ORACLE
ZFS STORAGE APPLIANCE

How to Use Microsoft Active Directory as an LDAP Source with Oracle ZFS Storage Appliance

ORACLE WHITE PAPER | OCTOBER 2018

ORACLE

Table of Contents

Introduction

Oracle ZFS Storage Appliance integrates advanced hardware and software architectures to offer a facile, multiprotocol storage system capable of running the most demanding workload. This workload includes a variety of simultaneously operating applications and advanced data services.

As a unified storage platform, Oracle ZFS Storage Appliance software can be configured to operate in multiple environments concurrently. In order to fully integrate into these environments, it is necessary to subscribe to the naming systems appropriate to the environment.

For Microsoft Windows, this is typically Active Directory and for UNIX environments, LDAP is one of the most commonly deployed directory systems. In some circumstances, it is desirable to provide services to both Microsoft Windows and UNIX environments where Active Directory is the only deployment directory service.

This document describes how to use the Active Directory service to provide LDAP services to allow Identity Mapping to bridge the different environments. It uses Windows Server 2016 for the Active Directory service and assumes Oracle ZFS Storage Appliance software version OS 8.8 and later.

For the purposes of this document, the Active Directory domain is assumed to be the fictional ‘example.org’

Active Directory LDAP Services

Microsoft Active Directory is the industry standard directory service for Microsoft Windows Environments. Active Directory (AD) is a highly integrated combination of Kerberos for authentication, LDAP for authorization and directory services, and DNS for host name resolution and service location.

AD is used to store information about users, groups, shares and many other types of shared objects.

Oracle ZFS Storage Appliance integrates directly with AD to provide consistent security and ownership details across Microsoft Windows Environments. By default however, AD does not have a way to represent UNIX environment identities which are defined by user IDs (UIDs) and group IDs (GIDs) represented by positive integers. Other details such as home directories, group membership, and default shell are also missing from AD by default. Some details (such as the GECOS field) can be borrowed from standard AD attributes.

AD is extensible by design by way of schema modification. This means that it is possible to add application required attributes to objects such as UIDs and GIDs to allow the Windows AD Domain Controller to interoperate with UNIX environment directory accesses.

Prior to Windows Server 2016, Windows provided these capabilities through Identity Management for Unix (IDMU) and NIS Server Role. These specific features are no longer part of Windows Server 2016 as documented in the Microsoft Technet Note https://blogs.technet.microsoft.com/activedirectoryua/2016/02/09/identity-management-for-unix-idmu-is-deprecated-in-windows-server/. Windows Server 2016, however, still maintains the necessary user and group attributes to continue using Active Directory with LDAP services.

Active Directory's LDAP service is not normally evident other than through the standard AD tools (such as ADSI Edit) which allows access to the raw LDAP directory. It is through tools like these that the directory structure can be verified when the AD configuration varies from a simple out-of-the-box setup. An example of a newly created Active Domain is shown in Figure 1 in the "Active Directory Users and Computers" application and also in the more structured "ADSI Edit" in Figure 2.

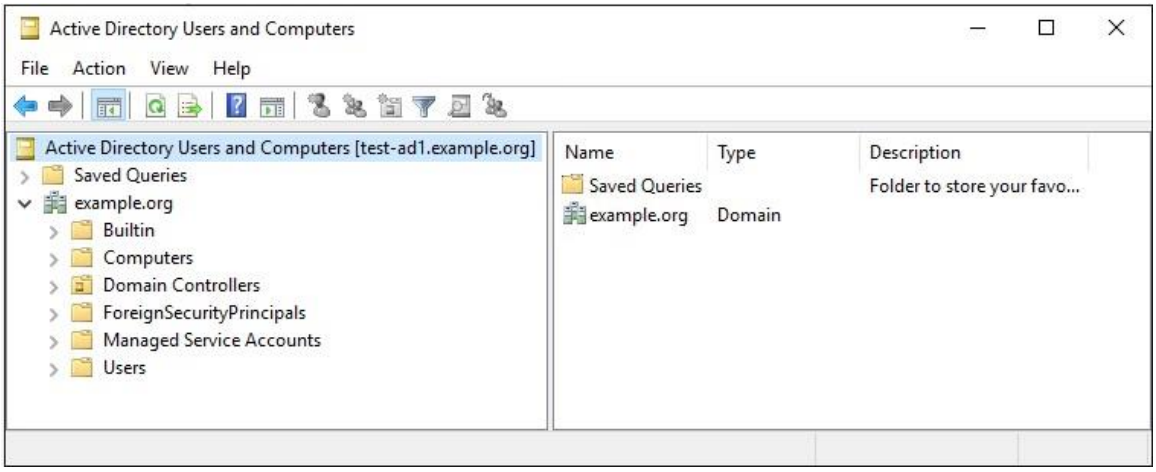

Figure 1 Active Directory Users and Computers view of Newly Created Domain

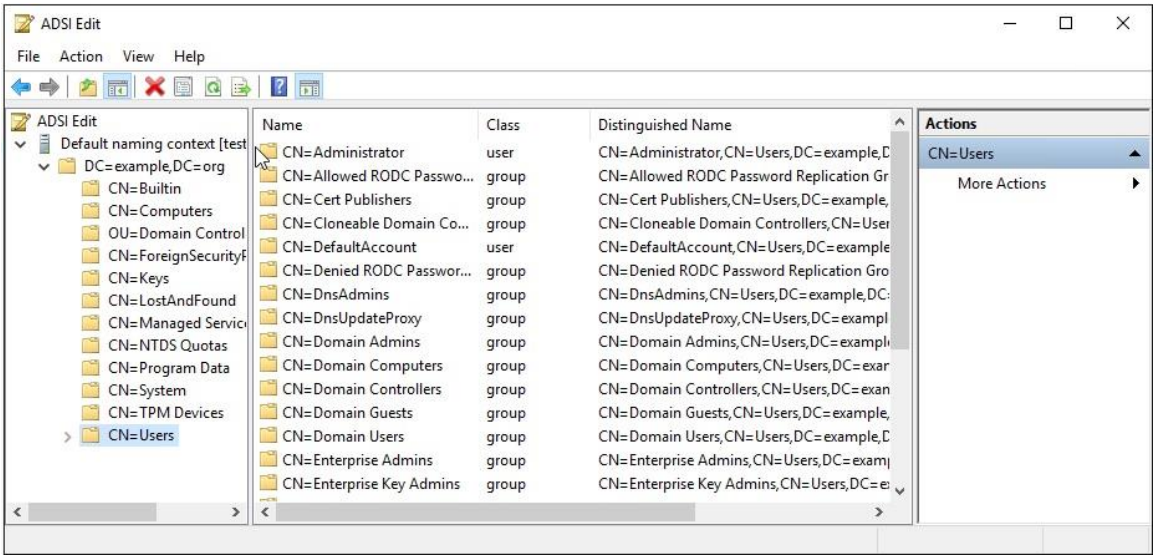

Figure 2 ADSI Edit View of the Newly Created Domain

The ADSI Edit view exposes more of the LDAP structure to the AD Schema.

