Oracle® Identity Management

User Reference

10*g* (10.1.4.0.1)

B15998-01

July 2006

ORACLE®

Oracle Identity Management User Reference, 10*g* (10.1.4.0.1)

B15998-01

Primary Author: Sumit Jeloka

Contributing Authors: Ellen Desmond, Don Gosselin, Richard Smith

Contents

4 Oracle Internet Directory Data Management Tools

5 Oracle Internet Directory Replication Management Tools

6 Oracle Directory Integration Platform Tools

8 Object Class Reference

9 Attribute Reference

List of Tables

Preface

The *Oracle Identity Management User Reference* provides reference information about the command-line tools and LDAP directory schema elements for Oracle Identity Management. This Preface contains the following topics:

Audience

Oracle Identity Management User Reference is intended for anyone who performs administration tasks for Oracle Identity Management components. You should be familiar with either the UNIX operating system or the Microsoft Windows operating system in order to understand the command-line syntax and examples. You also must be familiar with the **Lightweight Directory Access Protocol (LDAP)**.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following manuals in the Oracle Identity Management 10*g* (10.1.4.0.1) documentation set:

- *Oracle Identity Management Concepts and Deployment Planning Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Identity Management Guide to Delegated Administration*
- *Oracle Identity Management Integration Guide*
- *Oracle Identity Management Application Developer's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Command-Line Tool Reference

Part 1 of the *Oracle Identity Management User Reference* contains information about the command-line tools for Oracle Identity Management.

Part I contains the following chapters:

1

Command-Line Tools Overview

This chapter provides an overview of all of the command-line tools available for Oracle Identity Management. It contains the following topics:

Configuring Your Environment

Before you begin using the Oracle Identity Management command-line tools, you must configure your environment. This involves setting the appropriate environment variables. Also, if you will be running commands from a Microsoft Windows machine, you will need to install UNIX emulation software. See the following sections for more information:

Setting Environment Variables

The syntax and examples provided in this guide require that you have the following environment variables set:

- `ORACLE_HOME` - The location of your Oracle Identity Management installation.
- `ORACLE_SID` - The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in *`$ORACLE_HOME`*`/network/admin`.
- `NLS_LANG` (*`APPROPRIATE_LANGUAGE`*`.AL32UTF8`) - The default language set at installation is `AMERICAN_AMERICA`.
- `PATH` - The following directory locations should be added to your `PATH`:

  $*`ORACLE_HOME`*`/bin`

  $*`ORACLE_HOME`*`/ldap/bin`

  $*`ORACLE_HOME`*`/ldap/admin`

  $*`ORACLE_HOME`*`/opmn/bin`

UNIX Emulation Utilities for Windows

To run shell script tools on the Microsoft Windows operating system, you need one of the following UNIX emulation utilities:

- Cygwin 1.3.2.2-1 or later. Visit: `http://sources.redhat.com`
- MKS Toolkit 6.1. Visit: `http://www.datafocus.com/`

Oracle Identity Management Command-Line Tool Categories

The Oracle Identity Management command-line tools are organized into the following categories:

- Oracle Identity Management Server Administration Tools
- Oracle Internet Directory Database Administration Tools
- Oracle Internet Directory Data Management Tools
- Oracle Internet Directory Replication Management Tools
- Oracle Directory Integration Platform Tools

Oracle Identity Management Command-Line Tool List

The following table lists all of the Oracle Identity Management command-line tools in alphabetical order and gives a brief description of each tool.

Table 1–1 Oracle Identity Management Command-Line Tool List

Command	Tool Name	Description
bulkdelete	Bulk Deletion Tool	Used to efficiently delete a subtree from a directory.
bulkload	Bulk Loading Tool	Used to load a large number of entries into a directory server.
bulkmodify	Bulk Modification Tool	Used to modify a large number of existing entries in an efficient way.
catalog	Catalog Management Tool	Used to update the indexed attributes for a directory.
dipassistant	Directory Integration Platform Assistant	Used to administer the Oracle Directory Integration Platform server
hiqpurge.sh	Human Intervention Queue Purge Tool	Used to move a replication change from the human intervention queue to the purge queue.
hiqretry.sh	Human Intervention Queue Retry Tool	Used to move a replication change from the human intervention queue to the retry queue.
ldapadd	LDAP Data Add Tool	Used to add entries, their object classes, attributes, and values to the directory. This command is compliant with IETF (Internet Engineering Task Force) standards.
ldapaddmt	Multithreaded LDAP Data Add Tool	Used to add entries, their object classes, attributes, and values to the directory using multiple threads. This command is compliant with IETF standards.

Table 1–1 (Cont.) Oracle Identity Management Command-Line Tool List

Command	Tool Name	Description
ldapbind	Authentication Validation Tool	Used to see whether you can authenticate a client to a server. This command is compliant with IETF standards.
ldapcompare	Attribute Comparison Tool	Used to compare an attribute value that you specify on the command line to the attribute value in a directory entry. This command is compliant with IETF standards.
ldapdelete	LDAP Data Deletion Tool	Used to remove entries from the directory. This command is compliant with IETF standards.
ldapmoddn	LDAP DN/RDN Modification Tool	Used to change the RDN of an entry, or to move an entry to a new parent node in the directory tree. This command is compliant with IETF standards.
ldapmodify	LDAP Data Modification Tool	Used to add, delete, or replace attributes for entries by supplying an LDIF file as input. You can also delete or add entries. This command is compliant with IETF standards.
ldapmodifymt	Multithreaded LDAP Data Modification Tool	Used to add, delete, or replace attributes for entries in multi-threaded mode. This command is compliant with IETF standards.
ldapsearch	LDAP Search Tool	Used to search for and retrieve specific entries in the directory. This command is compliant with IETF standards.
ldifmigrator	Data Migration Tool	Used to convert LDIF files output from other directories or application-specific repositories into a format recognized by Oracle Internet Directory.
ldifwrite	Data Export Tool	Used to convert to LDIF all or part of the information residing in an Oracle Internet Directory.
odisrv	Oracle Directory Integration Server Control	Used to start a standalone Oracle Directory Integration Platform server.
odisrvreg	Oracle Directory Integration Platform Server Registration	Used to register an Oracle Directory Integration Platform server with Oracle Internet Directory.
oidca	Oracle Internet Directory Configuration Assistant	Used to create, upgrade, or delete an Oracle Context in Oracle Internet Directory or to configure the `ldap.ora` file.
oidctl	Oracle Internet Directory Control	Used to start, stop, or restart Oracle Identity Management server instances (Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Replication).
oiddiag	Oracle Internet Directory Server Diagnostic Tool	Used to collect diagnostic information about Oracle Internet Directory and output it to a file.
oidmon	Oracle Internet Directory Monitor	Used to initiate, monitor, and terminate Oracle Internet Directory server processes.
oidpasswd	Oracle Internet Directory Database Password Utility	Used to change the password, create a wallet, or unlock the super user account for the Oracle Internet Directory database.

Table 1–1 (Cont.) Oracle Identity Management Command-Line Tool List

Command	Tool Name	Description
oidpasswd	Oracle Internet Directory Database Password Utility	Used to change the password for the Oracle Internet Directory database, or to create a wallet for the database password and replication server password.
oidprovtool	Provisioning Subscription Tool	Used to create and manage provisioning integration profiles for applications.
oidcmprec	Compare and Reconcile Tool	Used to compare and reconcile one Oracle Internet Directory with another.
oidstats.sql	Oracle Internet Directory Database Statistics Collection Tool	Used to analyze the various Oracle Directory Server (ODS) database schema objects to estimate the statistics.
opmnctl	Oracle Process Manager and Notification Server Control	Used to manage Oracle Application Server components in an integrated way. This tool can be used to start the Oracle Internet Directory server, Monitor process, and database.
remtool	Replication Environment Management Tool	Used to set up and configure directory replication groups (DRG).
schemasync	Schema Synchronization Tool	Used to synchronize the schema between Oracle Internet Directory and a third-party directory.
stopodiserver.sh	Oracle Directory Integration Server Stop Command	Used to stop a standalone Oracle Directory Integration Platform server.
upgradecert.pl	Certificate Upgrade Tool	Used to update user certificates stored in the directory that were issued before Release 10.1.2.

Oracle Identity Management Command-Line Tool Common Tasks

The following table lists the common tasks that you can perform with the Oracle Identity Management command-line tools and the associated tool name.

Table 1–2 Task List for Oracle Identity Management *Command-Line Tools*

Task	Tool Name
Adding a New Node to an Oracle Database Advanced Replication-based DRG	remtool
Adding a Partial Replica to a DRG	remtool
Adding a Read-Only Replica to a DRG	remtool
Adding Concurrent Entries to the Directory Using an LDIF File	ldapaddmt
Adding Data to the Directory Using a DSML File	ldapadd
Adding Data to the Directory Using an LDIF File	ldapadd
Adding the Metadata of a Pilot Replica to a Master Replica	remtool
Backing Up the Metadata of a Pilot Replica to an LDIF File	remtool
Beginning Pilot Mode for a Replica	remtool
Bootstrapping a Directory Using a Configuration File	dipassistant
Bootstrapping a Directory Using a Synchronization Profile	dipassistant

Table 1–2 (Cont.) Task List for Oracle Identity Management ***Command-Line Tools***

Task	Tool Name
Changing the Password for the Oracle Directory Integration Platform Administrator	dipassistant
Changing the Password to the Oracle Internet Directory Database	oidpasswd
Changing the Password to the Oracle Internet Directory Database	oidpasswd
Changing the RDN of an Entry	ldapmoddn
Changing the Replication Administrator Password for an Advanced Replication-based DRG	remtool
Changing the Replication DN Password in the Oracle Internet Directory Wallet	remtool
Changing the Replication DN Password Used for LDAP-Based Replication	remtool
Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup	remtool
Cleaning Up an Oracle Database Advanced Replication-based DRG Setup	remtool
Collecting All Diagnostic Information	oiddiag
Collecting Selected Diagnostic Information	oiddiag
Comparing Attribute Values for an Entry	ldapcompare
Comparing and Reconciling Entire Directories	oidcmprec
Comparing and Reconciling Individual Entries in Two Directories	oidcmprec
Comparing and Reconciling Subtrees in Two Directories	oidcmprec
Configuring the ldap.ora File	oidca
Converting a Partial Naming Context to an LDIF File	ldifwrite
Converting All Entries under a Naming Context to an LDIF File	ldifwrite
Converting an Oracle Context to an Oracle Identity Management Realm	oidca
Creating a New Synchronization Profile	dipassistant
Creating a New Synchronization Profile Using an Existing Profile as a Template	dipassistant
Creating a Provisioning Profile	oidprovtool
Creating an Oracle Context	oidca
Creating an Oracle Database Advanced Replication-based DRG	remtool
Creating Wallets for Oracle Internet Directory Database and Oracle Directory Replication Server Passwords	oidpasswd
Creating Wallets for Oracle Internet Directory Database and Oracle Directory Replication Server Passwords	oidpasswd
Completely Deleting All Entries in a Naming Context	bulkdelete
Deleting a Provisioning Profile	oidprovtool
Deleting a Read-Only Replica from a DRG	remtool
Deleting a Single Entry	ldapdelete
Deleting a Synchronization Profile	dipassistant
Deleting an Oracle Context	oidca

Table 1–2 (Cont.) Task List for Oracle Identity Management ***Command-Line Tools***

Task	Tool Name
Deleting Multiple Entries Using an LDIF File	ldapdelete
Detecting and Correcting Errors in an Oracle Database Advanced Replication DRG Setup	remtool
Detecting Errors in an Oracle Database Advanced Replication DRG Setup	remtool
Disabling a Provisioning Profile	oidprovtool
Discarding a Range of HIQ Change Logs	hiqpurge.sh
Discarding a HIQ Change Log	hiqpurge.sh
Discarding all HIQ Change Logs from a Supplier	hiqpurge.sh
Displaying Errors for an Advanced Replication-based DRG	remtool
Displaying Queue Statistics for an Advanced Replication-Based DRG	remtool
Ending Pilot Mode for a Replica	remtool
Generating Change Logs	oidcmprec
Including and Excluding Attributes	oidcmprec
Indexing a Single Attribute	catalog
Indexing Multiple Attributes	catalog
Loading and Reconciling Data Using the Data Migration Tool	ldifmigrator
Loading Data for Multiple Nodes in a Replicated Environment	bulkload
Loading Data in Bulk Mode	bulkload
Loading Data for Multiple Nodes in a Replicated Environment	bulkload
Loading Data in Incremental Mode	bulkload
Managing Super User Access Control Points	oidpasswd
Managing Super User Access Control Points	oidpasswd
Merging Two Directories	oidcmprec
Modifying a Provisioning Profile	oidprovtool
Modifying a Synchronization Profile	dipassistant
Modifying an Entry	ldapmodify
Modifying Multiple Entries Concurrently	ldapmodifymt
Modifying the Directory Schema	ldapmodify
Moving an Entry	ldapmoddn
Moving an Integration Profile to a Different Identity Management Node	dipassistant
Overriding Data Migration Values in Lookup Mode	ldifmigrator
Overriding Default Conflict Resolution Rules	oidcmprec
Performing a Base Object Search	ldapsearch
Performing a One-Level Search	ldapsearch
Performing a Subtree Search	ldapsearch
Performing an Express Configuration for Microsoft Active Directory	dipassistant

Table 1–2 (Cont.) Task List for Oracle Identity Management ***Command-Line Tools***

Task	Tool Name
Performing Directory Schema Operations	oidcmprec
Performing User-Defined Compare and Reconcile Operations	oidcmprec
Previewing an Add Operation	ldapadd
Provisioning Users in Bulk	dipassistant
Recovering Data After a Load Error	bulkload
Recreating Indexes	bulkload
Registering the Oracle Directory Integration Platform Server With Oracle Internet Directory	odisrvreg
Removing a RMS Node from an Oracle Database Advanced Replication-based DRG	remtool
Removing an Attribute from the List of Indexed Attributes	catalog
Resetting the Replication DN Password for a Single Directory	remtool
Resetting the Super User Password	oidpasswd
Resetting the Super User Password	oidpasswd
Restarting an Oracle Internet Directory Server Instance	oidctl
Resuming Replication Activity for an Advanced Replication-based DRG	remtool
Retrying a Range of HIQ Change Logs	hiqretry.sh
Retrying a HIQ Change Log	hiqretry.sh
Retrying all HIQ Change Logs from a Supplier	hiqretry.sh
Running the Oracle Internet Directory Database Statistics Collection Tool	oidstats.sql
Running the Oracle Internet Directory Database Statistics Collection Tool	oidstats.sql
Searching for All User Attributes and Specified Operational Attributes	ldapsearch
Searching for Attribute Values of Entries	ldapsearch
Searching for Entries (More Examples)	ldapsearch
Searching for Entries with Attribute Options	ldapsearch
Setting the Wallet Password for the Oracle Directory Integration Platform Server	dipassistant
Showing a List of All Synchronization Profiles in Oracle Internet Directory	dipassistant
Starting a Directory Replication Server Instance	oidctl
Starting a Standalone Oracle Directory Integration Platform Server	odisrv
Starting All Oracle Internet Directory Server Instances Using opmnctl	opmnctl
Starting an Oracle Directory Integration Platform Server Instance	oidctl
Starting an Oracle Internet Directory Server Instance	oidctl
Starting and Stopping a Server Instance on a Virtual Host or Cluster Node	oidctl

Table 1–2 (Cont.) Task List for Oracle Identity Management ***Command-Line Tools***

Task	Tool Name
Starting Oracle Internet Directory Monitor	oidmon
Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node	oidmon
Stopping a Directory Replication Server Instance	oidctl
Stopping a Standalone Oracle Directory Integration Platform Server	stopodiserver.sh
Stopping All Oracle Internet Directory Server Instances Using opmnctl	opmnctl
Stopping an Oracle Directory Integration Platform Server Instance	oidctl
Stopping an Oracle Internet Directory Server Instance	oidctl
Stopping Oracle Internet Directory Monitor	oidmon
Suspending Replication Activity for an Advanced Replication-based DRG	remtool
Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory	schemasync
Unlocking the Super User Account	oidpasswd
Unlocking the Super User Account	oidpasswd
Updating an Attribute for Multiple Entries at Once	bulkmodify
Upgrading an Oracle Context	oidca
Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2	upgradecert.pl
Using a Parameter File	oidcmprec
Using the Data Migration Tool by Supplying Your Own Values	ldifmigrator
Using the Data Migration Tool in Lookup Mode	ldifmigrator
Validating Authentication Credentials	ldapbind
Viewing the Details of a Specific Synchronization Profile	dipassistant

2

Oracle Identity Management Server Administration Tools

This chapter describes the following command-line tools used to administer the Oracle Identity Management servers:

- odisrv (Oracle Directory Integration Server Control)
- oidca (Oracle Internet Directory Configuration Assistant)
- oidctl (Oracle Internet Directory Control)
- oiddiag (Oracle Internet Directory Server Diagnostic Tool)
- oidmon (Oracle Internet Directory Monitor)
- opmnctl (Oracle Process Manager and Notification Server Control)
- stopodiserver.sh (Oracle Directory Integration Server Stop Command)

odisrv

The Oracle Directory Integration Server Control Tool (`odisrv`) is used to start an Oracle Directory Integration Platform server in a client-only installation, where the Oracle Internet Directory Monitor (`oidmon`) and Control (`oidctl`) tools are not available, and if the Oracle Directory Integration Platform server is *not* used for high-availability purposes.

