ORACLE®
METALINK

Headlines   **Knowledge**   Service Request   Configuration Support Manager   Patches & Updates   Forums   Certify

Knowledge Browser   **Advanced Search**   Bug Search   Secure Enterprise Search

Quick Find | Knowledge Base   Go   Secure Enterprise Search   Advanced   Saved Searches

Did this article help solve your problem? | Select   Would you recommend this document to others?   Select   Submit

TIP: Click help for a detailed explanation of this page.   Bookmark   Go to End

---

Subject: **Creating an OracleContext in Microsoft Windows 2003 Active Directory**

Doc ID: **Note:361192.1**   Type: **BULLETIN**

Last Revision Date: **05-SEP-2006**   Status: **MODERATED**

Creating an OracleContext in Microsoft Windows 2003 Active Directory

Purpose

An LDAP Schema is a collection of related entries (attributes, objectclasses) stored within an LDAP directory. An LDAP Context refers to all information relating to entries (users, groups, etc.) as well as their state.

An LDAP directory stores information (Schema/Context) pertaining to Oracle software under an entry called an Oracle Context (cn=OracleContext). An OracleContext may exist under any entry in a Directory Information Tree (DIT). Oracle Net Configuration Assistant (NetCA) can be used to create an OracleContext as well as to configure access to the directory. Once configured for directory access, Database Configuration Assistant (DBCA) can be used to register databases. Registration adds entries for databases and associated Oracle Net connect descriptors.

Though OracleContexts are typically created in Oracle Internet Directory (OID), they are not limited to using OID as their LDAP store. It is possible to create an OracleContext in a foreign Directory Schema, such as Microsoft Active Directory (AD).

The purpose of this article is to describe how to create an OracleContext within Microsoft Active Directory 2003.

Scope and Application

This article is intended for Microsoft Windows System Administrators and Oracle Database Administrators looking to create an OracleContext within Microsoft Active Directory.

Oracle Internet Directory (OID) provides rich features and functionality. However, depending on deployment requirements, the use of an OracleContext collocated within an existing Active Directory Schema may be sufficient. This approach does not require additional hardware, administration or maintenance of a dedicated Oracle Internet Directory installation.

Creating an OracleContext within Active Directory requires that you already have a fully functional and correctly configured Active Directory server.
The procedure described uses the following topology and product versions:

Oracle Client
Hostname: cyclops.home.com
IP Address: 192.168.1.90

Microsoft Windows Server 2003 Enterprise Edition Service Pack 1
Oracle Client Oracle10g Release 1 Patchset 2 (10.1.0.4.0) for Microsoft Windows

Active Directory Server
Hostname: cyclops.home.com
IP Address: 192.168.1.90
Microsoft Windows Server 2003 Enterprise Edition Service Pack 1
Active Directory Realm: home.com

Creating an OracleContext in Microsoft Windows 2003 Active Directory

This article describes how to create an OracleContext within Microsoft Windows Server 2003 Enterprise Edition Active Directory, however other Windows Server 2003 Editions, such as Standard or Datacenter, may also be used. The various features of Windows 2003 Editions can be compared at http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx .
Microsoft Windows 2003 Service Pack 1 was applied before the Server was promoted (*dcpromo*) to a standalone Domain Controller/DNS server in it's own forest.

1. Configuring Active Directory

After promoting Windows Server 2003 to become an Active Directory domain controller, Active Directory must be configured to allow an OracleContext to be created.
Log on to the Active Directory server with Administrative privilege.

1.1 Register Schema Management Library

To manage the Active Directory Schema, first register the *Active Directory Schema* library.
Click *Start*, *Run*, enter *regsvr32 %WINDIR%\system32\schmmgmt.dll*, then click *OK*.
Click *OK* in the confirmation dialog box.

1.2 Start Microsoft Management Console (MMC)

The Microsoft Management Console (MMC) hosts Windows administrative tools required to manage system components, networking and services.
Start the Microsoft Management Console.
Click *Start, Run*, enter *mmc*, then click *OK*.
An empty MMC Console window will appear.