Configuring Oracle ZFS Storage Appliance for Active Directory Access

In order for Oracle ZFS Storage Appliance to successfully join an AD domain, three components must be correctly configured. These components are DNS services, NTP services, and the actual domain configuration.

Configuring the DNS Service

DNS services are configured on the AD Domain Controller as part of the domain creation. The DNS service plays a large role in AD and Oracle ZFS Storage Appliance must therefore be configured to use the Windows DNS Service.

Using the browser user interface (BUI) of Oracle ZFS Storage Appliance, ensure that the DNS configuration refers to the same DNS server as the AD servers. Access the DNS Configuration screen by selecting **Configuration > Services > DNS**. Enter the DNS domain name, the DNS search domains, and add the IP address of the DNS server by clicking on the plus sign (+) next to "DNS Servers". Apply the changes. The `example.org` configuration is shown in Figure 3.

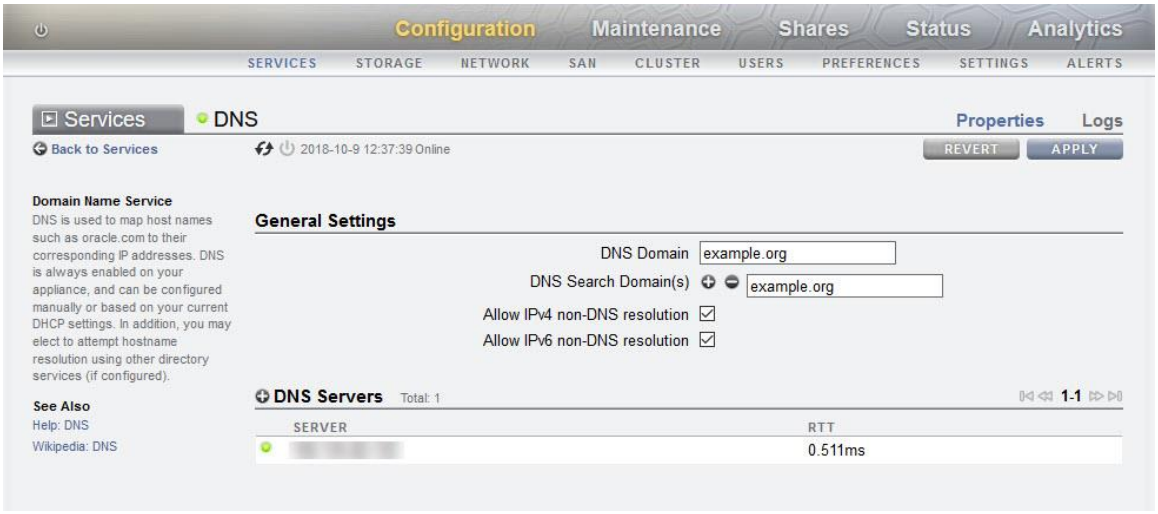

Figure 3 Configuring DNS Services

Configuring the NTP Service

Clock synchronization is also important for correct AD operation. Clock skew between Oracle ZFS Storage Appliance and the AD Domain Controllers must be less than 15 minutes for a successful AD join. It is highly recommended to install a Network Time Protocol (NTP) service and to configure the Oracle ZFS Storage Appliance and the AD Domain Controllers to become clients of the service.

Verify that the clocks on Oracle ZFS Storage Appliance and Windows AD Domain Controllers are in synchronization by navigating to the BUI and selecting **Configuration >Services > NTP**. Both the AD Domain Controllers and Oracle ZFS Storage Appliance should present the same time. The red box in Figure 4 displays the current time.

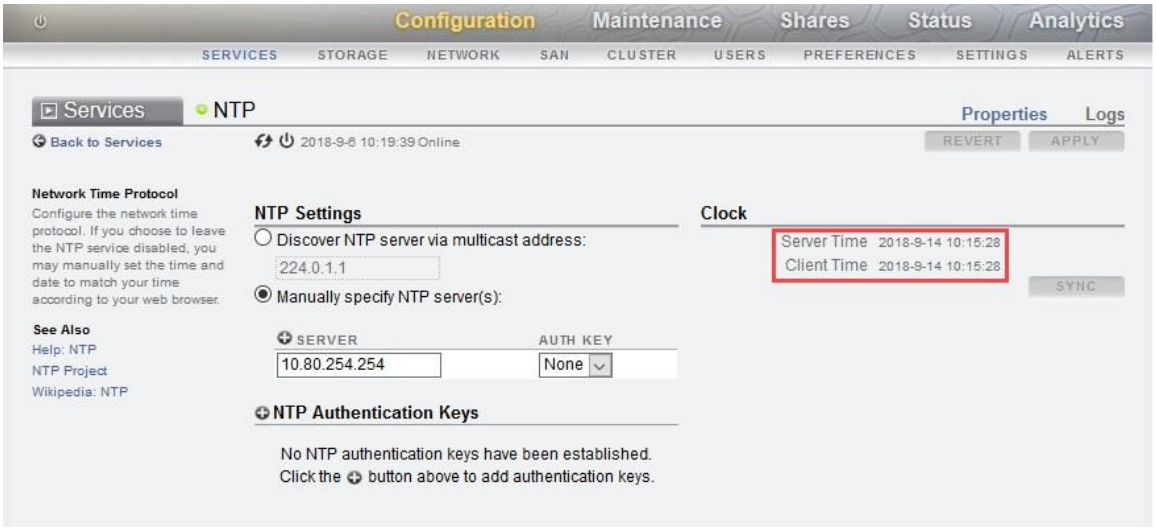

Figure 4 Verifying Clock Synchronization

Joining the AD Domain

To join the AD Domain, use the BUI to navigate to the **Configuration > Services > Active Directory** page. Initially Oracle ZFS Storage Appliance will be in "Workgroup" mode and be a member of the "Workgroup" workgroup. Click the "Join Domain" button as highlighted by a red box in Figure 5.