In a typical Oracle Internet Directory installation you should use the Oracle Internet Directory Monitor and Control utilities to start and stop the server. Oracle Corporation recommends that you use these utilities if available. This way, if the Oracle Directory Integration Platform server unexpectedly terminates, the Oracle Internet Directory Monitor utility automatically restarts it. See "oidmon" on page 2-16 and "oidctl" on page 2-8 for more information.

Syntax for odisrv

```
odisrv host=hostname port=port_number [config=configuration_set_number]
instance=instance_number [debug=debug_level] [refresh=interval_between_refresh]
[maxprofiles=number_of_profiles] [sslauth=ssl_mode]
```

Arguments for odisrv

host=*hostname*

Required. The host name of the Oracle Internet Directory server. If not specified, then the default of localhost is used.

port=*port_number*

Required. The port number used to connect to the Oracle Internet Directory server. If not specified, then the default of 389 is used.

config=*configuration_set_number*

Optional. The configuration set number to be used when starting the server.

instance=*instance_number*

Required. The instance number to assign to the Oracle Directory Integration Platform server. This instance number must be unique. OID Monitor verifies that the instance number is not already associated with a currently running instance of this server.

debug=*debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

refresh=*interval_between_refresh*

The number of minutes between server refreshes for any changes in Oracle Directory Integration Platform profiles. If not specified, the default of 2 is used.

maxprofiles=*number_of_profiles*

The maximum number of Oracle Directory Integration Platform profiles that can be executed concurrently for this server instance.

sslauth=*ssl_mode*

The number of the corresponding SSL mode. If not specified, the default of 0 is used. The modes are as follows:

- 0 — SSL is not used.

- 1 — SSL is used for encryption only, not for authentication.
- 2 — SSL is used for one-way authentication. With this mode you must also specify the complete path and file name of the server's Oracle Wallet.

Tasks and Examples for odisrv

Using the odisrv tool, you can perform the following task:

- Starting a Standalone Oracle Directory Integration Platform Server

Starting a Standalone Oracle Directory Integration Platform Server

The following example shows how to start an Oracle Directory Integration Platform server in a client-only installation:

Example:

```
odisrv host=host.company.com port=389 config=3 instance=1 debug=256 refresh=2
maxprofiles=3
```

Related Command-Line Tools for odisrv

- See "stopodiserver.sh" on page 2-19
- See "oidmon" on page 2-16
- See "oidctl" on page 2-8

oidca

During installation, the Oracle Internet Directory Configuration Assistant (`oidca`) configures Oracle Internet Directory. Once an installation has been completed, you can use it to:

- Create, upgrade, or delete an Oracle Context.
- Convert an Oracle Context to an Oracle Identity Management realm.
- Configure the `ldap.ora` file that is used to discover the directory server in the environment.

Use the Oracle Internet Directory Configuration Assistant with Enterprise User Security and Oracle Net Services under the following conditions:

Table 2–1 Conditions for Using Oracle Internet Directory Configuration Assistant for Specific Database Components

Component	Conditions
Enterprise User Security	Enterprise User Security works only with Oracle Identity Management realms created in the 9.0.4 or later release of Oracle Internet Directory. If you have Oracle Contexts created in prior releases, then you must use the Oracle Internet Directory Configuration Assistant to convert them to Oracle Identity Management realms. Use Oracle Internet Directory Configuration Assistant when creating or updating the `ldap.ora` configuration file. That file is used to discover the directory server in the environment.

Table 2–1 (Cont.) Conditions for Using Oracle Internet Directory Configuration Assistant for Specific Database Components

Component	Conditions
Oracle Net Services	Use Oracle Internet Directory Configuration Assistant when: ■ Creating, upgrading and deleting Oracle Contexts ■ Converting an Oracle Context from an earlier release to an Identity Management Realm ■ Setting up the `ldap.ora` configuration file. That file is used to discover the directory server in the environment.

Syntax for oidca

```
oidca -silent oidhost=hostname {nonsslport=port_number | sslport=port_number}
dn=binddn pwd=bindpwd {{mode=CREATECTX | UPGRADECTX | DELETECTX | CTXTOIMR
contextdn=oraclecontextdn} | {mode=LDAPORA adminctx=admincontextdn dirtype=OID |
AD [-update]}} | {propfile=filename}
```

Arguments for oidca

-silent

Required. The `silent` flag is used to run the `oidca` tool in command line or silent mode.

oidhost=*hostname*

Required. The host name of the Oracle Internet Directory server. If not specified, then the default of localhost is used.

nonsslport=*port_number* | sslport=*port_number*

Required. The port number used to connect to the Oracle Internet Directory server.

To connect to the directory in non-SSL mode, supply the unsecure LDAP port with the nonsslport argument (the default is 389).

To connect to the directory in SSL mode, supply the secure LDAP port with the sslport argument (the default is 636).

dn=*binddn*

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

pwd=*bindpw*

Required. The user password needed to bind to the directory.

mode=CREATECTX | UPGRADECTX | DELETECTX | CTXTOIMR | LDAPORA

Required. Specifies the operation to perform. The choices are:

- `CREATECTX` creates a new Oracle Context under the given DN.
- `UPGRADECTX` upgrades the Oracle Context in the given DN. You cannot upgrade Oracle Context instances that belong to a realm.
- `DELETECTX` deletes an Oracle Context from the given DN.
- `CTXTOIMR` converts an Oracle Context to an Oracle Identity Management realm.

- `LDAPORA` configures the ldap.ora file that is used to discover the Oracle Internet Directory server in the environment.

contextdn=*oraclecontextdn*

Required when the mode argument equals CREATECTX, UPGRADECTX, DELETECTX, or CTXTOIMR. Specifies the DN under which the Oracle Context will be created, upgraded, deleted, or converted to an Oracle Identity Management realm.

adminctx=*admincontextdn*

Required when the mode argument equals LDAPORA. The default administrative context DN. For example, `dn=company, dc=com`.

dirtype=OID | AD

Required when the mode argument equals LDAPORA. The type of directory.

-update

Optional flag used when the `mode` argument equals `LDAPORA`. Use `-update` to overwrite an existing `ldap.ora` file. If not given, a new `ldap.ora` file will be created. If the `ldap.ora` file exists and the `-update` argument is not specified, then the Assistant exits with the message "ldap.ora exists".

propfile=*filename*

Instead of specifying the `mode` argument and its associated `contextdn`, `adminctx`, and `dirtype` arguments on the command-line, you can specify them in a properties file instead. Specify the full path and file name of the file containing these arguments.

Tasks and Examples for oidca

Using the Oracle Internet Directory Configuration Assistant command-line tool, you can perform the following tasks:

- Creating an Oracle Context
- Upgrading an Oracle Context
- Deleting an Oracle Context
- Converting an Oracle Context to an Oracle Identity Management Realm
- Configuring the ldap.ora File

Creating an Oracle Context

The following example shows how to create a new Oracle Context under the given context DN:

Example:

```
oidca -silent oidhost=host.company.com nonsslport=389 dn=cn=orcladmin pwd=password
mode=CREATECTX contextdn=dc=company,dc=com
```

The context DN must exist in the directory and have the format of `dc=your_company,dc=com`. A DN with the format of `cn=oraclecontext,dc=your_company,dc=com` must *not* exist in the directory.

When creating an Oracle Context, Oracle Internet Directory Configuration Assistant does the following:

1. It verifies that the `contextdn` has valid DN syntax.
2. Verifies if `OracleContext` exists. If `OracleContext` does not exist, then Oracle Internet Directory Configuration Assistant creates it under the given context DN.

Upgrading an Oracle Context

The following example shows how to upgrade an existing Oracle Context under the given context DN:

Example:

```
oidca -silent oidhost=host.company.com nonsslport=389 dn=cn=orcladmin pwd=password
mode=UPGRADECTX contextdn=cn=oraclecontext,dc=company,dc=com
```

The context DN must exist in the directory, and can have either the format of `dc=your_company,dc=com` or the format of `cn=oraclecontext,dc=your_company,dc=com`. The given context DN must contain an `OracleContext`. The `OracleContext` *cannot* belong to a realm.

When upgrading an Oracle Context, Oracle Internet Directory Configuration Assistant does the following:

1. It verifies that the context DN has a valid DN syntax and that `OracleContext` exists in Oracle Internet Directory. The Assistant cannot upgrade a root `OracleContext` explicitly. If there is no root `OracleContext`, then the Assistant sends an error message.
2. It verifies if the `OracleContext` already belongs to an Oracle Identity Management realm. You *cannot* upgrade `OracleContext` instances that belong to a realm.

   If `OracleContext` belongs to a realm, then Oracle Internet Directory Configuration Assistant exits with the appropriate message.
3. It verifies if the `OracleContext` is up-to-date.

   If the `OracleContext` is up-to-date, then the Assistant exits with the message "Oracle Context already exists and is up to date."

   If the `OracleContext` is not up-to-date, then the Assistant upgrades the `OracleContext` under this DN.

Deleting an Oracle Context

The following example shows how to delete an existing Oracle Context under the given context DN:

Example:

```
oidca -silent oidhost=host.company.com nonsslport=389 dn=cn=orcladmin pwd=password
mode=DELETECTX contextdn=cn=oraclecontext,dc=company,dc=com
```

The context DN must exist in the directory, and can have either the format of `dc=your_company,dc=com` or the format of `cn=oraclecontext,dc=your_company,dc=com`. The given context DN must contain an `OracleContext`. The `OracleContext` *cannot* belong to a realm.

When deleting an Oracle Context, Oracle Internet Directory Configuration Assistant does the following:

1. It verifies that the context DN has a valid DN syntax and that `OracleContext` exists in Oracle Internet Directory.

2. It verifies if the `OracleContext` already belongs to an Oracle Identity Management realm. You *cannot* delete `OracleContext` instances that belong to a realm.

   If `OracleContext` belongs to a realm, then Oracle Internet Directory Configuration Assistant exits with the appropriate message.

3. If the `OracleContext` does not belong to a realm, then Oracle Internet Directory Configuration Assistant deletes it.

Converting an Oracle Context to an Oracle Identity Management Realm

Oracle Database 10*g* entries must be stored in Oracle Internet Directory Release 9.0.4 or later. Moreover, Enterprise User Security, a feature of Oracle Database 10*g*, requires a Release 9.0.4 or later version of an Oracle Identity Management realm.

The following example shows how to convert an existing Oracle Context to an Oracle Identity Management realm:

Example:

```
oidca -silent oidhost=host.company.com nonsslport=389 dn=cn=orcladmin pwd=password
mode=CTXTOIMR contextdn=cn=oraclecontext,dc=company,dc=com
```

The context DN must exist in the directory, and can have either the format of `dc=your_company,dc=com` or the format of `cn=oraclecontext,dc=your_company,dc=com`. The given context DN must contain an `OracleContext`. The `OracleContext` *cannot* already belong to a realm.

When converting an Oracle Context to an Oracle Identity Management realm, Oracle Internet Directory Configuration Assistant does the following:

1. It verifies that the context DN has a valid DN syntax and that `OracleContext` exists in Oracle Internet Directory.
2. It verifies if the `OracleContext` already belongs to an Oracle Identity Management realm. You *cannot* convert `OracleContext` instances that already belong to a realm.
3. If the `OracleContext` does not belong to a realm, then the Assistant converts the OracleContext to an Oracle Identity Management realm.

Note:

- If the nickname attribute is not `cn`, then configure it as a user configuration attribute by using the Oracle Internet Directory Self-Service Console. See instructions in the *Oracle Identity Management Guide to Delegated Administration*
- To use the Oracle Internet Directory Self-Service Console to manage user and groups in the converted realm, be sure to configure the appropriate administrative privileges. For details, see the *Oracle Internet Directory Administrator's Guide*.

Configuring the ldap.ora File

The following example shows how to configure an`ldap.ora` file by overwriting the existing `ldap.ora` file:

Example:

```
oidca -silent oidhost=host.company.com nonsslport=389 dn=cn=orcladmin pwd=password
mode=LDAPORA adminctx=dc=company,dc=com dirtype=OID -update
```

When configuring the `ldap.ora` file, Oracle Internet Directory Configuration Assistant does the following:

1. Checks for the `ldap.ora` file location.
2. If `ldap.ora` exists and the `-update` flag is not specified, then the Assistant exits with the message "ldap.ora exists".
3. If `ldap.ora` exists and the `-update` flag is specified, then the Assistant updates the existing `ldap.ora` file.
4. If `ldap.ora` does not exist, then the assistant creates a new `ldap.ora` file in a location in the following order:

   `LDAP_ADMIN`

   `$ORACLE_HOME/ldap/admin`

Related Command-Line Tools for oidca

N/A

oidctl

Oracle Internet Directory Control Utility (`oidctl`) is a command-line tool for starting and stopping Oracle Identity Management server instances. You can use this utility to start, stop, or restart the following server processes:

- Oracle Internet Directory Server
- Oracle Directory Integration Platform Server
- Oracle Directory Replication Server

The commands issued by Oracle Internet Directory Control Utility are interpreted and executed by the Oracle Internet Directory Monitor process. Before starting a server instance with this utility, make sure that the Monitor process is running. See "oidmon" on page 2-16.

Syntax for oidctl

```
oidctl [connect=connect_string] [host=virtual_hostname]
{server=OIDLDAPD | ODISRV | OIDREPLD} instance=instance_number
[configset=configuration_set_number] [flags="flagname=value ..."]
{start | stop | restart | status}
```

Arguments for oidctl

connect=*connect_string*

Optional. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`. If not provided, defaults to the value of `$ORACLE_SID` environment variable.

host=*hostname*

Optional. Enables you to specify a virtual host name for the server or the name of an Oracle Application Server Identity Management Cluster Node. If not given, the default of `localhost` is used.

server=OIDLDAP |ODISRV | OIDREPLD

Required. The name of the type of server process you want to start, stop, or restart. The options are:

- `OIDLDAPD` — Oracle Internet Directory server
- `ODISRV` — Oracle Directory Integration Platform server
- `OIDREPLD` — Directory Replication server

instance=*instance_number*

Required. An instance number assigned to the server process. The instance number must be unique for each server process. It cannot be associated with a currently running instance of the specified server type. Value must be greater than 0 but less than 100.

configset=*configuration_set_number*

Optional. The configuration set number to be used when starting the server. Defaults to 0 if not specified.

flags="*flagname=value* | *-flag value* ..."

