Configuring Microsoft Active Directory for Oracle Net Naming

An Oracle White Paper
April 2014

Configuring Microsoft Active Directory for Oracle Net Naming

Configuring Microsoft Active Directory for Oracle Net Naming

INTRODUCTION

The Oracle Net naming method resolves names to a database connect descriptor. One of the naming methods is directory-naming method. Directory naming resolves a database service name, net service name, or net service alias stored in a centralized LDAP-compliant directory server, including Oracle Internet Directory and Microsoft Active Directory. Centralized administration of database services and net service names makes them easier to add or relocate. Users initiate a connection request by providing a connect string. A connect string includes a username and password, along with a connect identifier. A connect identifier can be the connect descriptor itself or a name that resolves to a connect descriptor

Active Directory has to be configured for Oracle usage in order to use functionality provided by directory naming. This involves extending Active Directory schema objects and creating OracleContext container. Oracle Schema objects are sets of rules for Oracle Net Services and Oracle Database entries and their attributes stored in Active Directory. Active Directory name resolution provides central administration of database services and net service names, making it easier to add or relocate services leveraging existing windows environment in an enterprise.

Oracle Net naming with Active Directory is supported for clients on Windows hosts. Services (database) can be running on any machine, and do not necessarily have to be Windows hosts.

This paper outlines detailed steps to configure Active Directory for supporting net service naming in Windows Server 2008 and higher for Oracle Database 11g Release 2 (11.2.0.3) and higher.

Following are the main steps to configure Active Directory for Oracle Net Naming:

- Enable anonymous browsing of Active Directory
- Create Oracle Context with NetCA
- Creating Display Specifiers

STEPS TO CONFIGURE ACTIVE DIRECTORY

After promoting a Windows Server to become an Active Directory domain controller, Active Directory must be configured to allow an Oracle Context to be created.

Enable Anonymous Browsing

Windows Server Active Directory allows only authenticated users to initiate an LDAP request against Windows Server based domain controllers. An LDAP browser/modifier is required to enable anonymous browsing. An easy way to modify required attribute values is to use the Windows ADSI Edit utility.

To invoke ADSI Edit, issue the adsiedit.msc command from a Windows command window. Or in the MMC Console Root, click File, Add/Remove Snap-in, Add, select ADSI Edit, click Add, Close, then click OK. Select, then right-click ADSI Edit, click Connect to, select Configuration Naming Context, and then click OK.

Expand the Configuration container and navigate to:

Configuration [acme.com]

CN=Configuration, DC=ACME, DC=COM

CN=Services

CN=Windows NT

CN=Directory Service

Right- click the CN=Directory Service container, select Properties, and then scroll down to select the dSHeuristics attribute.

Edit the dSHeuristics attribute and set its value to 0000002. Setting this value allows anonymous clients to perform any operation that is permitted by the access control list (ACL)

Extending Schema and Creating Oracle Context

You must create an Oracle Context to use Oracle Net directory naming features with Active Directory. Oracle Context is the top-level Oracle entry in the Active Directory tree. It contains Oracle Database service and Oracle Net service name object information.

Use Oracle Net Configuration Assistant (NetCA) to extend the schema and create your Oracle Context. Oracle NetCA is a graphical, wizard-based tool used to configure and manage Oracle Network configurations. You can create the Oracle Context during or after Oracle Database custom installation.

You can create only one Oracle Context for each Windows domain (administrative context). You must have the right to create domain and enterprise objects in order to create the Oracle Context in Active Directory with Oracle Net Configuration Assistant.

1. Run the Network Configuration Assistant (NetCA):
   a) Click Start, and then click All Programs.
   b) Click Oracle, Configuration and Migration Tools, then Net Configuration Assistant.
2. Select the Directory Usage Configuration radio button, and then click next.
3. Select Directory Type Microsoft Active Directory, and then click next.