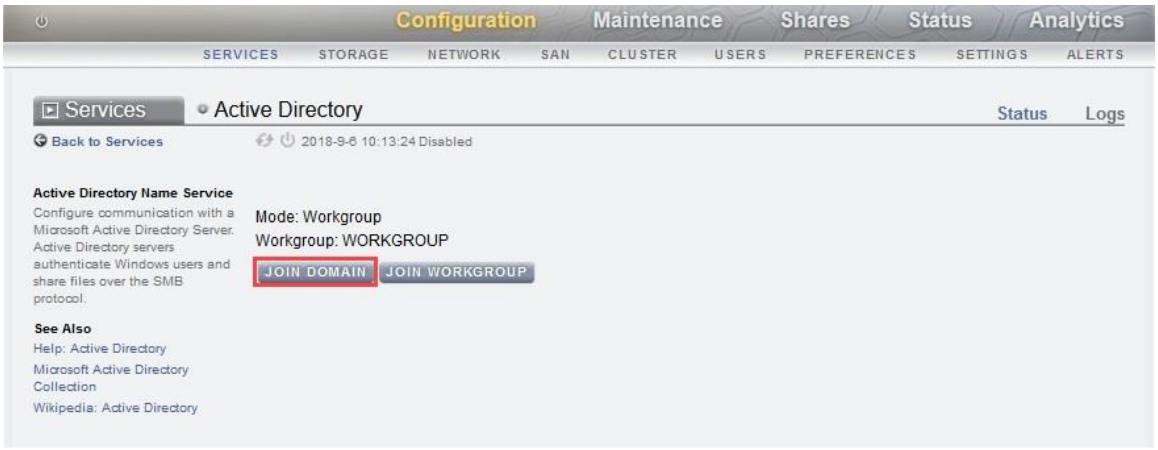

Figure 5 Active Directory Service Page

Enter the details of a Domain Administrator with the authority to allow Oracle ZFS Storage Appliance to join the AD, as demonstrated in Figure 6, and "Apply" the configuration.

Figure 6 Enter the AD Administrator Details

A successful join will provide an acknowledgement similar to Figure 7.

Figure 7 Successful AD Join

If a message indicating 'Access is denied' is displayed, verify that the provided information was correct. If it is correct, then it may be necessary to change the LAN Manager server compatibility setting on Oracle ZFS Storage Appliance. From the BUI, select **Configuration > Services > SMB** and use the drop down menu next to "LAN Manager server compatibility" to choose level "3 – NTLMv2, NTLM, and LM", as shown in Figure 8.

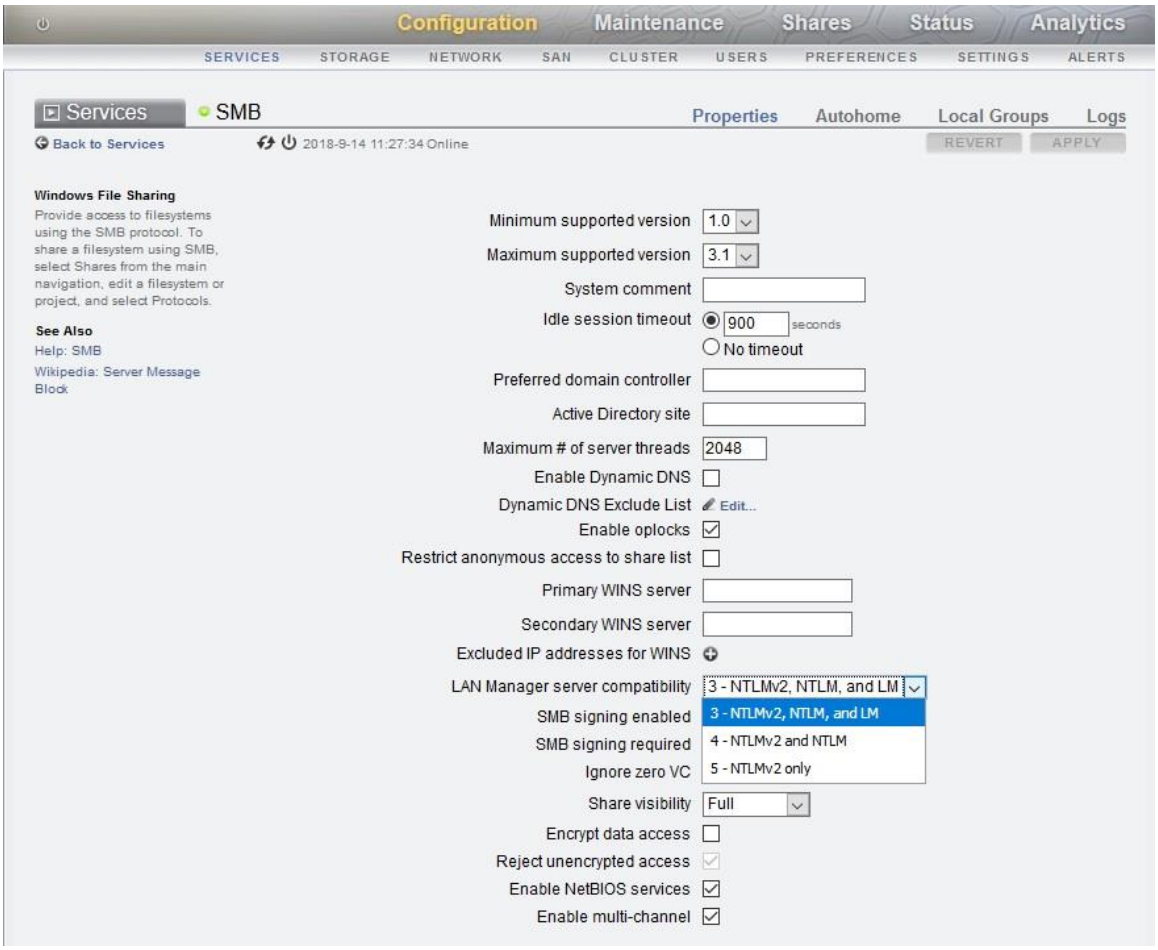

Figure 8 Configuring the LAN Manager server compatibility setting

After applying this change, the AD join operation can be tried again.

The Oracle ZFS Storage Appliance is now able to resolve Windows environment users and groups from Active Directory. In addition, the necessary permissions are now in place for Oracle ZFS Storage Appliance to access AD through the LDAP interface.

Configuring Oracle ZFS Storage Appliance for LDAP Access

The AD domain "`example.org`" is represented in the LDAP interface as the Distinguished Name (DN) '`DC=example,DC=org`'. This DN will be used as the base for searches.

To configure the Oracle ZFS Storage Appliance LDAP client, use the BUI to navigate to **Configuration > Services > LDAP**.

The 'Base Search DN' should be entered as determined above (in this example, `DC=example,DC=org`).

Subtree (or recursive) searches should be enabled to allow the LDAP client to descend into the appropriate tree structures built up in AD.

It is possible to create a proxy user in AD to allow the Oracle ZFS Storage Appliance to access LDAP, but as the previous section configured AD to allow access to LDAP, the bind credential level can be set to 'Self' which will avoid the need to store the proxy user DN and password.

Add the AD Domain Controllers as LDAP Servers. In the example shown in Figure 9, the two AD Domain Controllers are test-ad1 and test-ad2.