Depending on the server process and the operation you are performing, you may also need to supply some additional flags on the command-line. Enclose all flags in quotation marks and separate *flagname =value* or *-flag value* pairs with a space. If the flags are not specified on the command-line, *configset* values are used. See the appropriate section for the flags related to each server type:

- "OIDLDAPD Flags" on page 2-9
- "ODISRV Flags" on page 2-10
- "OIDREPLD Flags" on page 2-11

These flags are passed to the server exactly as specified on the command-line—the `oidctl` or `oidmon` tools do not validate the values passed with the `flags` argument. If any values are invalid, the Oracle Internet Directory server will not start, but the `oidmon` tool will start. If this occurs, you should use `oidctl` to stop the server instance.

start | stop | restart | status

Required. The `start`, `stop`, or `restart` operation to perform on the given server process. The `status` option reports the status of each server configured on the node.

OIDLDAPD Flags

-debug *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

-l true | false

Optional. Turns replication change logging on or off. Use `true` to enable change logging. Use `false` to disable change logging. The default is `true`.

-p *ldap_port*

Optional. Specifies the LDAP port that this Oracle Internet Directory server instance will use. If not specified the default 389 is used.

-server number_of_processes

The number of server processes to start on this port.

-sport *ssl_port*

Optional. Specifies the LDAPS port that this Oracle Internet Directory server instance will use. If not specified the default 636 is used.

-work *maximum_threads*

The maximum number of worker threads for this server.

ODISRV Flags

host=*hostname*

The host name of the Oracle Internet Directory server. If not specified, then the default of `localhost` is used.

port=*port_number*

The port number used to connect to the Oracle Internet Directory server. If not specified, then the default of 389 is used.

debug=*debug_level*

Optional. If not specified the default of 0 (not enabled) is used. See "-debug debug_level" on page 2-9 for a description of the debug levels.

refresh=interval_between_refresh

The number of minutes between server refreshes for any changes in Oracle Directory Integration Platform profiles. If not specified, the default of 2 is used.

grpID=*group_id_profile*

The group ID of profiles to be scheduled.

maxprofiles=*number_of_profiles*

The maximum number of Oracle Directory Integration Platform profiles that can be executed concurrently for this server instance.

sslauth=*ssl_mode*

The number of the corresponding SSL mode. If not specified, the default of 0 is used. The modes are as follows:

- 0 — SSL is not used.
- 1 — SSL is used for encryption only, not for authentication.
- 2 — SSL is used for one-way authentication. With this mode you must also specify the complete path and file name of the server's Oracle Wallet.

OIDREPLD Flags

-p *directory_port_number*

Required for a start operation. Port number used to connect to Oracle Internet Directory server. The default is 389.

-h *directory_hostname*

Required for a start operation. The host name of the Oracle Internet Directory server to which the replication server connects. If not specified, `localhost` is used.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. See "-debug debug_level" on page 2-9 for a description of the debug levels.

-m true | false

Optional. Use `true` to enable conflict resolution. Use `false` to disable conflict resolution. The default value is `true`.

-z *transaction_size*

Optional. The number of changes applied in each replication update cycle. If not specified the value from the Oracle Internet Directory server size limit configuration parameter, which has a default of 1024.

Tasks and Examples for oidctl

Before using Oracle Internet Directory Control, make sure that Oracle Internet Directory Monitor is running. To verify this on UNIX, enter to following at the command-line:

```
ps -ef | grep oidmon
```

See "oidmon" on page 2-16 for more information about Oracle Internet Directory Monitor.

Using Oracle Internet Directory Control, you can perform the following tasks:

- Starting an Oracle Internet Directory Server Instance
- Stopping an Oracle Internet Directory Server Instance
- Restarting an Oracle Internet Directory Server Instance
- Starting an Oracle Directory Integration Platform Server Instance
- Stopping an Oracle Directory Integration Platform Server Instance
- Starting a Directory Replication Server Instance
- Stopping a Directory Replication Server Instance
- Starting and Stopping a Server Instance on a Virtual Host or Cluster Node
- Reporting the Status of Each Server

Starting an Oracle Internet Directory Server Instance

When starting an Oracle Internet Directory server, you must supply the `instance`, `server=OIDLDAPD`, and `start` arguments. All other arguments are optional.

Example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=2 configset=5 flags="-p 636 -debug
1024 -l" start
```

Stopping an Oracle Internet Directory Server Instance

Example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=2 stop
```

Restarting an Oracle Internet Directory Server Instance

A restart operation is useful when you want to refresh the server cache immediately, or when you have changed a configuration set entry and want your changes to take effect on an active server instance. When the Oracle Internet Directory server restarts, it maintains the same arguments it had before it stopped.

For example, if you changed a configuration set that was being referenced by an active instance of Oracle Internet Directory server, you could update it by restarting that server instance. You do not need to supply the `configset` argument again, as it is maintained from the prior start operation.

Example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=1 restart
```

To restart all active instances on a node, do not specify the `instance` argument. Note that a server is momentarily unavailable to client requests during a restart.

Starting an Oracle Directory Integration Platform Server Instance

It is recommended that you use the Oracle Internet Directory Control and Monitor utilities to start an integration and provisioning server. If these tools are not available, you can start a client-only integration and provisioning server instance using the `odisrv` utility. See "odisrv" on page 2-1.

The following example shows the recommended way to start an Oracle Directory Integration Platform server. You must make sure the Monitor utility is running before you can start a server. See "oidmon" on page 2-16.

Example:

```
oidctl connect=dbs1 server=ODISRV instance=1 configset=1
flags="host=ldaphost.company.com port=389 grpID=odipgroup maxprofiles=5 sslauth=2"
start
```

Stopping an Oracle Directory Integration Platform Server Instance

Server instances that are started using the Oracle Internet Directory Control utility must also be stopped in the same way. If you started a standalone Oracle Directory Integration Platform server using the `odisrv` utility, you should use the `stopodiserver.sh` script to stop the server.

The following example shows how to stop a server instance that was started using the Oracle Internet Directory Control utility.

Example:

```
oidctl server=ODISRV instance=1 stop
```

Starting a Directory Replication Server Instance

When starting an Oracle Directory Replication server you need to supply the information it needs to connect to the Oracle Internet Directory server.

Example:

```
oidctl connect=dbs1 server=OIDREPL instance=1 flags="-p 389 -h
ldaphost.company.com -d 1024" start
```

Stopping a Directory Replication Server Instance

Example:

```
oidctl connect=dbs1 server=OIDREPLD instance=1 stop
```

Starting and Stopping a Server Instance on a Virtual Host or Cluster Node

Use the `host` argument to specify a virtual host name when starting an Oracle Internet Directory server, Oracle Directory Integration Platform server, or Oracle Internet Directory Replication server on a virtual host or a Oracle Application Server Identity Management Cluster Node.

When communicating with the directory server, the directory replication server uses the virtual host name. Further, the `replicaID` attribute that represents the unique replication identification for the Oracle Internet Directory node is generated once. It is independent of the host name and hence requires no special treatment in Oracle Application Server Cold Failover Cluster (Identity Management).

When communicating with the directory server, the Directory Integration Platform server uses the virtual host name.

The following example shows how to start an Oracle Internet Directory server (OIDLDAPD) on a virtual host. The same syntax can be used to also start a directory replication server (OIDREPLD) or integration and provisioning server (ODISRV) on a virtual host.

Example:

```
oidctl connect=dbs1 host=vhost.company.com server=OIDLDAPD instance=1 configset=2
[flags="..."] start
```

Reporting the Status of Each Server

The `status` argument is used to report the status of each server running on the node.

Example:

```
oidctl connect=dbs1 status
```

Related Command-Line Tools for oidctl

- See "opmnctl" on page 2-18
- See "oidmon" on page 2-16
- See "odisrv" on page 2-1
- See "stopodiserver.sh" on page 2-19

oiddiag

The Oracle Internet Directory Server Diagnostic command-line tool (`oiddiag`) collects diagnostic information that helps triage issues reported on Oracle Internet Directory. The tool connects to the database used as the directory store (also called Metadata Repository) of Oracle Internet Directory and reads the information. The tool makes no recommendations on potential fixes to issues. Rather, it collects information to help Support and Development understand a problem and determine its solution. The tool can collect four types of diagnostic information:

- Directory information tree (DIT)
- Data consistency
- Server manageability statistics
- System and process information

If you use either the `collect_all=true` or the `collect_sub=true` arguments, you will be prompted to supply the following information:

- The fully domain-qualified database host name
- The database listener port number
- The database service name
- The ODS database user password

You can find the hostname, port number and service name in the file `tnsnames.ora`. For example, in the following `tnsnames.ora` file, the hostname, port number and service names are, respectively, `sun16.us.oracle.com`, `1521`, and `orcl.us.oracle.com`:

```
ORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = sun16.us.oracle.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.us.oracle.com)
    )
  )
```

Note: You must set the ORACLE_HOME environment variable before executing the OIDDIAG tool.

Syntax for oiddiag

```
oiddiag {listdiags=true [targetfile=filename]} | {collect_all=true
[outfile=filename]} | {collect_sub=true [infile=filename] [outfile=filename]} |
{audit_report=true [outfile=file_name]}
```

Arguments for oiddiag

listdiags=true

Writes a list of available diagnostics that can be collected. The list is written to an output file, which is $*ORACLE_HOME*/ldap/log/oiddiag.txt by default. You should run a listdiags command before running a collect_sub command. The collect_sub command uses the file that is output by listdiags. You can edit this file as needed to contain only the diagnostic items you want.

targetfile=*filename*

This is the location of the output file where the diagnostic tool writes the list of available diagnostics when listdiags=true is given. If not specified, the tool writes the list to $*ORACLE_HOME*/ldap/log/oiddiag.txt.

collect_all=true

Collect all of the diagnostic information available and writes it to an output file. You will be prompted to provide the Oracle Internet Directory database host name, listener port, net service name, and password.

outfile=*filename*

The name of the output file that the diagnostic information is written to. If not specified, the default output file is written to $*ORACLE_HOME*/ldap/log/oiddiag*timestamp*.log. The timestamp format is YYYYMMDDHHmmss.

collect_sub=true

Collects a subset of diagnostic information (based on the diagnostics specified in the input file) and writes it to an output file. You will be prompted to provide the Oracle Internet Directory database host name, listener port, net service name, and password.

You should run a listdiags command before running a collect_sub command. The collect_sub command uses the file that is output by listdiags. You can edit this file as needed to contain only the diagnostic items you want.

infile=*filename*

A file that contains the list of diagnostic items for which you want to output information. By default, the diagnostic tool looks for this file in $*ORACLE_HOME*/ldap/log/oiddiag.txt, which is the default target file location of the listdiags command. You can edit this file as needed to contain only the diagnostic items you want.

audit_report=true

Generates standard reports for Secure Events Tracking and writes them to an output file.

Tasks and Examples for oiddiag

Using the Oracle Internet Directory diagnostic tool, you can perform the following tasks:

- Collecting All Diagnostic Information
- Collecting Selected Diagnostic Information
- Collecting Stack Trace Information

Collecting All Diagnostic Information

The following example shows how to collect all available diagnostic information and write it to the specified output file.

Example:

```
oiddiag collect_all=true output=~/myfiles/oid.log
```

Collecting Selected Diagnostic Information

To collect a subset of diagnostic data, you must first run the `oiddiag` tool with the `listdiags` argument. This outputs a list of available diagnostics, which you can then edit. This list is then passed in to the `collect_sub` command to determine the diagnostics for which to collect output. The following example uses the default file locations of `$ORACLE_HOME/ldap/log/oiddiag.txt` (for the list) and `$ORACLE_HOME/ldap/log/oiddiagtimestamp.log` (for the output file).

Example:

```
oiddiag listdiags
oiddiag collect_sub
```

Collecting Stack Trace Information

An important type of information that the `oiddiag` tool collects is the stack trace data for Oracle Internet Directory processes. Examining the stack trace is useful if you are experiencing slow response times or if your system stops responding. Because Oracle Internet Directory is usually started as a `setuid-root` program, you must log in as the root user before you can use the `oiddiag` tool to trace the stack for any Oracle Internet Directory processes. The root user must belong to the same operating system group that the Oracle operating system user belongs to. The following example logs in as the root user and changes to the `dba` group before executing the `oiddiag` tool:

```
su
newgrp dba
oiddiag collect_all=true
```

oidmon

The Oracle Internet Directory Monitor (`oidmon`) initiates, monitors, and terminates directory server processes. If you elect to start a replication server or integration and provisioning server, Monitor controls it. When you issue commands through Oracle Internet Directory Control (`oidctl`) to start or stop directory server instances, your commands are interpreted by this process.

Syntax for oidmon

```
oidmon [connect=connect_string] [host=hostname] [sleep=seconds] start | stop
```

Arguments for oidmon

connect=*connect_string*

Optional. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`. If not provided, defaults to the value of `$ORACLE_SID` environment variable.

host=*hostname*

Optional. Enables you to specify a virtual host name for the server or the name of an Oracle Application Server Identity Management Cluster Node. If not given, the default of `localhost` is used.

sleep=*seconds*

Optional. The number of seconds after which Oracle Internet Directory Monitor should check for new requests from Oracle Internet Directory Control and for requests to restart any server instances that may have stopped. The default is 10 seconds.

start | stop

Required. The operation to perform (start or stop the Monitor process).

Tasks and Examples for oidmon

Using Oracle Internet Directory Monitor, you can perform the following tasks:

- Starting Oracle Internet Directory Monitor
- Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node
- Stopping Oracle Internet Directory Monitor

Starting Oracle Internet Directory Monitor

You should start Oracle Internet Directory Monitor before using Oracle Internet Directory Control.

Example:

```
oidmon connect=dbs1 sleep=15 start
```

Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node

Use the `host` argument to specify a virtual host name when starting an Oracle Internet Directory Monitor on a virtual host or a Oracle Application Server Identity Management Cluster Node.

Example:

```
oidmon connect=dbs1 host=virtualhostname.company.com start
```

Stopping Oracle Internet Directory Monitor

Stopping Oracle Internet Directory Monitor will also stop all other Oracle Internet Directory processes. The `oidmon` tool does not remove server instance information

from the ODS_PROCESS table. When an oidmon start operation is executed, it will start all the server processes it had stopped previously.

Example:

```
oidmon connect=dbs1 stop
```

Related Command-Line Tools for oidmon

- See "oidctl" on page 2-8

opmnctl

The Oracle Process Manager and Notification Server Control Utility (opmnctl) enables you to manage Oracle Application Server components in an integrated way. If you use it to start an Oracle Internet Directory server, then you do not need to separately start Oracle Internet Directory Monitor or the directory-designated database. Instead, opmnctl starts those components for you.

> **Note:** This section only discusses how to use the OPMN Control Utility to start and stop Oracle Internet Directory servers. For detailed information on how to use the OPMN Control Utility, see *Oracle Process Manager and Notification Server Administrator's Guide*.

You can use opmnctl to do the following:

- Start and stop a default, that is, out-of-the-box, Oracle Internet Directory server instance.
- On a given node, stop, then restart, all running Oracle Internet Directory servers—that is, directory servers, directory replication server, and Directory Integration Platform server.

Once you have used opmnctl to start the default directory server, you cannot then use it to start or stop a particular instance of an Oracle Internet Directory server. To start or stop particular instances, use oidctl. See "oidctl" on page 2-8.

Syntax for opmnctl

```
opmnctl {startproc | stopproc} ias-component=OID
```

Arguments for opmnctl

startproc | stopproc

Required. The operation to perform (start or stop all Oracle Internet Directory server processes).

ias-component=OID

Required. Identifies the Oracle Internet Directory server processes as the Oracle Application Server processes to start or stop.

Tasks and Examples for opmnctl

Using OPMN Control Utility, you can perform the following Oracle Internet Directory server management tasks:

- Stopping All Oracle Internet Directory Server Instances Using opmnctl
- Starting All Oracle Internet Directory Server Instances Using opmnctl

Stopping All Oracle Internet Directory Server Instances Using opmnctl

The following example shows how to stop all running directory server processes (Oracle Internet Directory, Oracle Directory Integration Platform server, and Oracle Directory Replication server).

Example:

