

Oracle Net Services Configuration With OID

Author: Andy Rivenes
AppsDBA Consulting

Overview

The following will detail the installation of an OID database for use as a directory server for Oracle Net Services. The details will cover Oracle9i version 9.2. Both a Solaris install and a Linux install were performed. Due to issues with the creation of the OID schemas into an existing database, standalone databases were created with the DBCA OID template.

In addition, we migrated the definitions from the 8.0.5 version of Oracle Names to one of the Directory Servers, and then unloaded and reloaded these definitions from the first Directory Server to the other. The eventual goal is to have two directory servers performing replication to stay in sync, and act as high availability Oracle Net Services resolvers.

Pre-Installation

The following pre-installation tasks were performed:

- Oracle 9.2 must be installed with the OID option. The OID database can also be created during this process, or afterward. If the OID database is installed then the OID configuration assistant will be run as well.
- Recommend applying the latest patchset, although no OID components are patched as of 9.2.0.2.

Linux Specific:

- The OID configuration assistant requires korn shell.

Installation

1. Install the OID pre-configured database. This is done through the Database Configuration Assistant (dbca).
2. Run the OID configuration assistant (oidca). This will install the appropriate schemas and start the oidmon and oidlapd processes.

This process will create several database schemas, of which the ODS schema will be used by some of the OID utilities. The default password for the ODS schema is ODS.

A default context will be created and the Oracle Directory Manager will connect to this context through the port(s) defined during the oidca setup. The default non-SSL port

Oracle Net Services Configuration With OID

is 389 and the default SSL port is . We used 4032 and 4031 respectively. The Oracle context is "cn=orcladmin" with a password of "welcome".

Configuration

Configuration consists of running three Oracle utilities. Note: there are command line utilities to perform many additional functions as well.

The Oracle Directory Manager GUI is used to administer the Directory Server. Access is performed through the "Super-User DN" which is "cn=orcladmin" by default. The default password is "welcome" (the Oracle documentation states that it is "welcome1").

The Oracle Net Services administration is performed with the Net Configuration Assistant to create the initial client configuration files (e.g. ldap.ora and sqlnet.ora) and then Net Administrator is used to manage the actual Network connection definitions.

Existing network definitions were unloaded from the Oracle Names server(s) and then moved between the two active Directory Servers.

Unload Existing Network Definitions

Existing network definitions existed in a Version 8.0.5 Oracle Names infrastructure. Oracle introduced a "dump_ldap" command in Oracle8i Oracle Names, and since there were 8i tools available we were able to successfully dump the Oracle Names definitions from the 8.0.5 repository using the 8i Oracle Names tools.

The resulting file had to be edited and spurious dc= parameters removed from some of the dn: lines. An example follows:

```
dn: cn=hc_prd1,dc=world,dc=°ÿ
objectclass: top
objectclass: orclNetService
cn: hc_prd1
orclNetDescString:
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521))(CONNECT_DATA=(SID=hc_prd1)(Server=Dedicate
d)))
```

This was changed to:

```
dn: cn=hc_prd1,dc=world
objectclass: top
objectclass: orclNetService
cn: hc_prd1
orclNetDescString:
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521))(CONNECT_DATA=(SID=hc_prd1)(Server=Dedicate
d)))
```

Once this was accomplished, the resulting file was loaded into the Directory Server with the command:

Oracle Net Services Configuration With OID

```
$ORACLE_HOME/bin/ldapadd -p 4032 -h oiddb-1 -D cn=orcladmin -w welcome \  
-f onet.ldi
```

Move Network Definitions Between Directory Servers

Existing Oracle Net Services definitions can be unloaded from a Directory Server as a subtree. Since the existing tree structure was of the form “cn=<Net Service definition>,cn=OracleContext,dc=company,dc=com” the following command was used to unload the subtree:

```
/oracle$ ldifwrite -c oidt1 -b "cn=OracleContext,dc=company,dc=com" -f onet.ldi  
This tool can only be executed if you know database user password for OiD  
Enter OiD Password ::  
/oracle$
```

Due to a bug in the Oracle software, a korn shell script had to be run to strip spurious entries (see Note: 130752.1) and then the result was loaded using the ldapmodify command. Unfortunately there is a default ldapmodify command in the /usr/bin directory, so the script had to be further modified to append \$ORACLE_HOME/bin to each of the ldap commands.

OID Database Password Utility

The OID utility “oidpasswd” must be used to change the ODS and ODSCOMMON database user passwords. OID encrypts the ODSCOMMON password and stores it in a file. This is then used by the OID processes to connect to the OID database server (for additional details see the Oracle Note: 204900.1).

Example usage:

```
$ $ORACLE_HOME/bin/oidpasswd connect=oiddb1  
current password: ods  
new password: newsupersecret  
confirm password: newsupersecret  
password set.  
$
```

OID Database Statistics Collection Tool

The OID utility “oidstats.sh” tool is used to analyze the ODS database schema to estimate statistics. The tool prompts for the ODS database user password and should be run whenever significant changes in the directory data occur.

Example:

Oracle Net Services Configuration With OID

```
$ORACLE_HOME/ldap/admin/oidstats.sh -connect oiddb1 -all
```

Note: The script will prompt for the ODS password.