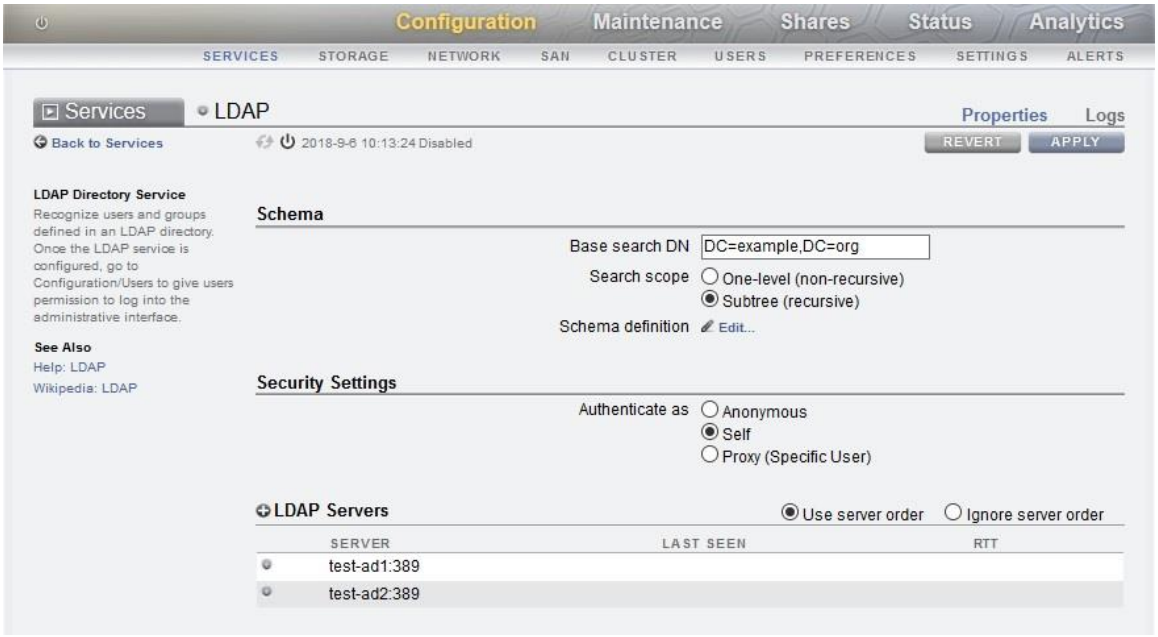

Figure 9 Configuring the LDAP client interface

There are two options regarding search order of the LDAP servers; "Use server order" and "Ignore server order". If the search order of the LDAP servers is unimportant, select "Ignore server order". If there is a preference, select the "Use server order" radio button. With this selection, the first LDAP server will always be tried first and then continue in the order of the list. It is possible to adjust the list order by clicking on the arrows presented on the left side of the list next to the LDAP server to be adjusted, as shown in Figure 10.

Figure 10 Ability to configure LDAP server order

In order to complete the LDAP configuration, the Schema definition needs to be modified to map Unix LDAP fields to Windows AD fields.

By design, Windows users and groups share the same namespace so a user and a group cannot have the same identifier/name. By default these objects live in the 'Users' container which is represented in AD as '`CN=Users,<BASE-DN>`'. This would be '`CN=Users,DC=example,DC=org`' for example.org.

This DN is then used as the User Search Descriptor in the Schema Definition.

UNIX environments however, have separate namespaces for users and group definitions which allow groups to be created with the same name as users. In order to cater for this difference, the group search descriptor has to be set to the same as the user search descriptor.

The following schema mappings need to be added in order for identity mapping to function correctly.

Context	Category	Mapping
Users	Search descriptor	`CN=Users,DC=<domain>,DC=<extension>`

	Attribute mappings	`homeDirectory=unixHomeDirectory`
		`gecos=cn`
		`uid=sAMAccountName`

	Object class mappings	`posixAccount=user` `shadowAccount=person`
Groups	Search descriptor	`CN=Users,DC=<domain>,DC=<extension>`
	Object class mappings	`posixGroup=group`

To implement these changes with the Oracle ZFS Storage Appliance BUI, navigate to **Configuration > Services > LDAP** (as shown in Figure 9) and select "Edit…" to the right of the "Schema definition" label.

An "Edit LDAP Schema Definition" dialog will be opened, as shown in Figure 11.

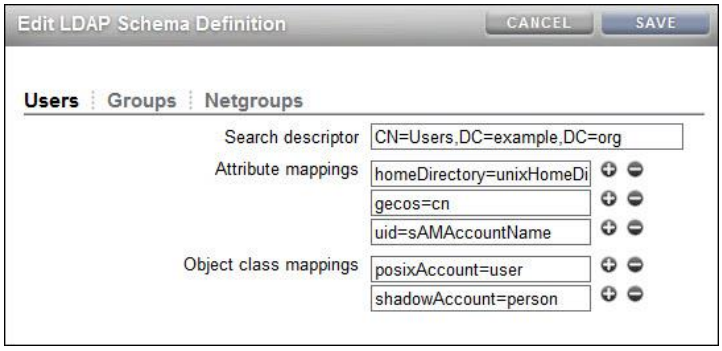

Figure 11 Edit LDAP Schema Definition – Users

Enter the appropriate Users Search descriptor, Attribute mappings, and Object class mappings according to the entries from the earlier table, using your site specific domain and extension.

Click on the Groups tab and enter the appropriate Grooups Search descriptor and Object class mappings, as shown in Figure 12.

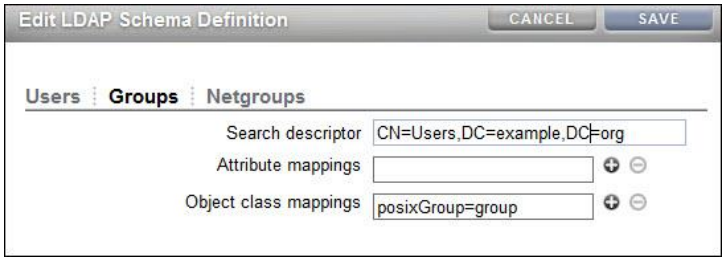

Figure 12 Edit LDAP Schema Definition – Groups

No entries are needed on the Netgroups tab.

Save the changes to apply the new schema edits.

Adding Users and Groups to Active Directory with Unix Properties

Since Windows Server 2016 no longer provides the IDMU interface, adding values to the Unix style fields need to be performed using the Attribute Editor. The Attribute Editor is only accessible by selecting “Advanced Features” in the View meu of the Active Directory Users and Computers tool. The selection of Advanced Features is shown in Figure 13.