```
opmnctl stopproc ias-component=OID
```

Starting All Oracle Internet Directory Server Instances Using opmnctl

The following example shows how to start all directory server processes previously stopped by OPMNCTL (Oracle Internet Directory, Oracle Directory Integration Platform server, and Oracle Directory Replication server).

Example:

```
opmnctl startproc ias-component=OID
```

Related Command-Line Tools for opmnctl

- See "oidmon" on page 2-16
- See "oidctl" on page 2-8

stopodiserver.sh

If you used the `odisrv` command to start an Oracle Directory Integration Platform server, you must then stop that server process with the `stopodiserver.sh` command. You should only use these commands in a client-only installation, where the Oracle Internet Directory Monitor and Control tools are not available. The `stopodiserver.sh` tool is located in the *`$ORACLE_HOME`*`/ldap/odi/admin` directory.

Syntax for stopodiserver.sh

```
$ORACLE_HOME/ldap/odi/admin/stopodiserver.sh -LDAPhost oid_hostname -LDAPport
ldap_port -binddn admin_dn -bindpass admin_password -instance instance_number
[-clean]
```

Arguments for stopodiserver.sh

-LDAPhost *oid_hostname*

Required. The host name of the Oracle Internet Directory server. If not specified, then the default of `localhost` is used.

-LDAPport *ldap_port*

Required. The port number used to connect to the Oracle Internet Directory server. If not specified, then the default of `389` is used.

-binddn *admin_dn*

Required. The DN of the Oracle Internet Directory super user needed to bind to the directory (for example, `cn=orcladmin`).

-bindpass *admin_password*

Required. The super user password needed to bind to the directory.

-instance *instance_number*

Required. The instance number of the Oracle Directory Integration Platform server instance to stop.

-clean

Optional. If the Oracle Directory Integration Platform server is stopped by any means other than the `oidctl` or `stopodiserver.sh` command, then the server cannot be started from the same host. In that case, the footprint of the previous execution in the directory needs to be removed by using the `-clean` argument.

Tasks and Examples for stopodiserver.sh

Using the stopodiserver.sh command you can perform the following task:

- Stopping a Standalone Oracle Directory Integration Platform Server

Stopping a Standalone Oracle Directory Integration Platform Server

The following example shows how to stop an Oracle Directory Integration Platform server in a client-only installation. Use the `-clean` argument to remove the footprint of the previous execution in the directory:

Example:

```
$ORACLE_HOME/ldap/admin/stopodiserver.sh -LDAPhost oidhost.company.com -LDAPport
389 -binddn cn=orcladmin -bindpass welcome -instance 1 -clean
```

Related Command-Line Tools for stopodiserver.sh

- See "odisrv" on page 2-1
- See "oidmon" on page 2-16
- See "oidctl" on page 2-8

3

Oracle Internet Directory Database Administration Tools

This chapter describes the following command-line tools used to administer the Oracle Internet Directory database:

- oidpasswd (Oracle Internet Directory Database Password Utility)
- oidstats.sql (Oracle Internet Directory Database Statistics Collection Tool)

oidpasswd

The Oracle Internet Directory Database Password Utility (`oidpasswd`) is used to:

- Change the password to the Oracle Internet Directory database.

  Oracle Internet Directory uses a password when connecting to an Oracle database. The default for this password matches the value you specified during installation for the Oracle Application Server administrator's password. You can change this password by using the OID Database Password Utility.
- Create wallets for the Oracle Internet Directory database password and the Oracle directory replication server password.
- Unlock or reset the directory super user account, namely, `cn=orcladmin`.
- Reset an access control point (ACP) so that the subtree is accessible by the Oracle Internet Directory super user.
- Manage the restricted super user ACL.

Syntax for oidpasswd

```
oidpasswd [connect=connect_string] [change_oiddb_pwd=true | create_wallet=true |
unlock_su_acct=true| reset_su_password=true | manage_su_acl=true]
```

Arguments for oidpasswd

connect=*connect_string*

Optional. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in $*ORACLE_HOME*`/network/admin`. If not provided, defaults to the value of `$ORACLE_SID` environment variable.

change_oiddb_pwd=true | unlock_su_acct=true | reset_su_password=true | manage_su_password=true

Required. The operation you want to perform. Depending on the operation you choose, the Oracle Internet Directory Database Password Utility will prompt you for additional information. The following choices are available:

- `change_oiddb_pwd=true` - Changes the password to the Oracle Internet Directory database. You will be prompted to provide the current database password, enter a new database password, and confirm the new password.

  Note: In an Oracle Real Application Clusters (RAC) environment, if you update the password on one Oracle RAC node, then you would need to update the wallet on the other Oracle RAC nodes. Refer to "About Changing the ODS Password on an Oracle RAC System" in the *Oracle Application Server High Availability Guide* for more information.

- `create_wallet=true` - Create a wallet named `oidpwdlldap1` for the Oracle Internet Directory database password, and a wallet, named `oidpwdr`*`sid`*, for the Oracle directory replication server password.

  The *`sid`* is obtained not from the environment variable *`SID`* but from the connected database.

  You need to provide the ODS password to authenticate yourself to the ODS database before the ODS wallet can be generated. Note that the default ODS password is the same as that for the Oracle Application Server administrator.

- `unlock_su_acct=true` - Unlocks a super user account that has been locked.
- `reset_su_password=true` - Resets the password for the Oracle Internet Directory super user account. You will be prompted to provide the Oracle Internet Directory database password, enter a new super user password, and confirm the new super user password.
- `manage_su_acl=true` - Manages the restricted super user ACL.

Tasks and Examples for oidpasswd

Using Oracle Internet Directory Database Password Utility, you can perform the following tasks:

- Changing the Password to the Oracle Internet Directory Database
- Creating Wallets for Oracle Internet Directory Database and Oracle Directory Replication Server Passwords
- Unlocking the Super User Account
- Resetting the Super User Password
- Managing Super User Access Control Points

Changing the Password to the Oracle Internet Directory Database

The following example shows how to change the Oracle Internet Directory database password, assuming the database in on the same machine.

Example:

```
oidpasswd
current password: oldpassword
```

```
new password: newpassword
confirm password: newpassword
password set.
```

The Oracle Internet Directory Database Password Utility prompts you for the current password. Type the current password, then the new password, then a confirmation of the new password.

The utility assumes by default that the password being changed is that of the local database (as defined by *ORACLE_HOME* and ORACLE_*SID*). If you are changing the password on a remote database, you must use the connect=*connect_string* option.

Note:

- User responses are not echoed to the screen when you enter a password.
- Whenever you change the password to the Oracle Internet Directory database by using the OID Database Password Utility, you should also run the oidemdpasswd utility. This enables the Oracle Enterprise Manager Daemon (a component of Oracle Enterprise Manager) to properly cache that password and contact the ODS schema upon starting up. Once you have run the oidemdpasswd utility, you can monitor Oracle Internet Directory processes from the Oracle Enterprise Manager.

Creating Wallets for Oracle Internet Directory Database and Oracle Directory Replication Server Passwords

The following example shows how to create wallets for the Oracle Internet Directory database password and the Directory Replication server password.

Example:

```
oidpasswd connect=dbs1 create_wallet=true
```

The argument create_wallet=true is mandatory in this case. Except for the connect string, no other option can be specified.

Unlocking the Super User Account

The following example shows how to unlock the Oracle Internet Directory super user account, cn=orcladmin.

Example:

```
oidpasswd connect=dbs1 unlock_su_acct=true
```

The argument unlock_su_acct is mandatory. Except for connect string, no other option can be specified.

Resetting the Super User Password

If you forget the Oracle Internet Directory super user password, you can use the oidpasswd tool to reset it. You must provide the Oracle Internet Directory database password. When you first install Oracle Internet Directory, the super user password and Oracle Internet Directory database password are the same. After installation, however, you can change the Oracle Internet Directory super user password using

ldapmodify. You can change the Oracle Internet Directory super user password using the oidpasswd tool separately.

The following example shows how to reset the Oracle Internet Directory super user password. The oidpasswd tool prompts you for the Oracle Internet Directory database password.

Example:

```
oidpasswd connect=dbs1 reset_su_password=true
OID DB user password: oid_db_password
        password: new_su_password
confirm password: new_su_password
OID super user password reset successfully
```

Managing Super User Access Control Points

When an access control point (ACP) is set with an access control item (ACI) that has the keyword DenyGroupOverride, neither the Oracle Internet Directory super user nor members of DirectoryAdminGroup can access the subtree under that ACP. If necessary, you can use the oidpasswd tool to reset that ACP so that the subtree is accessible by the Oracle Internet Directory super user.

The following example shows how to reset a restricted ACP. The oidpasswd utility prompts you to enter the Oracle Internet Directory database password and to choose which super user restricted ACPs to reset.

Example:

```
oidpasswd conn=dbs1 manage_su_acl=true
OID DB user password: oid_db_password

The super user restricted ACP list
[1] o=oracle,c=us
[2] ou=personnel,o=oracle,c=us

Enter 'resetall' or the number(s) of the ACP to be reset separated by [,]
resetall
```

Once you have reset some ACPs so that the super user can access them, you can use ldapmodify to make the subtrees inaccessible to the super user again.

Related Command-Line Tools for oidpasswd

- See "ldapmodify" on page 4-27.
- See "oidctl" on page 2-8.

oidstats.sql

Use the Oracle Internet Directory Database Statistics Collection Tool (oidstats.sql) to analyze the various database ods (Oracle Directory Server) schema objects to estimate the statistics. It is located in the following directory: $*ORACLE_HOME*/ldap/admin/. You must run this utility whenever there are significant changes in directory data—including the initial load of data into the directory.

If you load data into the directory by any means other than the bulk load tool (bulkload.sh), then you must run the Oracle Internet Directory Database Statistics Collection tool after loading. Statistics collection is essential for the Oracle Optimizer to choose an optimal plan in executing the queries corresponding to the LDAP

operations. You can run Oracle Internet Directory Database Statistics Collection tool at any time, without shutting down any of the Oracle Internet Directory daemons.

> **Note:** If you do not use the bulkload utility to populate the directory, then you must run the `oidstats.sql` tool to avoid significant search performance degradation.

Syntax for oidstats.sql

```
sqlplus ods/ods_password@connect_string@oidstats.sql
```

Arguments for oidstats.sql

ods_password

Required. The ODS password to authenticate yourself to the ODS database. Note that the default ODS password is the same as that for the Oracle Application Server administrator.

connect_string

Required. The connect string for the ODS database. This is the network service name set in the `tnsnames.ora` file.

Tasks and Examples for oidstats.sql

You can perform the following task using the `oidstats.sql` tool:

- Running the Oracle Internet Directory Database Statistics Collection Tool

Running the Oracle Internet Directory Database Statistics Collection Tool

Example:

```
sqlplus ods/welcome1@dbs1@oidstats.sql
```

Related Command-Line Tools for oidstats.sql

- See bulkload

4

Oracle Internet Directory Data Management Tools

This chapter describes the following command-line tools used to administer the entries and data stored in Oracle Internet Directory:

- bulkdelete (Bulk Deletion Tool)
- bulkload (Bulk Loading Tool)
- bulkmodify (Bulk Modification Tool)
- catalog (Catalog Management Tool)
- ldapadd (LDAP Data Add Tool)
- ldapaddmt (Multi-Threaded LDAP Data Add Tool)
- ldapbind (Authentication Validation Tool)
- ldapcompare (Attribute Comparison Tool)
- ldapdelete (LDAP Data Deletion Tool)
- ldapmoddn (LDAP DN/RDN Modification Tool)
- ldapmodify (LDAP Data Modification Tool)
- ldapmodifymt (Multi-Threaded LDAP Data Modification Tool)
- ldapsearch (LDAP Search Tool)
- ldifmigrator (Data Migration Tool)
- ldifwrite (Data Export Tool)
- upgradecert.pl (Certificate Upgrade Tool)

bulkdelete

The `bulkdelete` command-line tool enables you to delete one or more subtrees efficiently. It can be used when both an Oracle Internet Directory server and Oracle Directory Replication servers are in operation. It uses a SQL interface to benefit performance. For this release, the `bulkdelete` tool runs on only one node at a time.

This tool does not support filter-based deletion. That is, it deletes an entire subtree below the root of the subtree. If the base DN is a user-added DN, rather than a DN created as part of the installation of the directory, it is included in the delete. You must restrict LDAP activity against the subtree during deletion.

Syntax for bulkdelete

```
bulkdelete connect=connect_string {[basedn=Base_DN]|[file=file_name]}
[cleandb="TRUE"|"FALSE"] [size=transaction_size] [encode=character_set]
[debug="TRUE"|"FALSE"] [threads=num_of_threads] [verbose="TRUE"|"FALSE"]
```

Arguments for bulkdelete

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in *$ORACLE_HOME*`/network/admin`.

basedn | file

Required. The base DN of the subtree to be deleted, for example, `"dc=company, dc=com"`. Enclose the DN in quotation marks. You can also specify multiple base DNs by putting them in a file and specifying the file name and path with the `file` argument.

cleandb

Optional. This is used to specify whether the deleted entries would be tomb stoned or deleted completely from the database. The default (`cleandb="TRUE"`) is to delete the entries completely.

size

Optional. The number of entries to be committed as a part of one transaction.

encode

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

debug

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `bulkdelete.log` file. This file can be found under `$ORACLE_HOME/ldap/log`.

threads

Optional. The number of threads to create. The default value is the number of CPUs on the machine plus one.

verbose

Optional. This is used to run the command in verbose mode.

Tasks and Examples for bulkdelete

The following examples show how to delete one or more subtrees from the directory:

- Deleting All Entries in a Naming Context and Making Them Tombstone Entries
- Completely Deleting All Entries in a Naming Context
- Deleting Entries in Multiple Naming Contexts

Deleting All Entries in a Naming Context and Making Them Tombstone Entries

Example:

```
bulkdelete connect="dbs1" basedn="cn=OracleContext" cleandb="FALSE"
```

Completely Deleting All Entries in a Naming Context

Example:

```
bulkdelete connect="dbs1" basedn="cn=OracleContext"
```

Deleting Entries in Multiple Naming Contexts

This example uses a file that contains a list of DNs to delete.

Example:

```
bulkdelete connect="dbs1" file="~/myfiles/dn.txt"
```

Related Command-Line Tools for bulkdelete

- See "bulkload" on page 4-3
- See "bulkmodify" on page 4-7
- See "ldapdelete" on page 4-23

bulkload

The `bulkload` command-line tool is useful for loading large number of entries into a directory server. It uses Oracle SQL*Loader to load the directory entries. The bulkload tool expects the input file to be in **LDAP Data Interchange Format (LDIF)**. See Appendix A, "LDIF File Format" for the correct format and syntax of an LDIF file.

Overview of the Bulk Loading Tool Operations

The Bulk Loading Tool performs its operations in the following phases:

1. **Check**

   In the check phase, all entries of LDIF files are verified for valid LDAP schema and duplicate entries. The Bulk Loading Tool will report any errors, which must be corrected before proceeding.

2. **Generate**

   In the generate phase, the LDIF input is converted into intermediate files that can be used by SQL*Loader to load the data into the Oracle Internet Directory directory store.

3. **Load**

   The Intermediate files generated in generate phase are loaded into the Oracle Internet Directory directory store. The Bulk Loading Tool supports two types of loading of data:

   - **Incremental Mode Loading**

     Incremental mode enables you to append data to existing directory data. Loading in this mode is faster than other add methods, but slower than bulk mode loading.

Use this mode when you want to append a small amount of data. Here, small amount is a relative number. It depends upon existing data in directory, the amount of data to be loaded, and the hardware capabilities to handle the load.

In this mode, the Bulk Loading Tool does not drop and rebuild catalog indexes. Instead, it uses SQL*Loader in insert mode to add data to the database and update indexes through inserts.

- **Bulk Mode Loading**

  In bulk mode, you must be able to add or append large number of entries to a directory. By default, the Bulk Loading Tool runs in bulk mode. Bulk mode is faster than incremental mode.

  In bulk mode, all Oracle Internet Directory server instances should be stopped. In this mode, the Bulk Loading Tool drops existing indexes and re-creates them after loading of data. For data loading, it uses SQL*Loader direct-path mode.

4. **Index Creation**

   After the load is complete, the indexes are re-created if the load was done in bulk mode. Also, the Bulk Loading Tool provides an option just to re-create all indexes. This is useful in case if previous index creation was unsuccessful for some reason.

5. **Directory Data Recovery**

   A failure in the load phase can leave directory data in an inconsistent state. The Bulk Loading Tool can revert back to original state that existed prior to the invocation of `bulkload`.

Before Using the bulkload Tool

Before running the bulkload tool:

1. Stop your Oracle Internet Directory server instance(s) before loading data in bulk mode.
2. If loading data in incremental mode, you do not need to stop the directory server, although you will need to put the directory server in read-modify mode. Read-modify mode restricts add, delete, and modify DN operations.
3. If loading an LDIF file with data from an older version of Oracle Internet Directory, see the *Oracle Application Server Upgrade and Compatibility Guide* for any special instructions about upgrading `orclguids` before you begin.

Syntax for bulkload

```
bulkload [connect=connect_string]
{[check="TRUE"|"FALSE" [restore="TRUE"|"FALSE"] [thread=num_of_threads]
[file=ldif_file]]
[generate="TRUE"|"FALSE" [append="TRUE"|"FALSE"] [restore="TRUE"|"FALSE"]
[thread=num_of_threads] file=ldif_file]
[load="TRUE"|"FALSE"  [append="TRUE"|"FALSE"] [threads=num_of_threads]]
[index="TRUE"|"FALSE"] [recover="TRUE"|"FALSE"]}
[encode=character_set] [debug="TRUE"|"FALSE"] [verbose="TRUE"|"FALSE"]
```

Arguments for bulkload

connect

Optional. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`. For loading data in single node, specify its connect string—for example `orcl`. For loading data in multiple nodes, specify connect strings of all nodes—for example, `orcl1 orcl2 orcl3`.

check | generate | load | recover | index

Required. The operation to perform. The operations are:

- `check` - Checks the LDIF file provided for schema inconsistencies and for duplicate entry DNs. You must provide the full path or relative path and file name of an LDIF file. You can optionally specify the number of threads. The `check` and `generate` operations can be issued at the same time.
- `generate` - Creates intermediate files suitable for loading entries into Oracle Internet Directory using SQL*Loader. You must provide the full path or relative path and file name of an LDIF file from which to generate entries. You can optionally specify the number of threads. The `check` and `generate` operations can be issued at the same time.

  Note: After the `generate` operation, the directory is left in the read-modify mode until you perform the `load` operation.

- `load` - Loads the files generated in the `generate` operation into the database. You can use the `append` option to specify if the data needs to be appended to the existing directory data. For load to succeed, the LDAP server must be running. You can optionally specify the number of threads. If you set the `ldplonly` option to `"TRUE"`, then the data is loaded in parallel but index creation takes place in serial mode. You must run a `generate` operation before a `load` operation.
- `recover` - In case of a failure during a `load` operation, recovers the directory with the original data. You cannot use any other option when using the `recover` option.
- `index` - Recreates indexes on all catalog tables.

file

Required for the `check` and `generate` operations. The fully qualified path or relative path and file name of the LDIF file that contains the entries you want to load.

threads

Optional for the `check`,`generate`, and `load` operations. The number of threads to create. The default value is the number of CPUs on the machine plus one.

restore

Optional with the `check` and `generate` operations. Assumes operational attributes, such as `orclguid`, `creatorsname`, and `createtimestamp`, are already present in the specified LDIF file. Duplicate operational attribute values are not created in the output SQL*Loader files.

append

Optional with the `generate` and `load` operations. Loads entries in incremental mode rather than bulk mode, which is the default. Incremental mode appends data to existing directory data, and is intended for loading small amounts of data.

encode

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

debug

Optional. The debug option turns debugging on or off. Turning debugging on (`debug="TRUE"`) is useful when the command runs into errors. The output is logged to the `bulkload.log` file. This file can be found under `$ORACLE_HOME/ldap/log`.

verbose

This is used to run the command in verbose mode.

Tasks and Examples for bulkload

Using the bulkload tool, you can perform the following tasks:

- Loading Data in Bulk Mode
- Loading Data for Multiple Nodes in a Replicated Environment
- Loading Data in Incremental Mode
- Verifying Indexes
- Recreating Indexes
- Recovering Data After a Load Error

Loading Data in Bulk Mode

The typical usage scenario is to load directory data after Oracle Internet Directory installation. First check the LDIF file for schema errors and generate the intermediate files. Next, load the data into the Oracle Internet Directory store.

The following example shows how to run the `bulkload` tool. The tool is first run with the `check` and `generate` options. The `check` option checks the input for schema and data consistency violations. The `generate` option generates the input files for SQL*Loader. Next, the command is run with the `load` option to load the data into the directory.

Example:

```
bulkload connect="orcl" check="TRUE" generate="TRUE" file="~/myfiles/data.ldif"
bulkload connect="orcl" load="TRUE"
```

Loading Data for Multiple Nodes in a Replicated Environment

When you load the same data into multiple nodes in a replicated network, ensure that the `orclGUID` parameter (global ID) is consistent across all the nodes. You can accomplish this by generating the bulk load data file once only (using the `generate` argument), and then using the same data file to load the other nodes (using the `load` argument).

Loading Data in Incremental Mode

If you need to add directory entries to an Oracle Internet Directory store already containing some user LDIF data, use the `append` argument to denote incremental mode. This mode is normally faster than other methods of adding entries to the directory. However, be sure that the directory server instances are in read-modify mode before you begin. The following example shows how to run `bulkload` in incremental mode.

Example:

```
bulkload connect="orcl" check="TRUE" generate="TRUE" load="TRUE" append="TRUE"
file="~/myfiles/data.ldif"
```

Verifying Indexes

You can verify existing indexes in the directory using the `check` option along with the `index` option.

Example:

```
bulkload connect="orcl" check="TRUE" index="TRUE"
```

Recreating Indexes

The `load` operation either updates or creates the indexes. However, due to issues like improper sizing, the indexes may not be updated or created properly. For this reason, the `bulkload` tool enables you to re-create all the indexes.

Example:

```
bulkload connect="orcl" index="TRUE"
```

Recovering Data After a Load Error

Due to issues like improper disk sizing, the `load` operation may fail. If this happens, then directory data can be inconsistent. For this reason, `bulkload` enables you to recover the directory data to the state that existed prior to the invocation of `bulkload`.

Example:

```
bulkload connect="orcl" recover="TRUE"
```

Related Command-Line Tools for bulkload

- See "bulkdelete" on page 4-1
- See "bulkmodify" on page 4-7
- See "ldapadd" on page 4-12
- See "ldapaddmt" on page 4-16

bulkmodify

The `bulkmodify` command-line tool enables you to modify a large number of existing entries in an efficient way. The `bulkmodify` tool supports the following:

- Subtree based modification
- LDAP search filter. For example, the filter could be `objectclass=*`, `objectclass=oneclass`, or `'(&(sn=Baileys)(cn=Kalid Baileys))'`.

- Attribute value addition and replacement. It modifies all matched entries in bulk.

The `bulkmodify` tool performs schema checking on the specified attribute name and value pair during initialization. All entries that meet the following criteria are modified:

- They are under the specified subtree.
- They meet the LDAP filter condition.
- They contain the attribute to be modified as either mandatory or optional.

The directory server and directory replication server may be running concurrently while bulk modification is in progress, but the bulk modification does not affect the replication server. You must perform bulk modification against all replicas.

Note: LDIF file based modification is not supported by `bulkmodify`. This type of modification requires per-entry-based schema checking, and therefore the performance gain over the existing ldapmodify tool is insignificant.

Make sure that when bulkmodify is invoked, server side entry cache is disabled.

You must restrict user access to the subtree during bulk modification. If necessary, **access control item (ACI)** restriction can be applied to the subtree being updated by `bulkmodify`.

You cannot use `bulkmodify` to add a value to single-valued attributes that already contain one value. If a second value is added, you must alter the directory schema to make that attribute multi-valued.

You cannot use `bulkmodify` to update the following attributes:

- dn (use `ldapmoddn` instead)
- Binary Attributes
- orclCertificateHash
- orclCertificateMatch
- cn (use `ldapmodify` instead)
- userPassword (use `ldapmodify` instead)
- orclPassword (use `ldapmodify` instead)
- orclACI (use `ldapmodify` instead)
- orclEntryLevelACI (use `ldapmodify` instead)

Syntax for bulkmodify

```
bulkmodify connect=connect_string basedn=Base_DN
{[add="TRUE"|"FALSE"]|[replace="TRUE"|"FALSE"]} attribute=attribute_name
value=attribute_value [filter=filter_string] [size=transaction_size]
[threads=num_of_threads] [debug="TRUE"|"FALSE"] [encode=character_set]
[verbose="TRUE"|"FALSE"]
```

Arguments for bulkmodify

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

basedn

Required. The DN of the subtree to be modified. Enclose the DN in quotes.

add | replace

Required. The operation to be performed on the attribute. Specifies whether you want to add an attribute value or replace an attribute value.

attribute

Required. The name of a single attribute for which a value needs to be added or replaced.

value

Required. The single attribute value to add or replace. If the value contains spaces, enclose it in quotes.

filter

Optional. A filter string that contains a single attribute. Defaults to `objectclass=*`.

size

Optional. The number of entries to be committed as part of one transaction. Defaults to 100.

threads

Optional. The number of threads to create. The default value is the number of CPUs on the machine plus one.

debug

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `bulkmodify.log` file. This file can be found under `$ORACLE_HOME/ldap/log`.

encode

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

verbose

This is used to run the command in verbose mode.

Tasks and Examples for bulkmodify

Using the `bulkmodify` tool, you can perform the following task:

- Updating an Attribute for Multiple Entries at Once

Updating an Attribute for Multiple Entries at Once

The following example shows how to modify an attribute for several entries using a filter. This command adds the telephone number 408-123-4567 to the entries of all employees who have Anne Smith as their manager.

Example:

```
bulkmodify connect="orcl" basedn="c=US" add="TRUE" attribute="telephoneNumber"
value="408-123-4567" filter="manager=Anne Smith"
```

Limitations of bulkmodify

`bulkmodify` has the following limitations:

- `bulkmodify` does not distinguish between attributes with or without subtypes, when performing the `replace` operation. `bulkmodify` replaces the attribute value irrespective of whether the attribute contains subtypes.
- `bulkmodify` allows the RDN to be modified without modifying the DN. If an attribute is part of a DN, then the attribute value is modified but the DN entry in the directory is not modified.
- `bulkmodify` does not perform an object class check when performing an `add` operation. When adding a new attribute to a directory entry, bulkmodify does not verify if the entry has the required object class to support the attribute.

Related Command-Line Tools for bulkmodify

- See "bulkdelete" on page 4-1
- See "bulkload" on page 4-3
- See "ldapmodify" on page 4-27
- See "ldapmodifymt" on page 4-31

catalog

Oracle Internet Directory uses indexes to make attributes available for searches. When Oracle Internet Directory is installed, the `cn=catalogs` entry lists available attributes that can be used in a search. You can index only those attributes that have:

- An equality matching rule
- Matching rules supported by Oracle Internet Directory (see "Matching Rules" on page 7-4)

If you want to use additional attributes in search filters, then you must add them to the catalog entry. You can do this at the time you create the attribute by using Oracle Directory Manager. However, if the attribute already exists, then you can index it only by using the Catalog Management Tool (`catalog`).

Before running `catalog`, be sure that the directory server is either stopped or in read-only mode.

Caution: Do not use the `catalog delete="TRUE"` argument on indexes created by the Oracle Internet Directory base schema. Removing indexes from base schema attributes can adversely impact the operation of Oracle Internet Directory.

Syntax for catalog

```
catalog connect=connect_string {[add="TRUE"|"FALSE"]|[delete="TRUE"|"FALSE"]}
{[attribute=attribute_name]|[file=file_name]} [logging="TRUE"|"FALSE"]
[threads=num_of_threads] [debug="TRUE"|"FALSE"] [verbose="TRUE"|"FALSE"]
```

Arguments for catalog

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in $*ORACLE_HOME*`/network/admin`.

add | delete

Required. The operation to perform. The `add` argument indexes the specified attribute. The `delete` argument drops the index for the specified attribute.

attribute | file

Required. The attribute or attributes to catalog. Use the `attribute` argument to specify a single attribute name on the command-line. Use the `file` argument to provide the full path and file name of a file that contains a list of several attribute names.

logging

Optional. This option is used to decide if redo logs are generated when a catalog is created.

threads

Optional. The number of threads to create. The default value is the number of CPUs on the machine plus one.

debug

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `catalog.log` file. This file can be found under `$ORACLE_HOME/ldap/log`.

verbose

Optional. This option specifies whether the command should be run in verbose mode.

Tasks and Examples for catalog

Using the `catalog` tool, you can perform the following tasks:

- Indexing a Single Attribute
- Indexing Multiple Attributes
- Removing an Attribute from the List of Indexed Attributes

Indexing a Single Attribute

The following example shows how to index a single attribute. The `catalog` tool will prompt you for the Oracle Internet Directory super user password.

Example:

```
catalog connect="orcl" add="TRUE" attribute="orclGender"
```

Indexing Multiple Attributes

The following example shows how to index multiple values at once by supplying a file that contains a list of attribute names. The `catalog` tool will prompt you for the Oracle Internet Directory super user password.

Example:

```
catalog connect="orcl" add="TRUE" file="~/myfiles/attrs.txt"
```

Removing an Attribute from the List of Indexed Attributes

The following example shows how to remove a single attribute from the list of indexed attributes. The `catalog` tool will prompt you for the Oracle Internet Directory super user password.

Example:

```
catalog connect="orcl" delete="TRUE" attribute="orclGender"
```

Related Command-Line Tools for catalog

- N/A

ldapadd

The `ldapadd` command-line tool enables you to add entries, their object classes, attributes, and values to the directory. To add attributes to an existing entry, use the `ldapmodify` command, explained in "ldapmodify" on page 4-27.

> **See Also:** For information on using attribute aliases with ldapadd refer to the "Attribute Aliases In the Directory" section in *Oracle Internet Directory Administrator's Guide*

Syntax for ldapadd

```
ldapadd -h oid_hostname -D "binddn" -w password [-Y "proxy_dn"] [-p ldap_port]
[-V ldap_version] {-f ldif_filename | -X dsml_filename}  [-b] [-n]
[-c [-o log_file_name]] [-M] [-v] [-O ref_hop_limit] [-i 1|0] [-k|-K]
[-U SSL_auth_mode {-W wallet_location -P wallet_password}] [-d debug_level]
[-E character_set]
```

Arguments for ldapadd

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-Y "*proxy_dn*"

Optional. The DN of a proxy user. After binding to the directory, the add operation will be performed as this user.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-f *ldif_filename* | -X *dsml_filename*

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See Appendix A, "LDIF File Format" on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See "Adding Data to the Directory Using a DSML File" on page 4-15 for more information about formatting a DSML file.

-b

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

-n

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

-c

Optional. Proceeds in spite of errors. All errors will be reported. If the `-c` argument is not used, the tool will stop when an error occurs.

-o *log_file_name*

Optional. Used with the `-c` argument. Writes the LDIF entries with errors to a log file. Specify the full path and name of the log file.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-v

Optional. Runs the tool in verbose mode.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-i 1 | 0

Optional. Specifies whether or not to bind as the current user when following referrals. 1 means bind as the current user, 0 means bind anonymously. The default is 0 (zero).

-k | -K

Optional. The `-k` argument authenticates using Kerberos authentication instead of simple authentication. To enable this option, you must compile with KERBEROS defined.You must already have a valid ticket granting ticket. Use the `-K` argument if you want to only perform the first step of the Kerberos bind.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations

- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for ldapadd

Using the ldapadd tool, you can perform the following tasks:

- Adding Data to the Directory Using an LDIF File
- Adding Data to the Directory Using a DSML File
- Previewing an Add Operation

Adding Data to the Directory Using an LDIF File

You can use `ldapadd` to add entries or schema information to the directory from an LDIF file. The file must be correctly formatted. See Appendix A, "LDIF File Format" on page A-1 for information about formatting an LDIF file.

Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -w password -p 389 -f
~/myfiles/input.ldif -v
```

Adding Data to the Directory Using a DSML File

You can use `ldapadd` to add entries or schema information to the directory from a Directory Service Markup Language (DSML) file that contains `<addRequest>` elements. For more information about the formatting DSML files, visit the OASIS Web site at `http://www.oasis-open.org`. The following example shows a sample DSML entry for a user.