1.3 Add Active Directory Schema Snap-in

Add the *Active Directory Schema* MMC snap-in to the MMC Console Root.
In the MMC window, select menu option *File*, click *Add/Remove Snap-in*, click *Add*, select *Active Directory Schema*, click *Close*, then *OK*.
The *Active Directory Schema* MMC snap-in is added under the MMC Console Root.

Explode the *Active Directory Schema* object to reveal the Classes (objectclasses) and Attributes folders.
The folders comprise all objectclasses and attributes contained in the Active Directory Schema.
At this point, no Oracle attributes or objectclasses exist in the Schema (i.e. orcl*).

1.4 Check Schema Permissions

To view user Schema permissions, collapse then right mouse click *Active Directory Schema* in the *Active Directory Schema* MMC, then select *Privileges*.
Not all users/groups are displayed, therefore add any unlisted users/groups by clicking the *Add* button under the *Group or user names* section.
Add the user/group intended to create the OracleContext.
By default, the Administrators group does not have Schema write permission - all other users/groups are granted read permission.

1.5 Grant Schema Write Privilege

To modify user/group Schema permissions, click the *Allow* and *Deny* check boxes beside the various listed permissions that you wish to grant or deny.
To apply additional permissions, or extend the scope of those permissions, click the *Advanced* button.
Edit permissions as required e.g. change a user permission from *Apply to:* '*This object*' to '*This object and All Child Objects*'.
Grant Schema write privilege to the user/group intended to create the OracleContext (Administrator in my case), then close the Permissions dialog box.

1.6 Extending the Schema

Caution: Active Directory Schema extensions are permanent - attributes and objectclasses, such as those created as part of OracleContext creation, cannot be removed.
Refer to http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/disabling_existing_classes_and_attributes.asp .
Taking a system/catalog backup prior to creating the OracleContext is highly recommended.

Having granted Schema write privileges, Active Directory must still then be explicitly configured to allow Schema modification.
This is achieved by adding a registry parameter.
Click *Start*, *Run*, enter *regedit*, then click *OK*.
Navigate to registry subkey
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`
Add new parameter '*Schema Update Allowed*' (of type REG_DWORD) with a hexidecimal value of 1.
The setting is dymanic and takes immediate effect.

1.7 Enable Anonymous Bind Operations

Depending on your source of Windows distribution, it may be necessary to configure Active Directory to allow anonymous operations.
For additional information refer to http://support.microsoft.com/default.aspx?scid=326690 .
When anonymous operations are disabled, anonymous operations performed against Active Directory will fail with the following error:

```
Operations Error (1)
Additional information: 00000000: LdapErr: DSID-0C0905FF, comment: In
order to perform this operation a successful bind must be completed on
the connection., data 0, vece
```

With DS event logging enabled (see Debugging section), the same is reported in Event Viewer Directory Service messages.

An LDAP browser/modifier is required to enable anonymous operations.
An easy way to modify required attribute values is to use the Windows ADSI Edit utility.
ADSI Edit, another MMC snap-in, is available as part of the Windows 2003 Support Tools located on the Windows Server 2003 CD-ROM i.e. X:\SUPPORT\TOOLS\SUPTOOLS.MSI.
Install the Windows 2003 Support Tools - refer to
http://technet2.microsoft.com/WindowsServer/en/Library/baa79cdd-83b0-4f10-9356-b2d14462d5b21033.mspx .

To invoke ADSI Edit, in the MMC Console Root, click *File*, *Add/Remove Snap-in*, *Add*, select *ADSI Edit*, click *Add*, *Close*, then click *OK*.
Select, then right mouse click *ADSI Edit*, click *Connect to ...*, select *Select a well known Naming Context (Domain),* then click *OK*.
Again, click *Connect to ...*, select *Select a well known Naming Context (Configuration)*, then click *OK*.
Explode the *Configuration* container and navigate to:
Configuration [cyclops.home.com]
  CN=Configuration,DC=home,DC=com
    CN=Services

    CN=Windows NT
      CN=Directory Service

Right mouse click the *CN=Directory Service* container, select *Properties*, then scroll down to select the *dSHeuristics* attribute.
Edit the *dSHeuristics* attribute and set its value to 0000002 (six zeros then two).