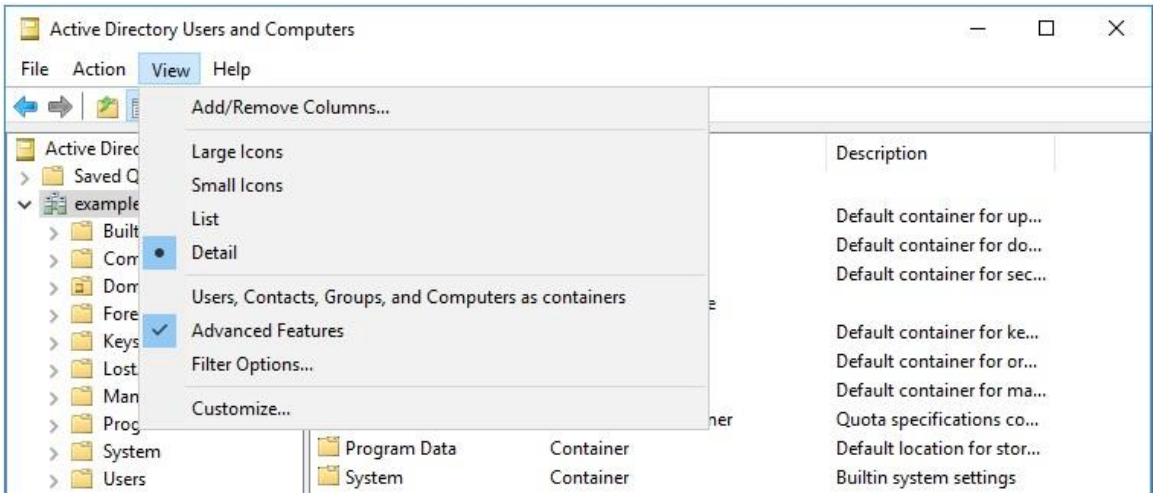

Figure 13 Configuring Advanced Features attribute editor

Create the group (with Group type: Security) corresponding with the group id number used with the Unix environment. For this example, the group `unixusers` was created. After creating the group, right-click on the group name and select "Properties" to open the Group Properties dialogue, then select the Attribute Editor tab. Scroll down to the "gidNumber" entry and double-click it to change the value to the corresponding Unix group number. For this example, the `unixuser` group is assigned the value 10000, as shown in Figure 14.

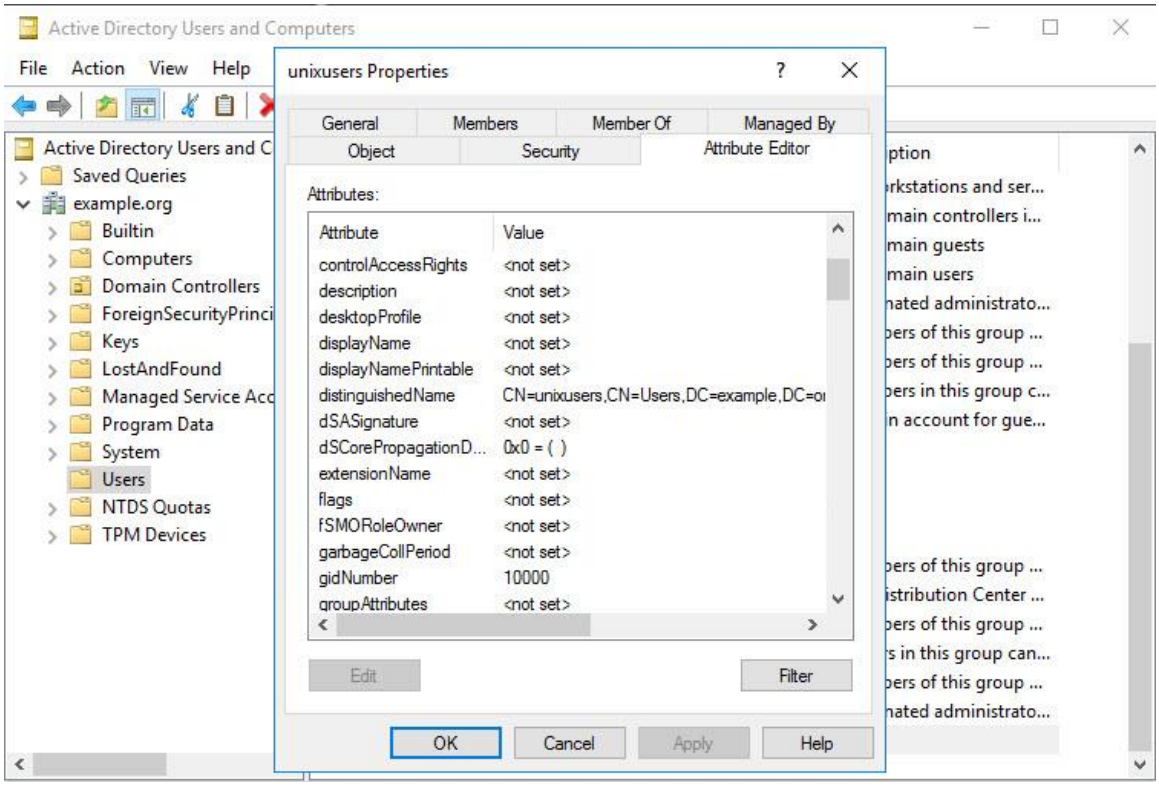

Figure 14 Setting the `gidNumber` for an AD group

Create (or select) the user that will need the Unix identity mapping. Right-click on the user name and select "Properties" to open the User Properties dialogue, then select the Attribute Editor tab. Scroll down the list of attributes and set:

- `uidNumber` – the unique integer corresponding with the Unix id number (e.g. 11001)
- `gidNumber` – the integer corresponding with the Unix group number (e.g. 10000 (unixusers))
- `unixHomeDirectory` – corresponding with Unix environment (e.g. /export/home/collin)
- `loginShell` – corresponding with Unix environment (e.g. /usr/bin/bash)

An example screenshot for user `collin` is in Figure 15.