Administration

Background

Access to OID services is performed through an LDAP server which runs as one or more “oidlapd” processes. Connections can be made through a non-SSL or an SSL port. Startup of the oidlapd process(es) involves starting a monitor process (e.g. oidmon) which then queries the OID database server to determine whether to start or stop the oidlapd process(es). To startup or shutdown the oidlapd processes involves running the oidctl utility. This utility updates the database with the desired state, and it is the oidmon process that actually starts or stops the oidlapd process(es).

Setup

The following entry should be added to the “oratab” file. This allows dbcontrol to start or stop the OID processes.

```
#LDAP:<${ORACLE_HOME}>:<db server>:<oidldapd|oidrepld>:<instance>:<configset>
```

Where:

- <\${ORACLE_HOME}> - The ORACLE_HOME of the OID installation
- <db server> - The database with the OID schemas (currently sets ORACLE_SID)
- <oidldapd|oidrepld> - Specifies which server to start (both requires two entries)
- <instance> - The instance number for the OID server, defaults to 1
- <configset> - Configuration set to be used, defaults to 0

Startup

To start the OID server the “oidmon” process must be started. This process actually starts and stops the OID process(es).

```
oidmon connect=<db server> start
```

To start the OID processes (this just updates the database which is why the oidmon process must be running):

```
oidctl connect=<db server> server=<oidldapd|oidrepld> instance=<0-1000> configset=<0-1000> start
```

Oracle Net Services Configuration With OID

Example:

```
oidmon connect=oiddb1 start  
oidctl connect=oiddb1 server=oidldapd instance=1 configset=0 start
```

Shutdown

To shutdown the OID server process(es) the oidmon process must be running, so the oidctl command must be run first, and then the oidmon process must be given enough time to recognize the state change and shutdown the process(es) (Note: the dbcontrol utility does this).

```
oidctl connect=<db server> server=<oidldapd|oidrepld> instance=<0-1000> stop
```

```
oidmon connect=<db server> stop
```

Example:

```
oidctl connect=oiddb1 server=oidldapd instance=1 stop  
oidmon connect=oiddb1 stop
```

Oracle Net Services Configuration With OID

Appendix A. Network Configuration Files

ldap.ora

```
# LDAP.ORA Network Configuration File: d:\oracle\ora920\network\admin\ldap.ora
# Generated by Oracle configuration tools.

DEFAULT_ADMIN_CONTEXT = "dc=company,dc=com"

DIRECTORY_SERVERS= (oiddb-1.company.com:4032:4031)

DIRECTORY_SERVER_TYPE = OID
```

sqlnet.ora

```
# SQLNET.ORA Network Configuration File: d:\oracle\ora920\network\admin\sqlnet.ora
# Generated by Oracle configuration tools.

NAMES.DEFAULT_DOMAIN=company.com

# Windows authentication - comment out if on UNIX
SQLNET.AUTHENTICATION_SERVICES=(NTS)

NAMES.DIRECTORY_PATH=(LDAP)
```

Oracle Net Services Configuration With OID

Appendix B. LDI Fix Script

```
#!/bin/ksh
#
# fix ldifwrite file so it can be loaded into an existing OID database
#
print "Removing Offending Entries"
#
egrep -v "orclguid|creatorsname|modifiersname|createtimestamp|modifytimestamp" onet.ldi > new.ldif
#
print "Removing Offending Entries"
#
$ORACLE_HOME/bin/ldapmodify -a -c -p 4032 -h oiddb-1 -D cn=orcladmin -w welcome -v -f ./new.ldif
#
print "Retrieve the New Entries"
#
$ORACLE_HOME/bin/ldapsearch -p 4032 -h oiddb-1 -b "" -v objectclass=*
```

Oracle Net Services Configuration With OID

References

Oracle9i Directory Service Integration and Deployment Guide, Release 2 (9.2), Oracle Corporation, Part No. A96579-01

Oracle Internet Directory Administrator's Guide, Release 9.2, Oracle Corporation, Part No. A96574-01

Oracle9i Net Services Administrator's Guide, Release 2 (9.2), Oracle Corporation, Part No. A96580-01

Oracle9i Net Services Reference Guide, Release 2 (9.2), Oracle Corporation, Part No. A96581-01

Note: 209613.1, *How to recreate the OID directory schema*, Oracle Corporation, 11-Sep-2002

Note: 191587.1, *Link Phase Fails for 'ins_ctx.mk' While Installing Oracle Server 9.2.0.1 on Linux*, Oracle Corporation, 11-Nov-2002

Note: 204900.1, *What oidpasswd Does And The Objects It Modifies*, Oracle Corporation, 04-Dec-2002

Note: 130752.1, *Constraint problems using ldapadd to load complete directory from ldifwrite*, Oracle Corporation, 16-Jun-2002

Note: 157761.1, *Loading a LDIF file created with ldifwrit*, Oracle Corporation, 30-Nov-2001

Note: 163251.1, *ldapadd fails on Unix with ldap_sasl_interactive_bind_s: No Such Attribute*, Oracle Corporation, 13-SEP-2002

Note: 170049.1, *Error "ldap_add: Insufficient access" when adding new entries*, Oracle Corporation, 24-JUN-2002

Note: 155790.1, *Troubleshooting Start/Stop of Oracle Internet Directory*, Oracle Corporation, 20-AUG-2002