Example:

```
<addRequest dn="CN=Alice,OU=HR,DC=Example,DC=COM">
     <attr name="objectclass"><value>top</value></attr>
     <attr name="objectclass"><value>person</value></attr>
     <attr name="objectclass"><value>organizationalPerson</value></attr>
     <attr name="sn"><value>Johnson</value></attr>
     <attr name="givenName"><value>Alice</value></attr>
     <attr name="title"><value>Software Design Engineer</value></attr>
</addRequest>
```

Once you have a correctly formatted DSML file, you can add data to the directory using `ldapadd` and supplying the DSML file as the input file.

Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -w password -p 389 -X
~/myfiles/input.xml -v
```

Previewing an Add Operation

Use the `-n` argument with an `ldapadd` command to preview the results of an add operation before actually adding any data to the directory.

Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -w password -p 389 -X
~/myfiles/input.xml -v -n
```

Related Command-Line Tools for ldapadd

- See "ldapaddmt" on page 4-16
- See "ldapmodify" on page 4-27
- See "bulkload" on page 4-3

ldapaddmt

The `ldapaddmt` tool performs the same functionality as the `ldapadd` command. It enables you to add entries, their object classes, attributes, and values to the directory. However, it also supports multiple threads for adding entries concurrently.

While it is processing entries, `ldapaddmt` logs errors in the `add.log` file within the current directory.

> **Note:** Increasing the number of concurrent threads improves the rate at which entries are created, but consumes more system resources.

Syntax for ldapaddmt

```
ldapaddmt -h oid_hostname -D "binddn" -w password -T number_threads [-p ldap_port]
[-V ldap_version] {-f ldif_filename | -X dsml_filename}  [-b] [-c] [-M] [-O
ref_hop_limit] [-k|-K] [-U SSL_auth_mode {-W wallet_location -P wallet_password}]
[-d debug_level] [-E character_set]
```

Arguments for ldapaddmt

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-T *number_threads*

Required. The number of threads for concurrently processing entries.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-f *ldif_filename* | -X *dsml_filename*

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See Appendix A, "LDIF File Format" on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See "Adding Data to the Directory Using a DSML File" on page 4-15 for more information about formatting a DSML file.

-b

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

-c

Optional. Proceeds in spite of errors. All errors will be reported. If the `-c` argument is not used, the tool will stop when an error occurs.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-k | -K

Optional. The `-k` argument authenticates using Kerberos authentication instead of simple authentication. To enable this option, you must compile with KERBEROS defined.You must already have a valid ticket granting ticket. Use the `-K` argument if you want to only perform the first step of the Kerberos bind.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for ldapaddmt

Using the `ldapaddmt` tool, you can perform the following task:

- Adding Concurrent Entries to the Directory Using an LDIF File

Adding Concurrent Entries to the Directory Using an LDIF File

You can use `ldapaddmt` to add concurrent entries or schema information to the directory from an LDIF file. The file must be correctly formatted. See Appendix A, "LDIF File Format" on page A-1 for information about formatting an LDIF file.

Example:

```
ldapaddmt -h myhost.company.com -D "cn=orcladmin" -w password -T 5 -p 389 -f
~/myfiles/input.ldif -v
```

Related Command-Line Tools for ldapaddmt

- See "ldapadd" on page 4-12
- See "bulkload" on page 4-3

ldapbind

The `ldapbind` command-line tool enables you to see whether you can authenticate a client to a server.

Syntax for ldapbind

```
ldapbind -h oid_hostname -D "binddn" -w password [-p ldap_port] [-V ldap_version]
[-n] [-O "auth"] [-Y "DIGEST-MD5|EXTERNAL"] [-R SASL_realm]
[-U SSL_auth_mode {-W wallet_location -P wallet_password}] [-E character_set]
```

Arguments for ldapbind

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-O "auth"

Optional. Specifies SASL security properties. The security property supported is `-O "auth"`. This security property is for `DIGEST-MD5` SASL mechanism. It enables authentication with no data integrity or data privacy.

-Y "DIGEST-MD5 | EXTERNAL"

Optional. Specifies a **Simple Authentication and Security Layer (SASL)** mechanism. The following mechanisms are supported:

- `DIGEST-MD5`
- `EXTERNAL` - The SASL authentication in this mechanism is done on top of two-way SSL authentication. In this case the identity of the user stored in the SSL wallet is used for SASL authentication.

-R *SASL_realm*

Optional. A SASL realm.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for ldapbind

Using the `ldapbind` tool, you can perform the following task:

- Validating Authentication Credentials

Validating Authentication Credentials

The following example shows how to validate the authentication credentials used to bind to the directory server when using SSL.

Example:

```
ldapbind -h myhost.company.com -D "cn-orcladmin" -w password -p 636 -U 2
-W "file:/home/my_dir/my_wallet" -P password
```

Related Command-Line Tools for ldapbind

- N/A

ldapcompare

The `ldapcompare` command-line tool enables you to compare an attribute value that you specify on the command line to the attribute value in a directory entry.

Syntax for ldapcompare

```
ldapcompare -h oid_hostname -D "binddn" -w password [-Y "proxy_dn"] [-p ldap_port]
-a attribute_name -b "basedn" -v "attribute_value" [-U SSL_auth_mode {-W
wallet_location -P wallet_password}] [-d debug_level] [-E character_set]
```

Arguments for ldapcompare

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-Y "*proxy_dn*"

Optional. The DN of a proxy user. After binding to the directory, the add operation will be performed as this user.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-a *attribute_name*

Required. The attribute for which to perform the comparison of values.

-b "*basedn*"

Required. The DN of the entry for which to perform the comparison.

-v "*attribute_value*"

Required. The attribute value that you want to compare to the value in the entry.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.

- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for ldapcompare

Using `ldapcompare` you can perform the following task:

- Comparing Attribute Values for an Entry

Comparing Attribute Values for an Entry

The following example shows how to check an entry for a person named *Anne Smith* to see if her *title* is *Manager*.

Example:

```
ldapcompare -h myhost.company.com -D "cn=orcladmin" -w password -p 389 -a title -b
"cn=Anne Smith,ou=Sales,o=IMC,c=US" -v "Manager"
```

Related Command-Line Tools for ldapcompare

- N/A

ldapdelete

The `ldapdelete` command-line tool enables you to remove entire entries from the directory.

> **See Also:** For information on using attribute aliases with ldapdelete refer to the "Attribute Aliases In the Directory" section in *Oracle Internet Directory Administrator's Guide*

Syntax for ldapdelete

```
ldapdelete -h oid_hostname -D "binddn" -w password [-Y proxy_dn] [-p ldap_port]
[-V ldap_version] {-f ldif_filename | "entry_dn"} [-n] [-M] [-v] [-O
ref_hop_limit] [-k|-K] [-U SSL_auth_mode {-W wallet_location -P wallet_password}]
[-E character_set]
```

Arguments for ldapdelete

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-Y "*proxy_dn*"

Optional. The DN of a proxy user. After binding to the directory, the add operation will be performed as this user.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-f *ldif_filename* | "*entry_dn*"

Required. The full path and file name of the input file that contains the entry DNs you want to delete, or a single entry DN supplied on the command-line.

Use the `-f` argument to supply an LDIF file. See Appendix A, "LDIF File Format" on page A-1 for information on formatting an LDIF file.

To delete one entry, supply the DN of the entry in quotes.

-n

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-v

Optional. Runs the tool in verbose mode.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-k | -K

Optional. The `-k` argument authenticates using Kerberos authentication instead of simple authentication. To enable this option, you must compile with KERBEROS defined.You must already have a valid ticket granting ticket. Use the `-K` argument if you want to only perform the first step of the Kerberos bind.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for ldapdelete

Using `ldapdelete` you can perform the following tasks:

- Deleting a Single Entry
- Deleting Multiple Entries Using an LDIF File

Deleting a Single Entry

The following example shows how to delete an entry for a person named *Anne Smith*.

Example:

```
ldapdelete -h myhost.company.com -D "cn=orcladmin" -w password -p 389
"cn=Anne Smith,ou=Sales,o=IMC,c=US"
```

Deleting Multiple Entries Using an LDIF File

The following example shows how to delete many entries at once by supplying an LDIF file that contains the DNs of the entries to delete. See Appendix A, "LDIF File Format" on page A-1 for information about formatting an LDIF file.

Example:

```
ldapdelete -h myhost.company.com -D "cn=orcladmin" -w password -p 389
-f /home/mydir/delete.ldif
```

Related Command-Line Tools for ldapdelete

- See bulkdelete on page 4-1

ldapmoddn

The `ldapmoddn` command-line tool enables you to change the RDN of an entry, or to move an entry to a new parent node in the directory tree.

> **See Also:** For information on using attribute aliases with ldapmoddn refer to the "Attribute Aliases In the Directory" section in *Oracle Internet Directory Administrator's Guide*

Syntax for ldapmoddn

```
ldapmoddn -h oid_hostname -D "binddn" -w password [-p ldap_port] [-V ldap_version]
-b "base_dn" {-R "new_rdn"|-N "new_parent"} [-r] [-M] [-O ref_hop_limit]
[-U SSL_auth_mode {-W wallet_location -P wallet_password}] [-E character_set]
```

Arguments for ldapmoddn

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-b "*base_dn*"

Required. The DN of the entry to be moved to a new parent DN or have its RDN updated.

-R "*new_rdn*" | -N "*new_parent*"

Required. The action to perform. Use the `-R` argument to change the RDN of the entry. Use the `-N` argument to move the entry to a new parent node in the directory tree.

-r

Optional. Specifies that the old RDN is not retained as a value in the modified entry. If not included, the old RDN is retained as an attribute in the modified entry.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for ldapmoddn

Using the `ldapmoddn` command-line tool, you can perform the following tasks:

- Changing the RDN of an Entry
- Moving an Entry

Changing the RDN of an Entry

The following example shows how to change the RDN of an entry from *Mary Smith* to *Mary Jones*.

Example:

```
ldapmoddn -h myhost.company.com -D "cn=orcladmin" -w password -p 389 -b "cn=Mary
Smith,dc=Americas,dc=IMC,dc=com" -R "cn=Mary Jones" -r
```

Moving an Entry

The following example shows how to move an entry to another parent node in the directory subtree. The entry with the RDN of *Mary Smith* is moved from the *dc=Americas* parent node to the *dc=Australia* parent node.

Example:

```
ldapmoddn -h myhost.company.com -D "cn=orcladmin" -w password -p 389 -b "cn=Mary
Smith,dc=Americas,dc=IMC,dc=com" -N "dc=Australia,dc=IMC,dc=com"
```

Related Command-Line Tools for ldapmoddn

- See "ldapmodify" on page 4-27

ldapmodify

The `ldapmodify` command-line tool enables you to add, delete, or replace attributes for entries by supplying an LDIF file as input. You can also delete or add entries using `ldapmodify`.

See Appendix A, "LDIF File Format" on page A-1 for more information about the correct formatting of LDIF files.

> **See Also:** For information on using attribute aliases with ldapmodify refer to the "Attribute Aliases In the Directory" section in *Oracle Internet Directory Administrator's Guide*

Syntax for ldapmodify

```
ldapmodify -h oid_hostname -D "binddn" [-Y "proxy_dn"] -w password [-p ldap_port]
[-V ldap_version] {-f ldif_filename | -X dsml_filename}  [-a] [-b]
[-c [-o log_file_name]] [-n] [-v] [-M] [-O ref_hop_limit] [-i 1|0] [-k|-K]
[-U SSL_auth_mode {-W wallet_location -P wallet_password}] [-E character_set]
[-d debug_level]
```

Arguments for ldapmodify

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-Y "*proxy_dn*"

Optional. The DN of a proxy user. After binding to the directory, the add operation will be performed as this user.

-w *password*

Required. The user password needed to bind to the directory.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-f *ldif_filename* | -X *dsml_filename*

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See Appendix A, "LDIF File Format" on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See "Adding Data to the Directory Using a DSML File" on page 4-15 for more information about formatting a DSML file.

-a

Optional. Denotes that the LDIF or DSML input file has new entries to be added.

-b

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

-c

Optional. Proceeds in spite of errors. All errors will be reported. If the `-c` argument is not used, the tool will stop when an error occurs.

-n

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

-v

Optional. Runs the tool in verbose mode.

-o *log_file_name*

Optional. Used with the `-c` argument. Writes the LDIF entries with errors to a log file. Specify the full path and name of the log file.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-i 1 | 0

Optional. Specifies whether or not to bind as the current user when following referrals. 1 means bind as the current user, 0 means bind anonymously. The default is 0 (zero).

-k | -K

Optional. The `-k` argument authenticates using Kerberos authentication instead of simple authentication. To enable this option, you must compile with KERBEROS defined.You must already have a valid ticket granting ticket. Use the `-K` argument if you want to only perform the first step of the Kerberos bind.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

Tasks and Examples for ldapmodify

Using the `ldapmodify` command-line tool, you can perform the following tasks:

- Modifying the Directory Schema
- Modifying an Entry

Modifying the Directory Schema

First, you must prepare your LDIF file to define the new schema elements you want to add. See "LDIF Format for Adding Schema Elements" on page A-5 for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the new schema definitions into the directory schema.

Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -w password -p 389
-f /home/myfiles/modify.ldif  -v
```

Modifying an Entry

To modify the attributes or attribute values for an entry, you must first prepare your LDIF file correctly. See "LDIF Format for Modifying Entries" on page A-3 for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the changes.

Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -w password -p 389
-f /home/myfiles/modify.ldif  -v
```

Related Command-Line Tools for ldapmodify

- See "ldapadd" on page 4-12
- See "ldapdelete" on page 4-23
- See "ldapmoddn" on page 4-25

ldapmodifymt

The `ldapmodifymt` command-line tool is similar to `ldapmodify` in that it enables you to add, delete, or modify entries by supplying an LDIF file as input. However, `ldapmodifymt` runs in multi-threaded mode allowing you to operate on multiple entries concurrently.

See Appendix A, "LDIF File Format" on page A-1 for more information about the correct formatting of LDIF files.

Syntax for ldapmodifymt

```
ldapmodifymt -h oid_hostname -D "binddn" -w password [-p ldap_port]
[-V ldap_version] -T number_of_threads {-f ldif_filename | -X dsml_filename}
[-a] [-b] [-c [-o log_file_name]] [-M] [-O ref_hop_limit] [-k|-K]
[-U SSL_auth_mode {-W wallet_location -P wallet_password}] [-E character_set]
[-d debug_level]
```

Arguments for ldapmodifymt

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-T *number_threads*

Required. The number of threads for concurrently processing entries.