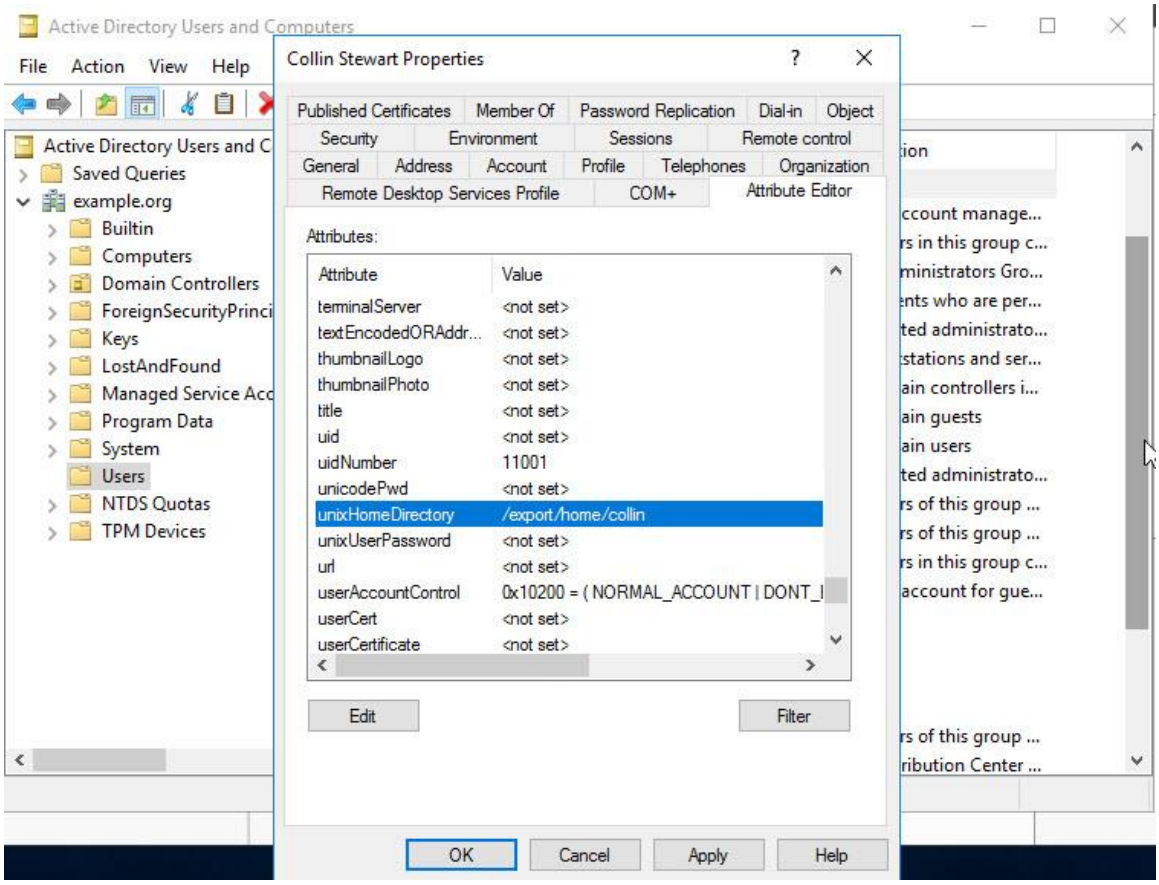

Figure 15 Using Attribute Editor to modify Unix user attributes

Perform the group and user creations and modifications as needed for the environment.

Verifying Oracle ZFS Storage Appliance Identity Mapping

Once all of these changes have been made, it is necessary to check that the mapping will occur as expected to ensure that consistent ownership and permissions are maintained between Windows and UNIX environments.

From the Oracle ZFS Storage Appliance BUI, navigate to **Configuration > Services > Identity Mapping**.

Ensure that the Mapping mode is set to "IDMU", as shown in Figure 16.

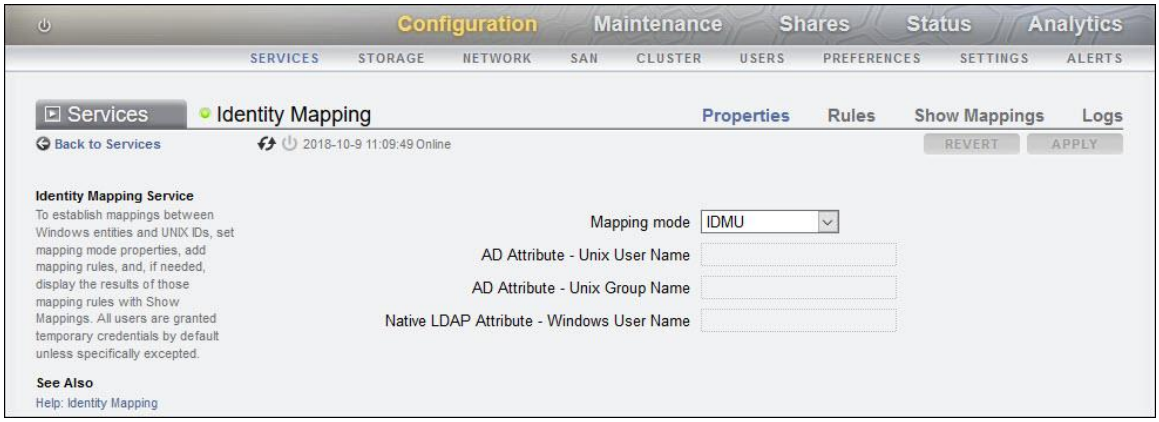

Figure 16 Configuring the IDMU Mapping mode

Select the "Show Mappings" tab. With the Windows radio button selected, either the Windows user name or group name can be checked. After entering the name, click on the "Show Mapping" button to view the results. If the name is a valid user, the user mapping information will display under the User Properties section. If the name is a valid group, the group mapping information will display under the Group Properties section. Examples of username `collin` and group name `unixusers` identity mappings from Windows to Unix are shown in Figures 17 and 18.

