DIRECTORY NAMING MIGRATION - NEW FEATURES AND A CASE STUDY

David Chen, Oracle
Isobel Eckhardt, Boeing
*Vinay Khandelwal, Oracle*
Ed Meador, Boeing

ABSTRACT

This technical white paper first gives an overview of Oracle Net Services Directory Naming and several new features in 9i. It then illustrates the deployment scenarios, migration procedures from Oracle Names and TNSNAMES.ORA file to Directory Naming, and a Boeing Company case study. The paper finally concludes with a strong recommendation to move to Directory Naming to take advantage of superior features in Oracle9i.

DIRECTORY NAMING OVERVIEW

An LDAP directory service provides a centralized vehicle for managing and configuring distributed, heterogeneous networks. The directory becomes the central repository for all "meta-data" about databases, network components, user and corporate policies and preferences, replacing localized files on the clients and servers themselves. Administrators (or those they delegate to) can then manage these objects in one directory; all systems on the heterogeneous network can refer to a single directory for needed location, authentication, and authorized user information. LDAP stands for lightweight directory access protocol, which requires a very minimal amount of networking software on the client side, making it particularly attractive for Internet based, thin-client applications.

LDAP has been available with Oracle8i and later versions. Oracle Net Services, Oracle's networking functionality, supplies a Directory Naming solution that is the industry's most comprehensive, enterprise-wide data access solution for complex computing environments.

Oracle Net Services Directory Naming is the process of resolving a net service name using Oracle Internet Directory (OID), an LDAP-compliant directory service. Directory Naming allows net service names to be stored in and retrieved from OID. Net service names stored in such a directory are accessible by any client machine in the network as long as the client has sufficient access privileges. An explanation of Directory Naming working process is shown below:
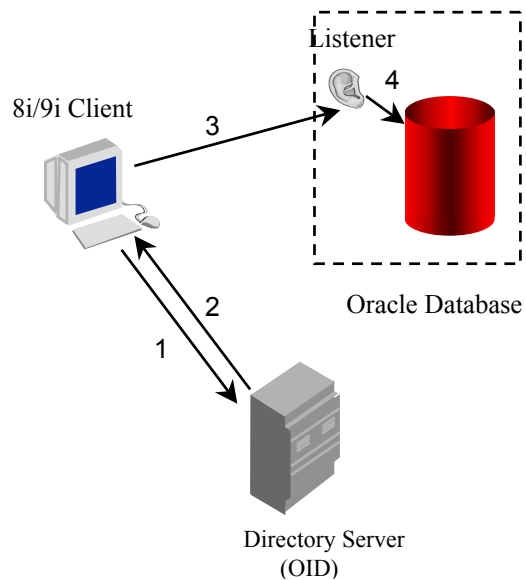
1) A client initiates a connect request providing a connect identifier (e.g., sales.us.oracle.com).

2) The connect identifier is resolved to a connect descriptor (e.g., port number, host name, protocol, service_name, …) by a directory server, e.g., OID, and is sent back to the client.

3) The client makes the connect request to the address provided in the connect descriptor, which typically is a listener's address.

4) The listener then receives the request and directs it to the database server.

Figure 1. Directory Naming Working Process

The centralized network names and addresses of Oracle Net Services Directory Naming facilitate easy administration of new information and updates. It eliminates the need for an administrator to make changes to a large number of clients. This centralized naming feature makes network changes transparent to users and client applications on several different levels such as location transparency and containment transparency.

LOCATION TRANSPARENCY

Using Directory Naming lets administrators hide the details of a service's network location from client applications. All the client needs to know is the network-wide name assigned to the service. Oracle Net Services takes care of resolving this service name into a service address at connect time.

CONTAINMENT TRANSPARENCY

Containment transparency refers to how easily server resources can be moved without requiring changes to client applications. With Directory Naming, services can be relocated from one server platform to another with a minimum of disruption and downtime for administration. A change may only need to be made once in the central repository to reflect the new location of the service. No changes to client configuration files or applications are necessary. This makes "right-sizing" of applications easier by allowing administrators to stage services on the correct platform.