To be able to view all Containers under the default naming realm (*DC=home,DC=com* in this case) once NetCA is run later, enable the *View Advanced Features* option in *Active Directory Users and Computers*.
Click *Start*, *All Programs*, *Administrative Tools*, then *Active Directory Users and Computers*.
Click menu option *View*, then select *Advanced Feature*s.

In preparation for Oracle Clients to be able to query the OracleContext and resolve service names, ensure the Active Directory server remains configured to allow anonymous binds.
If anonymous binding is disabled, Oracle Clients configured for directory access (LDAP naming resolution) will likely fail with error - ORA-12154: TNS:could not resolve the connect identifier specified, in which case refer to References section for related Notes.

2. Oracle Installation

At time of writing, the minimum Oracle versions known to work include:

- Oracle 10g Release 1 with Patchset 2 (10.1.0.4.0) and Patch bundle 1

For Oracle 10g Release 1 (10.1.0):

- Install Oracle 10gR1 (10.1.0.2.0) - at a minimum, install an Oracle Client installation
- Apply the Oracle 10gR1 Patchset 2 (10.1.0.4.0) per MetaLink Patch 4163362
- Then apply Oracle 10.1.0.4.0 Patch 1 per MetaLink Patch 4287619

In this case, the Oracle Client installation was performed by Administrator on the Active Directory server itself.
However, the Oracle installation may be performed on another machine (an Oracle client or server), then NetCA run from that machine.
In this case, ensure aforementioned patches are applied, then log in to the server as the domain user/group member granted Schema write privilege to create the OracleContext per **Step 1.5** above.
If choosing to perform a custom installation, at a minimum, ensure that all components provided as part of the default Oracle Client installation profile are installed.
Once installation is complete, ensure that the Oracle LDAP toolset are installed to `%ORACLE_HOME%`
`\bin` e.g. `ldapadd.exe`, `ldapbind.exe`, `ldapmodify.exe`, etc.

3. Creating an OracleContext

3.1 Network Configuration Assistant (NetCA)

Oracle Net Configuration Assistant (NetCA) is a graphical, wizard-based tool used to configure and manage Oracle Network configurations.
Run the Network Configuration Assistant (NetCA).

To start NetCA, click *Start*, *All Program*s, *Oracle*, *Configuration and Migration Tools* then *Net Configuration Assistant*.
Select the '*Directory Usage Configuration*' radio button, then click Next.
Select Directory Type '*Microsoft Active Directory*', then click Next.
Note: The '*Microsoft Active Directory*' configuration option is only available in the Windows version of NetCA.
Select the option to configure the directory for Oracle usage and create the Oracle Schema and Context, then click *Next*.
Enter the Active Directory hostname (cyclops.home.com in my case), then click *Next*.
Select the option to upgrade the Oracle Schema, then click *Next*.

The next page should denote successful Directory configuration i.e.:

> Directory usage configuration complete!
> The distinguished name of your default Oracle Context is:
> cn=OracleContext,DC=home,DC=com

Click *Next*, then click *Finish*.

Due to base Bug 3947653, the message above may only denote partial success i.e.:

> The Assistant is unable to create or upgrade the Oracle Schema
> for the following reason: ConfigException: Oracle Schema creation
> was successful, but Active Directory Display Specifier creation
> failed.oracle.net.config.ConfigException; TNS-04420: Problem
> running LDAPMODIFY

Click *OK*, then click *Finish*.

If you receive the above error, disregard the message and re-run NetCA using the originally supplied values.
The wizard should complete denoting successful Directory configuration i.e.:

> Directory usage configuration complete!
> The distinguished name of your default Oracle Context is:
> cn=OracleContext,DC=home,DC=com

Click *Next*, then click *Finish*.