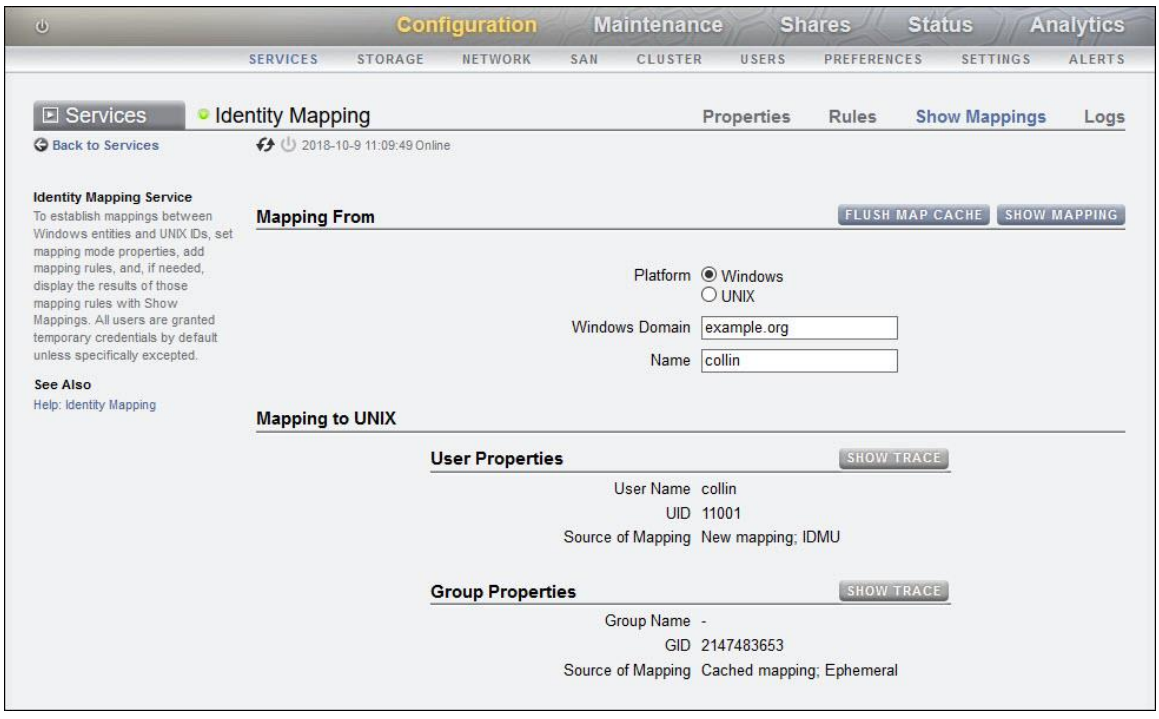

Figure 17 Windows to Unix identity mapping of user `collin`

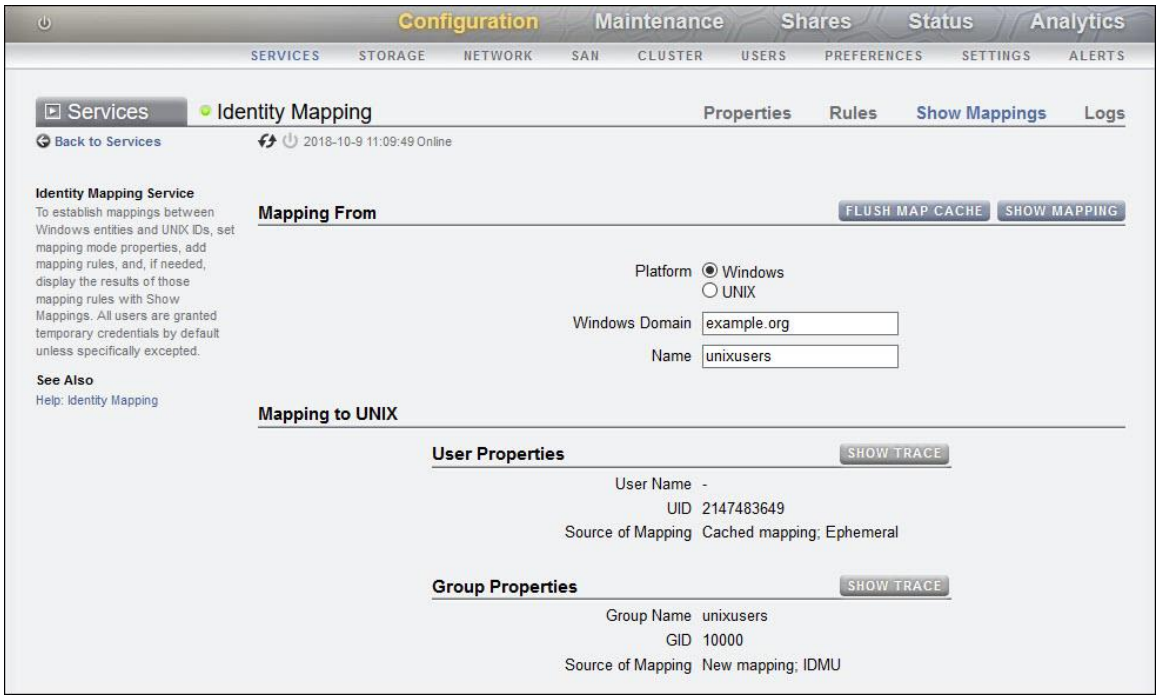

Figure 18 Windows to Unix identity mapping of group `unixusers`

Notice that when the user id is valid, the group information provides an invalid GID and shows the source to be "Ephemeral". This indicates a mapping that could not be located. The same occurs to the UID when the group id is valid. These values can be ignored.

To validate the identity mapping from Unix to Windows, select the Platform UNIX radio button. Here, the id type must be specified by either selecting the "User" or "Group" radio button. Example output for user `collin` and group `unixusers` are shown in Figures 19 and 20.

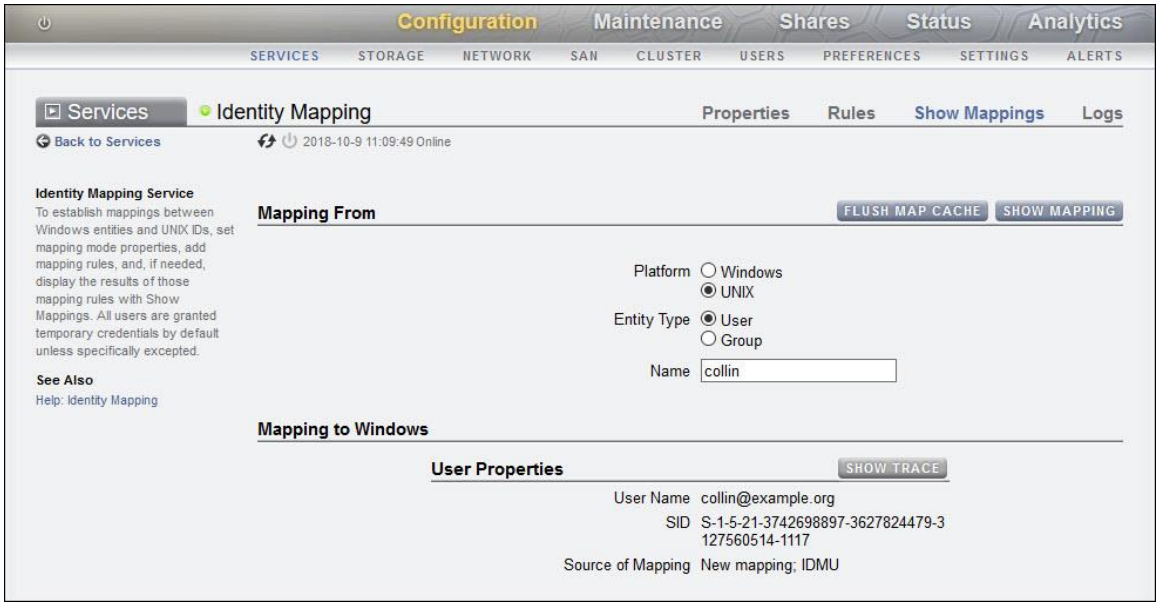

Figure 19 Unix to Windows identity mapping of user `collin`

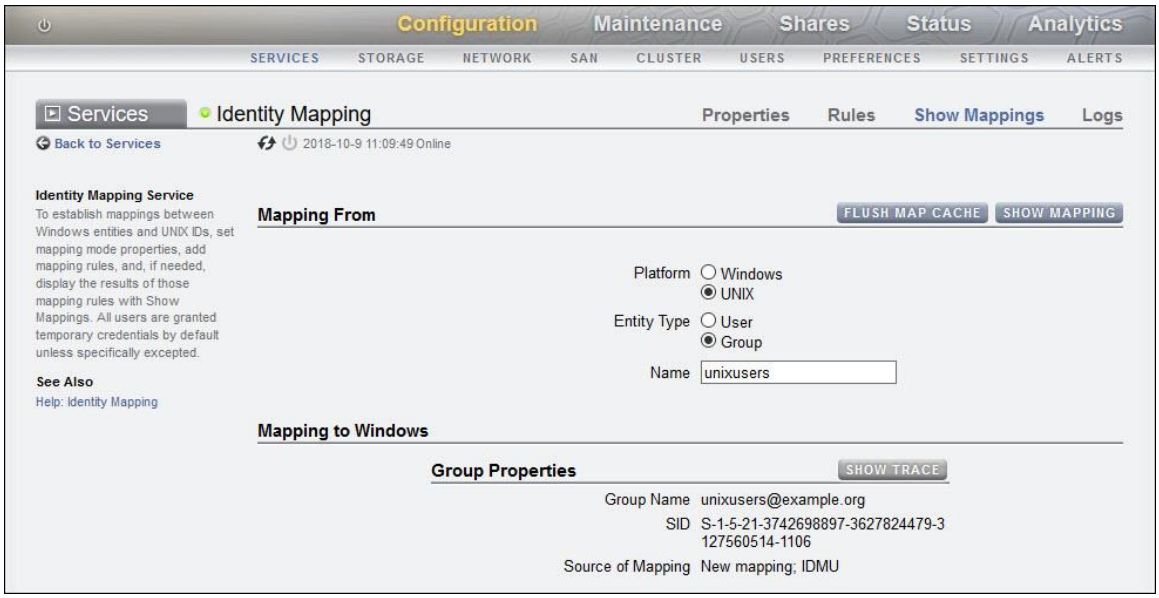

Figure 20 Unix to Windows identity mapping of group `unixusers`

If the expected mappings are not displayed correctly, verify the attributes entered for the users and groups in AD.