-f *ldif_filename* | -X *dsml_filename*

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See Appendix A, "LDIF File Format" on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See "Adding Data to the Directory Using a DSML File" on page 4-15 for more information about formatting a DSML file.

-a

Optional. Denotes that the LDIF file has entries to be added.

-b

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

-c

Optional. Proceeds in spite of errors. All errors will be reported. If the `-c` argument is not used, the tool will stop when an error occurs.

-o *log_file_name*

Optional. Used with the `-c` argument. Writes the LDIF entries with errors to a log file. Specify the full path and name of the log file.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-k | -K

Optional. The `-k` argument authenticates using Kerberos authentication instead of simple authentication. To enable this option, you must compile with KERBEROS defined.You must already have a valid ticket granting ticket. Use the `-K` argument if you want to only perform the first step of the Kerberos bind.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-E character_set

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server

- 117440511 — All possible operations and data

Tasks and Examples for ldapmodifymt

Using the `ldapmodifymt` command-line tool, you can perform the following task:

- Modifying Multiple Entries Concurrently

Modifying Multiple Entries Concurrently

To modify multiple entries at once, you must first prepare your LDIF file correctly. See Appendix A, "LDIF File Format" on page A-1 for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodifymt` tool to import the changes.

The following example uses five concurrent threads to modify the entries specified in the file `/home/myfiles/modify.ldif`.

Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -w password -p 389
-T 5 -f /home/myfiles/modify.ldif  -v
```

Related Command-Line Tools for ldapmodifymt

- See "ldapaddmt" on page 4-16
- See "ldapmodify" on page 4-27

ldapsearch

The ldapsearch command-line tool enables you to search for and retrieve specific entries in the directory.

The LDAP filter that you use to search for entries must be compliant with the Internet Engineering Task Force (IETF) standards as specified in RFC 2254. Refer to the IETF Web site at `http://www.ietf.org` for more information about the standard filter format. Oracle Internet Directory supports all elements of RFC 2254 except for extensible matching.

Note: Various UNIX shells interpret some characters—for example, asterisks (*)—as special characters. Depending on the shell you are using, you may need to escape these characters.

See Also: For information on using attribute aliases with ldapsearch refer to the "Attribute Aliases In the Directory" section in *Oracle Internet Directory Administrator's Guide*

Syntax for ldapsearch

```
ldapsearch -h oid_hostname -D "binddn" -w password [-Y "proxy_dn"] [-p ldap_port]
[-V ldap_version] -b "basedn" {-s base|one|sub} {"filter_string" [attributes]|-f
input_file} [-F separator] [-T [-]sort_attribute] [-j page_size] [-A] [-a
never|always|search|find] [-S] [-R] [-i 1|0] [-t] [-u] [-L|-X] [-B] [-M] [-v] [-n]
[-l time_limit] [-z size_limit] [-O ref_hop_limit] [-U SSL_auth_mode {-W
wallet_location -P wallet_password}] [-d debug_level]
[-E character_set][-c]
```

Arguments for ldapsearch

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-Y "*proxy_dn*"

Optional. The DN of a proxy user. After binding to the directory, the add operation will be performed as this user.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-V *ldap_version*

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

-b "*basedn*"

Required. The base DN for the search.

-s base | one | sub

Required. The scope of the search within the DIT. The options are:

- `base` - Retrieves a particular directory entry. Along with this search depth, you use the search criteria bar to select the attribute `objectClass` and the filter `Present`.
- `one` - Limits your search to all entries beginning one level down from the root of your search.
- `sub` - Searches entries within the entire subtree, including the root of your search.

"*filter_string*" [*attributes*] | -f *input_file*

Required. Supply a single filter on the command-line within quotes followed by the attribute names whose values you want returned. Separate attributes with a space. If you do not list any attributes, all attributes are retrieved.

You can also supply an input file with the `-f` argument that contains a sequence of search operations to perform.

-F *separator*

Optional. Enables you to choose a separator to use between attribute names and values in the search output. The default is = (equal sign).

-T [-]*sort_attribute*

Optional. Instructs the tool to send a sort request to the server. The server returns entries sorted on the attribute, *sort_attribute*. A dash (-) before *sort_attribute* instructs the tool to sort the entries in reverse order.

-j *page_size*

Optional. Instructs the tool to send a page request to the server. The server returns paged entries with pages of size, *page_size*.

-A

Optional. Retrieves attribute names only (no values).

-a never | always | search | find

Optional. Specifies alias dereferencing. An alias entry in an LDAP directory is an entry that points to another entry. Following an alias pointer is known as dereferencing an alias. The options are:

- `never` - Never dereference alias entries. Choose this option to improve search performance if there are no alias entries in the directory that require dereferencing.
- `always` - Always dereference aliases. This selection is the default.
- `search` - Dereference alias entries subordinate to a specified search base, but do not dereference an alias search base entry.
- `find` - Deference an alias entry for a specified search base, but do not dereference alias entries subordinate to the search base.

-S *attr*

Optional. Sorts the results by the attribute specified.

-R

Optional. Disables the automatic following of referrals.

-i 1 | 0

Optional. Specifies whether or not to bind as the current user when following referrals. 1 means bind as the current user, 0 means bind anonymously. The default is 0 (zero).

-t

Optional. Writes files to `/tmp`.

-u

Optional. Includes user-friendly names in the output.

-L | -X

Optional. Prints entries in LDIF (`-L`) or DSML format (`-X`).

-B

Optional. Allows printing of non-ASCII values.

-M

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

-n

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

-v

Optional. Runs the tool in verbose mode.

-l *time_limit*

Optional. The maximum time in seconds to wait for an `ldapsearch` command to complete.

-z *size_limit*

Optional. The maximum number of entries to return.

-O *ref_hop_limit*

Optional. The number of referral hops that a client should process. Defaults to 5.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

-E *character_set*

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

-C

Optional. ldapsearch -C option causes ldapsearch to traverse a hierarchy and report direct memberships. The ldapsearch -C option essentially includes the CONNECT_BY control (2.16.840.1.113894.1.8.3) in the request sent to the client. ldapsearch doesn't have any means to pass values with a control. So, it sends the CONNECT_BY control without values. In this case the default values are assumed, that is, the hierarchy-establishing attribute name is obtained from the filter, and the number of levels is 0. Thus, the -C option can only be used to fetch *all containers of a containee* queries, for example, fetch all groups of a user, fetch all employees of a manager and so forth. Also, all levels of the hierarchy are traversed. For more information refer to Table 7–2.

> **See Also:** The "Performing Hierarchical Searches" section in Oracle Identity Management Application Developer's Guide

Tasks and Examples for ldapsearch

Using the `ldapsearch` command-line tool, you can perform the following tasks:

- Performing a Base Object Search
- Performing a One-Level Search
- Performing a Subtree Search
- Searching for Attribute Values of Entries
- Searching for Entries with Attribute Options
- Searching for All User Attributes and Specified Operational Attributes

- Searching for Entries (More Examples)

Performing a Base Object Search

The following example performs a base-level search on the directory from the root.

- `-b` specifies base DN for the search, root in this case.
- `-s` specifies whether the search is a base search (`base`), one level search (`one`) or subtree search (`sub`).
- `"objectclass=*"` specifies the filter for search.

Example:

```
ldapsearch -p 389 -h myhost -b "" -s base -v "objectclass=*"
```

Performing a One-Level Search

The following example performs a one level search starting at `"ou=HR, ou=Americas, o=IMC, c=US"`.

Example:

```
ldapsearch -p 389 -h myhost -b "ou=HR, ou=Americas, o=IMC, c=US" -s one \
           -v "objectclass=*"
```

Performing a Subtree Search

The following example performs a subtree search and returns all entries having a DN starting with `"cn=us"`.

Example:

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*"
```

Searching for Attribute Values of Entries

The following example returns only the `DN` attribute values of the matching entries:

Example:

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "objectclass=*" dn
```

The following example retrieves only the distinguished name along with the surname (`sn`) and description (`description`) attribute values:

Example:

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description
```

The following example retrieves the distinguished name (dn), surname (`sn`), and description (`description`) attribute values. The entries are sorted by surname (`sn`). There are 10 entries returned per page.

Example:

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description -T
sn -j 10
```

Searching for Entries with Attribute Options

The following example retrieves entries with common name (cn) attributes that have an option specifying a language code attribute option. This particular example retrieves entries in which the common names are in French and begin with the letter R.

Example:

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

Suppose that, in the entry for John, no value is set for the cn;lang-it language code attribute option. In this case, the following example does not return John's entry:

Example:

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

Searching for All User Attributes and Specified Operational Attributes

The following example retrieves all user attributes and the createtimestamp and orclguid operational attributes:

Example:

```
ldapsearch -p 389 -h myhost -b "ou=Benefits,ou=HR,ou=Americas,o=IMC,c=US" \
           -s sub "cn=Person*" "*" createtimestamp orclguid
```

The following example retrieves entries modified by Anne Smith:

Example:

```
ldapsearch -h sun1 -b "" "(&(objectclass=*)(modifiersname=cn=Anne
Smith))"
```

The following example retrieves entries modified between 01 April 2001 and 06 April 2001:

Example:

```
ldapsearch -h sun1 -b "" \
           "(&(objectclass=*)(modifytimestamp >= 20000401000000) \
           (modifytimestamp <= 20000406235959))"
```

Note: Because modifiersname and modifytimestamp are not indexed attributes, use catalog.sh to index these two attributes. Then, restart the Oracle directory server before issuing the two previous ldapsearch commands.

Searching for Entries (More Examples)

Each of the following examples searches on port 389 of host sun1, and searches the whole subtree starting from the DN "ou=hr,o=acme,c=us".

The following example searches for all entries with any value for the objectclass attribute.

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=*"
```

The following example searches for all entries that have orcl at the beginning of the value for the objectclass attribute.

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=orcl*"
```

The following example searches for entries where the `objectclass` attribute begins with `orcl` and `cn` begins with `foo`.

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" \
          -s subtree "(&(objectclass=orcl*)(cn=foo*))"
```

The following example searches for entries in which `cn` begins with `foo` or `sn` begins with `bar`.

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" \
          -s subtree "(|(cn=foo*)(sn=bar*))"
```

The following example searches for entries in which `employeenumber` is less than or equal to 10000.

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" \
           -s subtree "employeenumber<=10000"
```

Related Command-Line Tools for ldapsearch

- See "ldapcompare" on page 4-21
- See "catalog" on page 4-10

ldifmigrator

The Oracle Internet Directory Data Migration Tool (`ldifmigrator`) is used to convert LDIF files output from other directories or application-specific repositories into a format recognized by Oracle Internet Directory. The Data Migration Tool takes as input an LDIF file containing substitution variables, and outputs an LDIF file suitable for loading into Oracle Internet Directory.

See "LDIF Format for Migrating Entries" on page A-6 for the correct format of the LDIF input file for this tool.

Syntax for ldifmigrator

```
ldifmigrator "input_file=filename" "output_file=filename"
[-lookup -h oid_hostname -D "binddn" -w password [-p ldap_port]
[subscriber=subscriberDN]] ["s_VariableName1=replacement_value"
"s_VariableName2=replacement_value"...] [-load -reconcile
SAFE|SAFE_EXTENDED|NORMAL]
```

Arguments for ldifmigrator

"input_file=*filename*"

The full path and file name of the LDIF file that contains directory entry data and one or more substitution variables.

"output_*file=filename*"

The full path and file name of the output file produced by the `ldifmigrator` tool.

-lookup

If this flag is specified, then values of certain substitution variables will be obtained by looking up the correct values in the directory server. See "Substitution Variables for

Migration Input Files" on page A-6 for a list of substitution variables that can be looked up.

-h *oid_hostname*

Required if the `-lookup` flag is used. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required if the `-lookup` flag is used. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required if the `-lookup` flag is used. The user password needed to bind to the directory.

-p *ldap_port*

Optional if the `-lookup` flag is used. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

subscriber=*subscriberDN*

Optional. The subscriber whose attribute values will be used in place of the substitution variables. If not specified, then the default identity management realm specified in the Root Oracle Context will be used.

"s_*VariableName=replacement_value*"

Optional. You can specify a value for a substitution variable on the command-line. See "Substitution Variables for Migration Input Files" on page A-6 for instructions on adding a substitution variable to the input LDIF file. The `ldifmigrator` tool will replace all occurrences of the variable with the value you specify.

-load

Optional. Loads the data output by the `ldifmigrator` tool directly into Oracle Internet Directory. If an entry is already present in the directory then that directory entry will be logged to the file. The addition of the directory entries could fail for other reasons as well, for instance not enough permission to add or parent entry not being present.

-reconcile SAFE | SAFE_EXTENDED | NORMAL

Optional. The `-reconcile` option enables you to specify different modes if the tool tries to load data for entries that already exist, or modify attributes of entries that may have conflicts. The following modes are available:

- **SAFE** - This mode only adds new entries that don't exist or appends new attributes to existing entries.
- **SAFE-EXTENDED** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If you try to add a new value for existing attributes, then it will add it to the existing set of values.
- **NORMAL** - This mode applies all directives as intended, overwriting any conflicting attributes or entries with the data specified in the `ldifmigrator` output.

See "Reconcile Options for Migrated Entries" on page A-8 for more information about LDIF directives supported by the `-reconcile` option.

Tasks and Examples for ldifmigrator

Using the `ldifmigrator` command-line tool, you can perform the following tasks:

- Using the Data Migration Tool in Lookup Mode
- Overriding Data Migration Values in Lookup Mode
- Using the Data Migration Tool by Supplying Your Own Values
- Loading and Reconciling Data Using the Data Migration Tool

See "LDIF Format for Migrating Entries" on page A-6 for examples of correctly formatted LDIF input files for use with the Data Migration Tool.

Using the Data Migration Tool in Lookup Mode

In this example, Oracle Internet Directory server is present in the environment, and the migration tool will lookup the directory server to figure out certain substitution variables specified in the LDIF input file.

Example:

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
               -lookup "host=ldap.acme.com" "subscriber=acme" \
               "s_UserOrganization=Development"
```

Overriding Data Migration Values in Lookup Mode

In some cases, you want to use the lookup mode but would also like to override the values of one or more of the pre-defined substitution variables. This can be done by specifying the override value in the command-line. The following command line shows how one can set the `UserNickNameAttribute` to `cn` overriding the default of `uid`:

Example:

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
              -lookup "host=ldap.acme.com" "subscriber=acme" \
             "s_UserOrganization=Development" "s_UserNicknameAttribute=cn"
```

Using the Data Migration Tool by Supplying Your Own Values

The following example shows how you can specify your own values for substitution variables found in the LDIF input file, rather than using lookup mode.