NEW FEATURES

In Oracle9i, several new features have been added into Directory Naming, which enhance its functionality significantly. These new features are summarized as below:

- Improvements in Oracle Net Manager and Oracle Net Configuration Assistant ease directory configuration and management considerably. Oracle Net Configuration Assistant allows administrators to create multiple entries of OracleContext that stores Oracle databases and net service names. Oracle Net Manager allows administrators to change the default naming context so that all the information under different naming context can be viewed and edited. These improvements facilitate an easier management of a complex hierarchical naming structure.

- Oracle Names LDAP Proxy enables customers to migrate seamlessly from Oracle Names to Directory Naming. The proxy allows Oracle Names client machines to continue connecting to the same Oracle Names server now acting as a proxy loading data from an OID. Only one system, therefore, needs to be maintained during the migration period. This feature is especially useful for those customers having large number of Oracle Names client machines deployed. It would otherwise not be possible to configure thousands of client machines to have LDAP capability simultaneously. This is a new feature in Oracle9i Release1.

- Oracle Net Services Aliases Support: Oracle Net Services Aliases, the alternative service names for any defined net service name or database service, can be stored in an OID server today to allow clients to use the alternatives connecting to the databases. With aliases support, if a net service name or database service's information changes, the information only needs to be updated in one place, the original service name registration. The administrators can create, modify, and delete aliases through Oracle Net Manager. This is a new feature of Oracle9i Release2.

- Global database links support: The existing global database links in Oracle Names servers will be able to be migrated from Oracle Names servers, and will be supported in Directory Naming. However, authentication (user names/passwords) of global database links, if it is set up in Oracle Names, will not be supported in Directory Naming, due to the fact that this is not a common used feature and does not meet today's security requirement. This is also an Oracle9i Release2 feature.

PRODUCT DIRECTIONS

Without LDAP support, Oracle network configuration requires the existence of configuration files such as TNSNAMES.ORA and SQLNET.ORA in each client site; in addition to these files, the server site requires files of LISTENER.ORA, CMAN.ORA, and etc. Thus, when a new database system is configured, it has to be done locally, and the database information needs to be updated in each of the client sites that will need to access to the new database. Oracle's support of LDAP directory services, on the other hand, will enable remote configuration and easier maintenance. An administrator will therefore be able to configure a remote listener or install a service/instance on a remote node. These client site configuration files will be eliminated eventually.

In a future release, Oracle client profiles will be stored in an OID server to facilitate Web access and remote administration. The profiles will be able to be shared across multiple systems and users. As a result, SQLNET.ORA file will be eliminated from individual clients' nodes. Oracle's directory profiles can be one of the following: a) machine-specific, b) application-specific and c) service- or group-specific. In addition to directory profiles, an application can choose to retain a local profile (actually the same old SQLNET.ORA) that will be stored locally on its machine.

Oracle's current LDAP support still requires installing an LDAP.ORA file on each client site in order to identify LDAP directory server's location, i.e., host name and port number. In a future release, Oracle client will be able to discover the location of OID server running in a given enterprise. As a result, the client site will not need to maintain the LDAP.ORA file, which will reduce the administrative cost of maintaining the clients in large deployments.

LDAP directory based centralized management and configuration is our direction. Oracle Net Services will provide both a centralized configuration and management for the entire network, including net service name, listeners, profiles, and connection manager. Oracle Names will be obsolete in Oracle10i time frame.

In Oracle9i, Oracle Net Services supports both OID and Microsoft Active Directory. However, in a future release, e.g., 10i and beyond, Oracle Net Services will only support OID directly. Any other third party directory (e.g., Netscape Directory Server) will need to either migrate to OID, or to deploy Oracle Directory Integration platform, which enables you to synchronize various directories with OID.

THE MIGRATION

In order to explore superior features of Oracle Net Service Directory Naming, Oracle strongly recommends to migrate from Oracle Names and TNSNAMES.ORA file to Directory Naming. **Oracle9i is the terminal release of Oracle Names.**

There are several areas needed to be considered when migrating to LDAP Directory Naming:

TOPOLOGY DESIGN

The directory service's topology describes the way an organization divides its directory tree aiming physical servers and how it allocates those servers among the organization's physical locations. Making good choices about directory topology will help it achieve the best possible performance for its directory-enabled applications, increase directory availability, and better manage the directory.