3.2 Restart the Microsoft Management Console (MMC)

If already open, close then restart the Microsoft Management Console - this is required to refresh snap-in contents.
Click *Start, Run*, enter *mmc*, then click *OK*.

Add the *Active Directory Schema* MMC snap-in to the MMC Console Root.
In the MMC window, select menu option *File*, click *Add/Remove Snap-in*, click *Add*, select *Active Directory Schema*, click *Close*, then *OK*.
Navigate the Classes and Attributes folders noting newly created Oracle attributes and objectclasses that were added (orcl*).

Run the *Active Directory Users and Computers* snap-in - the OracleContext should now be visible under the *DC=home,DC=com* container.

3.3 Grant Write Permission to the OracleContext Container

Having created the OracleContext, grant permissions to users/groups.
Run the *ADSI Edit* MMC snap-in.
Select, then right mouse click *ADSI Edit*.
Click *Connect to ..., Select a well known Naming Context (Domain)*, then click *OK*.
Navigate to, the select the *CN=OracleContext* container under the *DC=home,DC=com* container.
Right mouse click the *CN=OracleContext* container, then click *Properties*.
Click on the *Security tab* then grant write permission to desired users/groups on the OracleContext container.

At this point, the OracleContext may be updated, for example by Net Manager for Directory Naming configuration and/or by Database Configuration Assistant (DBCA) to register databases, after which Oracle Clients may be configured for directory access to resolve service names from the OracleContext within Active Directory.

4. Debugging

Depending on your Active Directory configuration, and whether the above steps were performed

correctly and completely, NetCA will succeed as described or fail.
NetCA provides the ability to perform comprehensive debugging - contact Oracle Support for details of how to debug NetCA.
options '-DTRACING.ENABLED=TRUE' and '-DTRACING.LEVEL=2', also add the '-VERBOSE' option to produce more meaningful, detailed tracing.

For Active Directory related issues, AD Diagnostic Event Logging can be configured.
Refer to Active Directory diagnostic event logging in Windows Server at
http://support.microsoft.com/default.aspx?scid=kb;en-us;314980&sd=tech for details of how to configure.
Enabling logging for Directory Access (8) and DS Schema (24) at level 5 typically provides meaningful and useful output.
Also, review Event Viewer Directory Service messages.

5. References

Compare the Editions of Windows Server 2003
http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx

How to Extend the Schema
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/how_to_extend_the_schema.asp

Disabling Existing Classes and Attributes
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/disabling_existing_classes_and_attributes.asp

Anonymous LDAP operations to Active Directory are disabled on Windows Server 2003 domain controllers
http://support.microsoft.com/default.aspx?scid=326690

Install Windows Support Tools (Windows 2003)
http://technet2.microsoft.com/WindowsServer/en/Library/baa79cdd-83b0-4f10-9356-b2d14462d5b21033.mspx

Adsiedit Overview
http://technet2.microsoft.com/WindowsServer/en/Library/ebca3324-5427-471a-bc19-9aa1decd3d401033.mspx

Data Store Tools and Settings - Data Store Registry Settings
http://technet2.microsoft.com/WindowsServer/en/Library/14d95e79-3a86-4d75-b503-23f1098910e61033.mspx

How to configure Active Directory diagnostic event logging in Windows Server
http://support.microsoft.com/default.aspx?scid=kb;en-us;314980&sd=tech

Note.361528.1: Oracle Clients Cannot Resolve Service Names in AD After OracleContext is Created
https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=361528.1

Note.369514.1:ORA-12154 Testing LDAP Connection in MMC Console with Active Directy 2003
https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=369514.1

Bug 4163362: 10.1.0.4 PATCH SET FOR ORACLE DATABASE SERVER
Bug 4287619: ORACLE 10G 10.1.0.4 PATCH 1 FOR WINDOWS NT, 2000 , XP AND 2003(32 BIT)
Bug 3975572: NETCA FAILS TO CREATE AN ORACLE CONTEXT IN W2003
Bug 3947653: ADDISPLAYSPECIFIERS_*.SBS LOCALE FILES MISSING

.