HTTP	Disabled	2013-4-2 18:13:03 🔂 🙂		
	NDMP	Online	2013-4-2 18:14:48 分 山		
	Remote Replication	Online	2013-4-2 18:14:27 🗲 🙂		
	Shadow Migration	Online	2013-4-2 18:14:27 5 0		
	SFTP	Disabled	2013-4-2 18:13:05 🖘 😃		
	SRP SRP	Disabled	2013-4-2 18:13:04 🗇 😃		
	TFTP	Disabled	2013-4-2 18:14:45 🖅 😃		
	Virus Scan	Disabled	2013-4-2 18:13:04 🕫 😃		
	Directory Services				
	V NIS	Online	2013-4-2 18:14:45 🗲 🙂		
	LDAP	Disabled	2013-4-2 18:14:45 🔛 😃		
	Active Directory	Online	2013-4-2 18:14:46 🗲 🛈		
	Identity Mapping	Online	2013-4-2 18:14:44 🗲 🙂		
	System Settings				
	DNS	Online	2013-4-2 18:14:45 🚯 🖒		
	• IPMP	Online	2013-4-2 18:14:38 🚯 🕖		
	NTP	Online	2013-4-2 18:14:52 🗲 🙂		
	Phone Home	Disabled	2013-4-2 18:14:27 🗗 🔱		
	Dynamic Routing	Online	2013-4-2 18:14:48 🗲 🕛		

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.

0 4	Confi	guration	Mainte	nance	Share	s S	tatus A	nalytics
	SERVICES	STORAGE	NETWORK	SAN	CLUSTER	USERS	PREFERENCES	ALERTS
🗈 Services 🤍 Id	entity Mapping				Properties	Rules	Mappings	Logs
G Back to Services	€ 🖞 2013-4-10 12:45:36 Online						REVERT	APPLY
Identity Mapping Service Establish mappings between Windows entities and Unix Ibs. All users are granted temporary credentials by default unless specifically excepted. See Also Help: Identity Mapping	Native LD	AD Attribu AD Attribute AP Attribute - V	Mapping n te - Unix User N e - Unix Group N Vindows User N	node IDM Rul Dire JDM lame	1U e-based ectory-based			

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:

#### 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 <sup>3</sup> as shown in figure 53.

e <u>A</u> ction <u>V</u> iew <u>H</u> elp				
> -> 🖄 💼 🔏 🖬 🗙 🛛	1 Q 💩 🛛 🖬 🔂 🐱 🖄	7 2 2		
Active Directory Users and Comput	Name	Туре	Description	-
🗉 🚞 Saved Queries	🚨 Administrator	User	Built-in account for admini	
🖃 🚎 ad.lavemill.org	👫 ainsley	User		
🕀 🔛 Builtin	& Allowed RODC Password Replica	Security Group - Domain	Members in this group can	
E Computers	🚴 Andrew Ness	User		
🕀 📃 Domain Controllers	A Cert Publishers	Security Group - Domain	Members of this group are	
ForeignSecurityPrincipals	🛃 chloe	User		
Managed Service Accounts	🛃 connor	User		
	Replicat	Security Group - Domain	Members in this group can	
	A DnsAdmins	Security Group - Domain	DNS Administrators Group	
	& DnsUpdateProxy	Security Group - Global	DNS clients who are permi	
	Sea Domain Admins	Security Group - Global	Designated administrators	
	Somain Computers	Security Group - Global	All workstations and serve	
	A Domain Controllers	Security Group - Global	All domain controllers in th	
	Sector Se	Security Group - Global	All domain guests	
	Section 2015	Security Group - Global	All domain users	
	Rengineers	Security Group - Global		
	Senterprise Admins	Security Group - Universal	Designated administrators	
	Enterprise Read-only Domain Co	Security Group - Universal	Members of this group are	
	Scoup Policy Creator Owners	Security Group - Global	Members in this group can	
	🛃 Guest	User	Built-in account for guest	
	Section 1	Security Group - Global		
	RAS and IAS Servers	Security Group - Domain	Servers in this group can	
	Read-only Domain Controllers	Security Group - Global	Members of this group are	
	😣 Schema Admins	Security Group - Universal	Designated administrators	
	Solusers	Security Group - Global		
	Students	Security Group - Global		

Figure 53. Windows Active Directory Users and Computers screen

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

<u>F</u> irst name:	John		Initials: Q	
Last name:	Secretive			
Full name:	John Q. S	Secretive		
User logon name				
johns		@ad.lavem	ill.org	-
User logon name	(pre- <u>W</u> indows)	2000):		
(AD)		linhne		_

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.

Dial-in	Env	vironment	Sess	ions
Remote	control	Remote De	sktop Services Pr	ofile
ieneral   Addre	ss   Account   Profi	le   Telephones	Organization	Member (
Personal Vi	tual Desktop	COM+	UNIX AL	Indutes
To enable acco NIS domain this	ess to this user for Ut s user belongs to.	NIX clients, you t	will have to specif	y the
NIC Demains				_
NIS Domain:	ad			
	ad			
UID:	80598			
100				-
				_
Login Shell:	/bin/sh			
Users	-			_
Home Directory:	/home/johns			
Primary group	-			-
name/GID:	engineers		_	

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.

File Action V	iew Help	
-		
Microsoft Ider	htity Management for UN Name Synchronization based Computers	
🕀 🛃 ad	Map Updates Stop Service Start Service Start NIS Data Migration Wiz	ard
	Check for Updates Now	
	Check for Updates Now View	+
	Check for Updates Now View Refresh Export List	•
	Check for Updates Now View Refresh Export List Properties	•

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



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

Copyright © 2013, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0611

Hardware and Software, Engineered to Work Together