Depending on the company's IT structure, responsibility distribution, and speed/traffic of different locations in the physical network, an organization can have several different topology designs. Oracle Names customers can replicate the domain structure used in Oracle Names, or can develop an entirely different one depending on the company's needs. In order to simplify the migration procedure, Oracle recommends redesigning the topology prior to the migration in Oracle Names. It can be done after the migration in LDAP directory server, however, if required.

Below is an example of acme.com's topology. The hierarchical directory tree of acme.com is divided into three sub-domains of US, UK, and Canada, but they are all within one single directory server. A multiple registry like cn=sales is allowed, under dc=us and dc=ca respectively in this case. The administration responsibility can be divided into these three areas. Please note the entry of cn=OracleContext is required to create and store all Oracle objects. Choosing the location of cn=OracleContext depends on how the directory tree is managed.
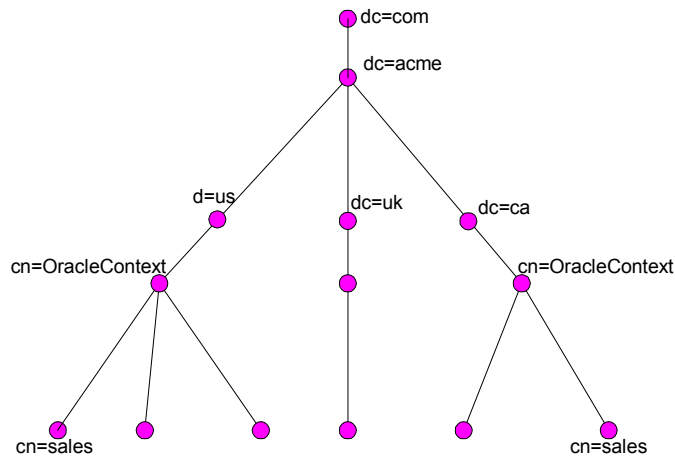
Figure 2: An Example of Directory Information Tree (DIT)

ORACLE NAMES MIGRATION

There are two ways when migrating from Oracle Names to Directory Naming:.

Method 1: Migrate directly without using Oracle Names LDAP Proxy.

The following tasks are required:

1. Create Oracle Contexts. Oracle Net Configuration Assistant enables administrators to create an entry called cn=OracleContext to store all Oracle objects.

2. Obtain list of objects to export: NAMESCTL utility offers three commands to help with this task: LIST_DOMAINS, LIST_DELEGATED, and LIST_OBJECTS.

3. Export objects to a directory server: The NAMESCTL utility exports network objects into the directory with the DUMP_LDAP command, which enables administrators to export the objects to an LDIF file or directly into an OID server. This command allows administrators to export to either a similar DIT or a dissimilar DIT in OID.

4. Configure clients to talk to OID server instead of Oracle Names server: Pre-Oracle8i clients will first need to be upgraded to 8i or a later version. The administrator will then need to choose LDAP instead of Oracle Names in the naming method panel, and follow the wizard in the Oracle Net Configuration Assistant tool

Method 2: Using Oracle Names LDAP Proxy.

It often is a huge challenge for customers having a large number of pre-Oracle8i clients to migrate because too many client machines would have to be configured simultaneously. To address this challenge, Oracle Net Services provides Oracle Names LDAP Proxy in Oracle9i, which allows pre-Oracle8i clients to communicate to Oracle Names servers as before. The Oracle Names servers will be acting as proxies to talk to the OID server. Only one data system will need to be maintained, and customers can update the old clients gradually.

In the case of using Oracle Names LDAP Proxy, the steps below need to be followed:

1. Upgrade Oracle Names Servers to Oracle9i Release1 or Oracle9i Release2. Releases prior to Oracle9iR1 do not support this new feature.

2. Start Oracle Names Servers by using Oracle Net Manager, which creates CKPPTOP.ORA file that will be used by the proxy.

3. Populate the OID server, which is the same as steps 1 – 3 in method 1.

4. Configure Oracle Names Servers as proxies by using Oracle Net Manager.

Please note, no client configuration is required if using Oracle Names LDAP Proxy.

If the Oracle Names structure has multiple administrative regions, Oracle Corporation recommends mirroring the current Oracle Names domain structure in the directory DIT structure. Using a different topology structure requires modifying the topology defined for the Oracle Names LDAP Proxy servers. Topology modification is not supported if using the proxy.