   Note: The Microsoft Active Directory configuration option is only available in the Windows version of NetCA.
4. Select the option to configure the directory for Oracle usage and create the Oracle Schema and Context, then click next.
5. Enter the Active Directory hostname, and then click next. If you are configuring the forest for the first time, you must enter the hostname of the Schema Master Controller and you must be logged in as a user from that domain with privilege to create schema objects.
6. Select the option to upgrade the Oracle Schema, and then click next.
7. The next page should denote successful directory configuration:

   Directory usage configuration complete!

   Example: The distinguished name of your default Oracle Context is:

   Cn =OracleContext, DC=ACME, DC=COM
8. Click next, and then click Finish.

The following restrictions apply to creating Oracle schema objects to use with Active Directory:

Only one Oracle schema object can be created for each forest.

The root domain controller must be the operations master that allows schema updates. See your operating system documentation for instructions.

If the Active Directory display is not configured to accept all 24-default languages, then Oracle schema object creation can fail while Oracle Net Configuration Assistant is configuring Active Directory as the directory server. Before running Oracle Net Configuration Assistant to complete directory access configuration, verify that the display specifiers for all 24 languages are populated by entering the following at the command prompt:

```
ldifde -p OneLevel -d cn=DisplaySpecifiers,
cn=Configuration, domain context -f temp file
```

where:

domain context is the domain context for this Active Directory server. For example, `dc=example, dc=com`

temp file is a file where you want to put the output.

If the command reports that fewer than 24 entries were found, then you can still use Oracle Net Configuration Assistant. However, the report will indicate that Oracle schema object creation failed, rather than simply reporting that display specifiers for some languages were not created.

Creating Display Specifiers

When Net Configuration Assistant creates the Oracle schema object in Active Directory, the display specifiers for Oracle entries are not created. This means you cannot view Oracle database entries in Active Directory interfaces.

You can manually add these entries into Active Directory after the Oracle schema object has been created by doing the following, using the same Windows user identification you used when creating the Oracle schema object with Net Configuration Assistant:

1. Open a command shell.
2. Change directory to ORACLE_HOME\ldap\schema\ad.
3. Copy adDisplaySpecifiers_us.sbs to adDisplaySpecifiers_us.ldif.
4. Copy adDisplaySpecifiers_other.sbs to adDisplaySpecifiers_other.ldif.
5. Edit each of these. ldif files, replacing all occurrences of %s_AdDomainDN% with the domain DN for the specific Active Directory into which you want to load the display specifiers (for example, dc=acme, dc=com).
6. Run the following commands:

```
ldapmodify -h <ad hostname> -Z -f adDisplaySpecifiers_us.ldif
```

```
ldapmodify -h <ad hostname> -Z -f adDisplaySpecifiers_other.ldif
```

where <ad hostname> is the hostname of the Active Directory domain controller to which you want to load the display specifiers.

Successful completion of OracleContext enables Active Directory to store NetServices and DatabaseServces. Net Manager or Oracle Enterprise Manager can be used to create service names in Active Directory.

Default access control lists (ACLs) on Net Service names do not allow anonymous reading of their attributes. If the Oracle client binds anonymously for name resolution, then ACLs on OracleContext and Net Service names should be changed to allow anonymous reading. Beginning with Oracle Database 11g, database administrators can restrict access to a service by configuring Oracle clients to authenticate and control the services available to them by ACLs on services. Use the NAMES.LDAP_AUTHENTICATE_BIND=TRUE parameter in sqlnet.ora to specify whether the LDAP naming adapter should attempt to authenticate when it connects to the Active Directory to resolve the name in the connect string. Windows client uses native authentication method to authenticate to Active Directory.

CONCLUSION

Windows Server Active Directory allows only authenticated users to initiate an LDAP request against Windows Server based domain controllers. Updating registry entry, one attribute of Active Directory helps in successful completion NetCA directory configuration. Thus, enabling it for Oracle Net Naming.

Configuring Microsoft Active Directory for Oracle Net Naming
April 2014

Author: Srinivas Pamu
Contributing Author: Kant Patel
Contributing Author: Norman Woo

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

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.