Complex Active Directory Schema Structures

Where large and complex AD schemas have been deployed, Windows AD administrators may impose a hierarchy of users broken down by geography and/or function.

It may be desirable then to limit the searches in certain circumstances to a single subtree or subtrees to allow optimum ID resolution speed by reducing the search space.

To illustrate this, the fictional `example.org` has over 20,000 active AD users defined spread across multiple countries. In order to maintain a manageable hierarchy, the AD administrators have implemented a geographically-arranged tree – a subset of this tree concentrating just on the users is shown in Figure 21.

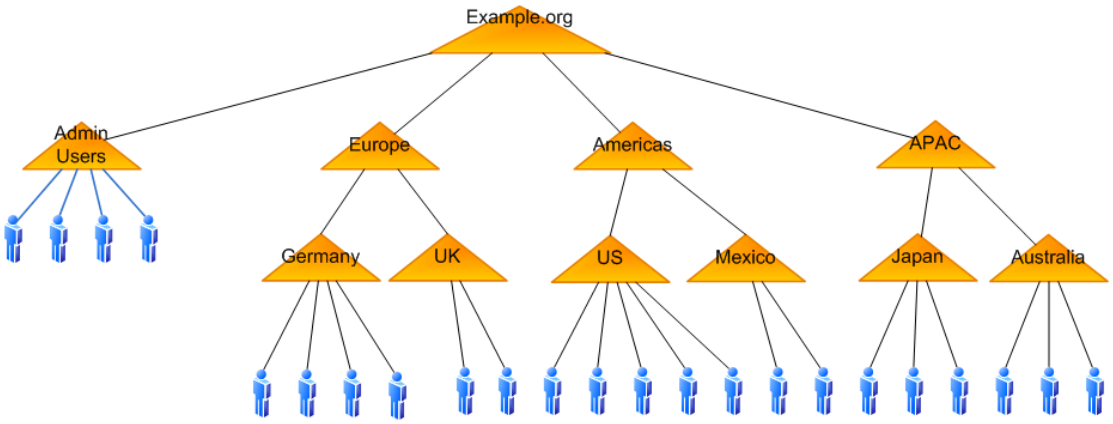

Figure 21 `Example.ORG` Hierarchy

In order to provide the best lookup performance, the Storage administrators have decided that they will restrict searches to just the geographic areas and the administrative user subtrees.

Users exist within the country Organizational Units (OU) and these countries are contained in the geographical OU. A separate `AdminUsers` OU has also been created to allow group policies to be applied to these users without affecting the geographical users or vice versa.

As there is no common node other than the root of the domain and it would not be advisable to search the entire tree for users for performance reasons, the Oracle ZFS Storage Appliance offers an alternative approach where the multiple subtrees can be nominated for searches by separating the DNs with a semicolon.

In the “simple” example from the previous sections, the LDAP schema definition user search descriptor was

```
CN=Users,DC=example,DC=org
```

Using the additional search feature, the user search descriptor for the more complex configuration becomes

```
OU=AdminUsers,DC=example,DC=org; OU=Americas,DC=example,DC=org;    \
OU=APAC,DC=example,DC=org; OU=Europe,DC=example,DC=org
```

The Oracle ZFS Storage Appliance will then search each of these subtrees in turn to attempt to resolve any references and thus it may make sense to alter the order for the OUs depending on where the Oracle ZFS Storage Appliances are sited and also which user base makes most use of the services offered by the Oracle ZFS Storage Appliance.

In addition, the Group search descriptor should also be changed if groups are arranged in a similar manner – i.e. under each geographical OU or if there's a separate OU created to hold the security groups in AD. This might be the case where the functional unit assignment is defined in a global sense rather than geographical.

The ADSI Edit view of the AD domain is provided in Figure 22.

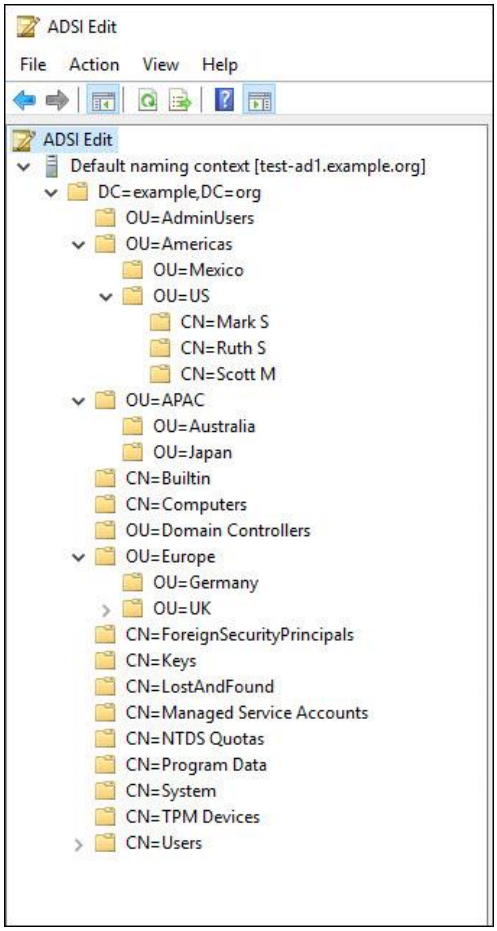

Figure 22 ADSI Edit view of geographical AD configuration

Conclusion

The Oracle ZFS Storage Appliance provides a platform which bridges the gap between Windows and UNIX environments in a secure and consistent manner.

Access authorization granted in one environment is mirrored in the other where the appropriate mappings are available.

By providing the flexibility to tailor the search descriptors, both simple and highly complex Active Directory schemas can be handled in a simple and consistent manner.

By providing the LDAP interfaces, the Identity Mapping feature brings together two disparate environments allowing the sharing of data and reduction in the number of storage islands where spare storage cannot be used in any other environment.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

How to Use Microsoft Active Directory as an LDAP Source with Oracle ZFS Storage Appliance
October 2018, Version 2
Authors Andrew Ness, Eric Polednik