LOCAL NAMING MIGRATION

When customers migrate from local naming to Directory Naming, the following steps are required:

1. Create Oracle Contexts. Oracle Net Configuration Assistant enables administrators to create an entry called cn=OracleContext to store all Oracle objects. This can be done either during the installation or after the installation.

2. Export TNSNAMES.ORA file to OID server, using the Directory Server Migration Wizard provided in Oracle Net Manager.

3. Configure this client to use Directory Naming instead of local TNSNAMES.ORA file using Oracle Net Manager, which will generate SQLNET.ORA. and LDAP.ORA files.

4. Configure other local naming clients to use Directory Naming by using Oracle Net Manager, or by distributing the new SQLNET.ORA and LDAP.ORA files.

A CASE STUDY

Boeing's enterprise wide implementation of Oracle Names has been in production for more than two years, and there are some areas at Boeing still using tnsnames.ora. The current plan is to migrate to Directory Naming in Oracle9i Release2. Boeing is now testing Oracle Net Services and OID of Oracle9i Release1 including OID replication on the AIX 4.3.3 platform.

Reasons for migrating include: Oracle Names is proprietary and the terminal release is 9i; Oracle Names has no built in security which requires using a Boeing written customized interface; Security is being addressed in Directory Naming and OID.

CURRENT ENVIRONMENT

Approximately 3000 databases are registered in Oracle Names with versions ranging from Oracle7.3.4 to Oracle9i. The Oracle Names servers are running on AIX 4.3.3 using Oracle 8.1.7.2 and HP UX 11 using Oracle 8.0.6 and 8.1.7.2. There are 18 Oracle Names servers using a two level hierarchy for region autonomy, with each region having at least two name servers for failover. Generic Oracle Name DNS aliases have been assigned to hosts so Oracle Names servers can be moved without impact. The alias feature, which will be available in Oracle9i Release2 Directory Naming, is used for common systems across regions and to establish application independence from particular database instances. Oracle Names entries are maintained using a customized script written at Boeing for providing access control, modification logs, history tables, and queries with wildcards.

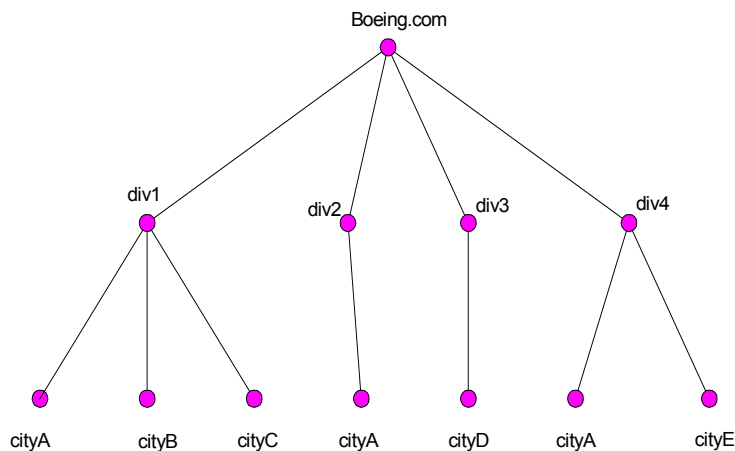The following is the hierarchical structure of Oracle Names at Boeing.

Figure 3: Boeing's Oracle Names Domain Structure

MIGRATION PROCEDURE

The Boeing's Oracle Names and OID/LDAP technical team meets weekly via teleconference for planning, reviewing status and resolving any issues. The migration plan is as follows:

1. OID server installation: Installation of OID 9i with replication support on multiple AIX 4.3.3 64 bit nodes. Gain expertise in directory naming and OID.

2. Replicate existing hierarchical structure of Oracle Names in the OID, and create cn=OracleContext under each region. The DIT in the OID looks as below:
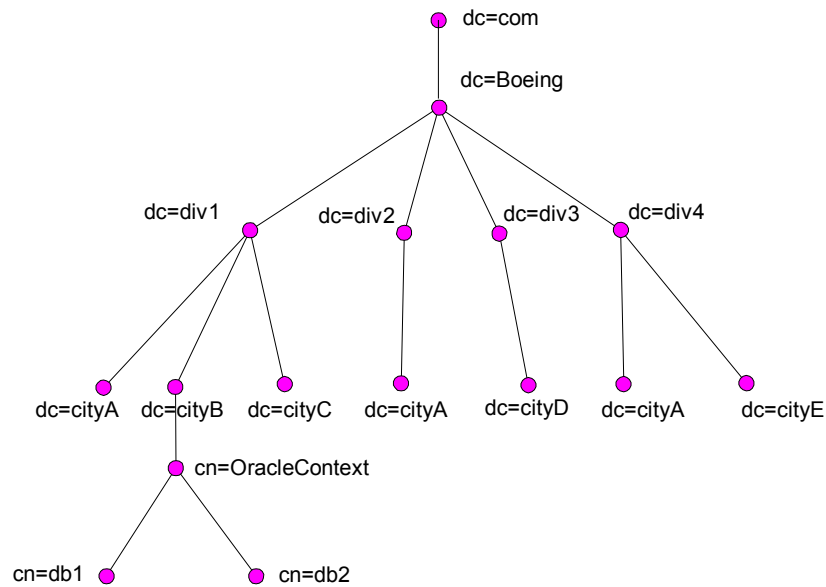
Figure 4: Boeing's DIT post migration

3. Upgrade Oracle Names servers to Oracle9i.

4. Set up test Oracle Names LDAP Proxy Servers.

5. Migrate sample data from Oracle Names servers to the OID server.

6. Test thoroughly, including the configuration of some clients to use the test proxy for naming resolution.

7. Gain expertise and develop automated procedures to maintain at least the level of functionality, security, performance, ease of use and reliability now provided by Oracle Names. Understand structure of tables underlying ODS schema (62 tables versus 4 in Oracle Names).

8. Wait until Oracle Net Services Alias support feature is available in Oracle9i Release2 before going production, and develop automated procedure to migrate Oracle names aliases. Thoroughly test and gain expertise in 9i Release2.

9. Before production environment migration have a backup system in place. Provide ample notification of schedule and issues to all users.

10. Configure Oracle Names servers in production to be proxies. No configuration changes will be required for clients at this time. Proxies will continue to be a requirement for those clients accessing pre 8i databases. Other clients can begin switching over to the Directory Naming configuration.

CHALLENGES AND EXPERIENCES

The basic procedures for migration as described in this paper have been tested successfully. The main challenge has been a steep learning curve. Oracle will be providing a hands-on directory naming migration class which will be very helpful. The primary challenge besides providing production support is to integrate with other LDAP projects at Boeing such as single sign-on.

The joint Boeing and Oracle technical team would like to share some of their experiences and lessons learned:

1. Support from senior management is of utmost importance for a project of this scope. The large number (3000) of Oracle databases in the Boeing Company made the benefits of a central naming repository obvious to management.

2. It is crucial to have a well thought plan for testing, migration and deployment; it is important for the project team to meet on regular basis to discuss the status and resolve any technical issues in a timely manner.

3. In order to simplify administration of the LDAP servers, a set of shell scripts were created that call a custom script to set common environment variables. This helps in eliminating repetitive retyping of host, port number, connection service name, etc. and also ensured accuracy when switching from one server to another.

4. For Oracle Naming, the DBCA tool gives the option to register databases. This is different from registering a net service names and Boeing is not planning on using this feature now.

5. The default security mechanism at Directory Naming and OID allows any member of OracleNetAdmins in a given OracleContext to manage all net service and database names under that OracleContext. Boeing would like to have more granular access control for its DBAs. Oracle is going to provide an interim solution for Boeing in Oracle9i Release2 and will provide tighter access control in a later release.

CONCLUSION

Oracle Net Services Directory Naming has been provided starting from Oracle8i Release2. LDAP is the clear direction for Oracle databases networking management and configurations. Oracle9i takes a great step forward by enhancing several features in Directory Naming, which is expected to reduce customer's TCO significantly. In order to take advantage of these superior features, Oracle strongly recommends that customers migrate from Oracle Names and TNSNAMES.ORA file to Directory Naming at the first opportunity. The functionality provided in Oracle9i facilitates a seamless and easy migration. [NOTE]

Note: The Boeing team contributes to the section of "A Case Study" only, therefore, the Boeing Company has no responsibility for the statements in any other sections of this white paper.