Example:

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif"  \
              "s_UserContainerDN=cn=Users,o=Acme,dc=com" \
              "s_UserNicknameAttribute=uid" "s_UserOrganization=Development"
```

Loading and Reconciling Data Using the Data Migration Tool

The Data Migration Tool gives your the option of loading the data directly into Oracle Internet Directory. Use the `-load` and `-reconcile` options to load data and safely reconcile any conflicts.

Example:

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
               -lookup "host=ldap.acme.com" "subscriber=acme" \
               "s_UserOrganization=Development"
               -load -reconcile SAFE
```

Related Command-Line Tools for ldifmigrator

- See "ldapadd" on page 4-12
- See "ldapmodify" on page 4-27
- See "ldifwrite" on page 4-45

Error Messages for ldifmigrator

The Data Migration Tool can display these error messages:

Table 4–1 Error Messages of the Data Migration Tool

Message	Reason	Remedial Action
Environment variable *ORACLE_HOME* not defined	*ORACLE_HOME* is not defined.	Set the environment variable *ORACLE_HOME*
Error while parsing the input parameters. Please verify	Not all the required parameters are provided. The required parameters are Input_File, Output_File and at least one substitution variable	Specify the input parameters properly. Use the `-help` option to print the usage.
Input_File parameter not specified. Please specify	Input_File parameter is a mandatory parameter.	Specify the input parameters properly. Use the `-help` option to print the usage.
Output_File parameter not specified. Please specify	Output_File parameter is a mandatory parameter.	Specify the input parameters properly. Use the `-help` option to print the usage.
The specified input file does not exist	The specified file location is invalid.	Check the input file path
Check the input file. Zero byte input file	The input file does not contain any entries.	Provide a valid file with pseudo LDIF entries
Cannot create the output file. Output file already exists	The output file already exists	Check the Output_File flag
Access denied, cannot read from the input file	The specified input file does not have read permission	Check the read permission of the input file.
Access denied, cannot create the output file	You do not have permission to create the output file.	Check the permission of the directory under which the output file needs to be created.
Directory server name not specified. When -lookup option is used the host parameter should be specified	When the `-lookup` option is specified, the host parameter is mandatory.	Specify the host parameter.
Bind Dn parameter name not specified. When -lookup option is used the dn parameter should be specified	When the `-lookup` option is specified, the DN parameter is mandatory.	Specify the DN parameter.
The port number specified is invalid	The port number should be a numeric value.	Check the port number parameter
Unable to establish connection to directory. Please verify the input parameters: host, port, dn & password	The directory server may not be running on the specified host and port, or credentials may be invalid.	Check the host, port, DN and password parameters. Check `$`*`ORACLE_HOME`*`/ldap/install/LDIFMig_YYYY_MM_DD_HH_SS.log file`.

Table 4–1 (Cont.) Error Messages of the Data Migration Tool

Message	Reason	Remedial Action
Naming exception occurred while retrieving the subscriber information from the directory. Please verify the input parameters	The specified identity management realm does not exist in the directory	Check the realm parameter
Not all the substitution variables are defined in the directory server specified	If the identity management realm entry does not contain the required attributes, then this error occurs.	Check the realm entry in the directory
Error occurred while migrating LDIF data to Oracle Internet Directory	This might occur if something goes wrong in the middle of a process—for example, a failure of the directory server or disk.	Report the error message to the administrator

When an error condition occurs, the log messages are logged to this file: *ORACLE_HOME*/ldap/install/LDIFMig_YYYY_MM_DD_HH_SS.log.

ldifwrite

The `ldifwrite` command-line tool enables you to convert to LDIF all or part of the information residing in an Oracle Internet Directory. Once you have converted the information, you can load it into a new node in a replicated directory or another node for backup storage.

> **Note:** The `ldifwrite` tool output does not include operational data of the directory itself—for example, `cn=subschemasubentry`, `cn=catalogs`, and `cn=changelog entries`. To export these entries into LDIF format, use `ldapsearch` with the `-L` flag.

The `ldifwrite` tool performs a subtree search, including all entries below the specified DN, including the DN itself.

Syntax for ldifwrite

```
ldifwrite connect=connect_string basedn=Base_DN ldiffile=LDIF_Filename
[filter=LDAP_Filter] [threads=num_of_threads] [debug="TRUE"|"FALSE"]
[encode=character_set] [verbose="TRUE"|"FALSE"]
```

Arguments for ldifwrite

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in $*ORACLE_HOME*/network/admin. If not provided, defaults to the value of `$ORACLE_SID` environment variable.

basedn

Required. The base DN of the subtree to be written out in LDIF format.

If the base DN is a replication agreement entry, then you can back up part of the naming context based on the LDAP naming context configuration. Specify the replication agreement DN in this case.

ldiffile

Required. The full path and file name of the output LDIF file.

filter

Optional. This is the LDAP filter to be used. You can specify a filter to select entries that match a particular criteria. Only these entries would be written to the LDIF file.

threads

Optional. The number of threads used to read from the directory store and write to the LDIF output file. The default is the number of CPUs plus one.

debug

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `ldifwrite.log` file. This file can be found under `$ORACLE_HOME/ldap/log`.

encode

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

verbose

Optional. This is used to run the command in verbose mode.

Tasks and Examples for ldifwrite

Using the `ldifwrite` command-line tool, you can perform the following tasks

- Converting All Entries under a Naming Context to an LDIF File
- Converting a Partial Naming Context to an LDIF File
- Converting Entries that Match a Criteria to an LDIF File

Converting All Entries under a Naming Context to an LDIF File

The following example writes all the entries under `ou=Europe,o=imc,c=us` into the `output1.ldif` file.

The LDIF file and the intermediate file are always written to the current directory.

The `ldifwrite` tool includes the operational attributes of each entry in the directory, including `createtimestamp`, `creatorsname`, and `orclguid`.

When prompted for the Oracle Internet Directory password, enter the password of the ODS database user account. The default password is `ods`.

Example:

```
ldifwrite connect="nldap" basedn="ou=Europe, o=imc, c=us" file="output1.ldif"
```

Converting a Partial Naming Context to an LDIF File

The following example uses the following naming context objects defined in partial replication:

```
dn: cn=includednamingcontext000001,
 cn=replication namecontext,
 orclagreementid=000001,
 orclreplicaid=node replica identifier,
 cn=replication configuration
orclincludednamingcontexts: c=us
orclexcludednamingcontexts: ou=Americas, c=us
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

In this example, all entries under `c=us` are backed up except `ou=Americas,c=us`. The `userpassword` attribute is also excluded.

Example:

```
ldifwrite connect="nldap" basedn="cn=includednamingcontext000001, \
          cn=replication namecontext,orclagreementid=000001, \
          orclreplicaid=node replica identifier,cn=replication configuration" \
          file="output2.ldif"
```

Converting Entries that Match a Criteria to an LDIF File

The following example writes entries under `ou=users,o=test,c=us` that have `sn="Stuart"` to an output LDIF file, `output3.ldif`.

Example:

```
ldifwrite connect="nldap" basedn="ou=users, o= test, c=us" filter="sn=xyz"
ldiffile="output3.ldif"
```

Related Command-Line Tools for ldifwrite

- See "ldapsearch" on page 4-34
- See "ldifmigrator" on page 4-41
- See "bulkload" on page 4-3

upgradecert.pl

Starting with Release 10.1.2, a certificate hash value can be used to bind to Oracle Internet Directory. The introduction of this hash value requires that user certificates issued before Release 10.1.2 be updated in the directory. This is a post-upgrade step and it is required only if user certificates are provisioned in the directory. The `upgradecert.pl` tool is used for this purpose.

Before running the `upgradecert.pl` tool:

1. Make sure that the Oracle Internet Directory server instance is up and running.
2. Check that you are running Perl 5.6 or later. Run this command:

   ```
   perl -version
   ```

3. Make sure that the environment variable PERL5LIB is set to the proper PERL library location.

4. Check that you can run `ldapmodify` and `ldapsearch` from your command prompt.
5. Determine whether you have enough disk space to run the tool. The amount of disk space required depends upon the number of certificates stored.

Syntax for upgradecert.pl

```
perl $ORACLE_HOME/ldap/bin/upgradecert.pl -h oid_hostname -D "binddn" -w password
[-p ldap_port] [-t temp_dir]
```

Arguments for upgradecert.pl

-h *oid_hostname*

Required. The host name or IP address of the Oracle Internet Directory server.

-D "*binddn*"

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

-w *password*

Required. The user password needed to bind to the directory.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 389.

-t *temp_dir*

Optional. The location of the temporary working directory. This is where the log file is found. The default is `$ORACLE_HOME/ldap/log` if the `ORACLE_HOME` environment variable is set. If this variable is not set, the default is the current directory.

Tasks and Examples for upgradecert.pl

Using the `upgradecert.pl` tool, you can perform the following task:

- Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2

Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2

Example:

```
perl $ORACLE_HOME/ldap/bin/upgradecert.pl -h myhost.company.com -D "cn=orcladmin"
-w password
```

Related Command-Line Tools for upgradecert.pl

- N/A

5

Oracle Internet Directory Replication Management Tools

This chapter describes the following command-line tools used to administer Oracle Internet Directory replication:

- hiqretry.sh (Human Intervention Queue Retry Tool)
- hiqpurge.sh (Human Intervention Queue Purge Tool)
- oidcmprec (Oracle Internet Directory Compare and Reconcile Tool)
- remtool (Replication Environment Management Tool)

> **See Also:**
>
> - *Oracle Application Server Administrator's Guide*

hiqretry.sh

When a replication conflict arises, the Oracle Internet Directory replication server places the change in the retry queue and tries to apply it from there for a specified number of times. If it fails after that specified number, then the replication server puts the change in the human intervention queue. From there, the replication server repeats the change application process at less frequent intervals while awaiting your action.

At this point, you need to:

1. Examine the change in the human intervention queue.
2. Reconcile the conflicting changes using the Compare and Reconcile Tool (see "oidcmprec" on page 5-5).
3. Either place the change back into the retry queue (using `hiqretry.sh`) or into the purge queue (see "hiqpurge.sh" on page 5-3).

> **Note:** The Oracle Internet Directory server parameter `orclSizeLimit`, which is 1000 by default, limits the number of entries that the Human Intervention Queue Manipulation Tool can process. If you have more than 1000 entries in the human intervention queue, you must increase `orclSizeLimit`, or some entries will never be processed. Setting the parameter `orclSizeLimit` very high will impact server performance, because `orclSizeLimit` also controls the maximum number of entries to be returned by a search.

Syntax for hiqretry.sh

```
hiqretry.sh -connect connect_string {{-start change_number -end change_number }|
{-equal change_number }} -supplier supplier_node
```

Arguments for hiqretry.sh

-connect *connect_string*

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

-start *change_number*

When specifying a range of change numbers to move from the human intervention queue into the retry queue, this argument specifies the starting change number. If you skip this argument, then the tool moves all the changes with change numbers less than or equal to the specified end change number back to the retry queue.

-end *change_number*

When specifying a range of change numbers to move from the human intervention queue into the retry queue, this argument specifies the ending change number. If you skip this argument, then the tool moves all the changes with change numbers greater than or equal to the specified start change number back to the retry queue.

-equal *change_number*

This argument specifies a single change number to move from the human intervention queue to the retry queue. This argument cannot be used with the `-start` or `-end` arguments.

-s *supplier_node*

Required. Specifies the supplier node where the changes originate.

Tasks and Examples for hiqretry.sh

Using the `hiqretry.sh` command-line tool, you can perform the following tasks:

- Retrying a HIQ Change Log
- Retrying a Range of HIQ Change Logs
- Retrying all HIQ Change Logs from a Supplier

Retrying a HIQ Change Log

The following example shows how to move a single replication change log conflict from the human intervention queue (HIQ) back into the retry queue. It moves the change numbered `10519` coming from the supplier node `ldap_rep1`.

Example:

```
hiqretry.sh -connect oiddb1 -equal 10519 -supplier ldap_repl
```

Retrying a Range of HIQ Change Logs

The following example shows how to move a range of replication change log conflicts from the human intervention queue (HIQ) back into the retry queue. It moves changes numbered between `10324` to `10579` coming from the supplier node `ldap_rep1`.

Example:

```
hiqretry.sh -connect oiddb1 -start 10324 -end 10579 -supplier ldap_repl
```

Retrying all HIQ Change Logs from a Supplier

The following example shows how to move all replication change log conflicts originating from a certain supplier from the human intervention queue (HIQ) back into the retry queue. It moves changes coming from the supplier node `ldap_rep1`.

Example:

```
hiqretry.sh -connect oiddb1 -supplier ldap_repl
```

Related Command-Line Tools for hiqretry.sh

- See "hiqpurge.sh" on page 5-3
- See "oidcmprec" on page 5-5

hiqpurge.sh

When a replication conflict arises, the Oracle Internet Directory replication server places the change in the retry queue and tries to apply it from there for a specified number of times. If it fails after that specified number, then the replication server puts the change in the human intervention queue. From there, the replication server repeats the change application process at less frequent intervals while awaiting your action.

At this point, you need to:

1. Examine the change in the human intervention queue.
2. Reconcile the conflicting changes using the Compare and Reconcile Tool (see "oidcmprec" on page 5-5).
3. Either place the change back into the retry queue (see "hiqretry.sh" on page 5-1) or into the purge queue (using `hiqpurge.sh`).

Syntax for hiqpurge.sh

```
hiqpurge.sh -connect connect_string {{-start change_number -end change_number }|
{-equal change_number }} -supplier supplier_node
```

Arguments for hiqpurge.sh

-connect *connect_string*

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

-start *change_number*

When specifying a range of change numbers to move from the human intervention queue into the purge queue, this argument specifies the starting change number. If you skip this argument, then the tool moves all the changes with change numbers less than or equal to the specified end change number to the purge queue.

-end *change_number*

When specifying a range of change numbers to move from the human intervention queue into the purge queue, this argument specifies the ending change number. If you skip this argument, then the tool moves all the changes with change numbers greater than or equal to the specified start change number to the purge queue.

-equal *change_number*

This argument specifies a single change number to move from the human intervention queue to the purge queue. This argument cannot be used with the `-start` or `-end` arguments.

-s *supplier_node*

Required. Specifies the supplier node where the changes originate.

Tasks and Examples for hiqpurge.sh

Using the `hiqpurge.sh` command-line tool, you can perform the following tasks:

- Discarding a HIQ Change Log
- Discarding a Range of HIQ Change Logs
- Discarding all HIQ Change Logs from a Supplier

Discarding a HIQ Change Log

The following example shows how to move a single replication change log conflict from the human intervention queue (HIQ) into the purge queue. It moves the change numbered `10519` coming from the supplier node `ldap_rep1`.

Example:

```
hiqpurge.sh -connect oiddb1 -equal 10519 -supplier ldap_repl
```

Discarding a Range of HIQ Change Logs

The following example shows how to move a range of replication change log conflicts from the human intervention queue (HIQ) into the purge queue. It moves changes numbered between `10324` to `10579` coming from the supplier node `ldap_rep1`.

Example:

```
hiqpurge.sh -connect oiddb1 -start 10324 -end 10579 -supplier ldap_repl
```

Discarding all HIQ Change Logs from a Supplier

The following example shows how to move all replication change log conflicts originating from a certain supplier from the human intervention queue (HIQ) into the purge queue. It moves changes coming from the supplier node `ldap_rep1`.

Example:

```
hiqpurge.sh -connect oiddb1 -supplier ldap_repl
```

Related Command-Line Tools for hiqpurge.sh

- See "hiqretry.sh" on page 5-1

oidcmprec

The Compare and Reconcile Tool allows you to compare one Oracle Internet Directory with another, detect conflicts or discrepancies, and optionally resolve them. The directories being compared can be standalone directories or part of the same replication group. You can compare two individual entries, subtrees, or entire directories.

The `oidcmprec` tool can detect and resolve the following conflict scenarios:

- Entry only in source directory (`entos`)
- Entry only in destination directory (`entod`)
- Attribute only in source directory (`atros`)
- Attribute only in destination directory (`atrod`)
- Single-valued attribute differs (`svatrdif`)
- Multi-valued attribute differs (`mvatrdif`)
- Entry DN differs (`dndif`)

The `oidcmprec` tool can also detect and resolve the following schema conflict scenarios:

- Object class definition exists only in source directory (`odefos`)
- Object class definition exists only in destination directory (`odefod`)
- Object class definition different in source and destination directory (`odefdif`)
- Attribute definition exists only in source directory (`adefos`)
- Attribute definition exists only in destination directory (`adefod`)
- Attribute definition different in source and destination directory (`adefdif`)

Syntax for oidcmprec

```
oidcmprec operation=compare | reconcile | merge | merge_dryrun |userdefinedcr
          source=host:port/replication_dn_password
          destination=host:port/replication_dn_password
          base="'dn1' 'dn2' 'dn3' ..."
          [ dns2exclude="'edn1' 'edn2' 'edn3' ..."]
          [ scope=base | subtree | onelevel ]
          [ threads=number_of_worker_threads ]
          [ dnthreads=number_of_dn_threads ]
          [ excludeattr=space_separated_list_of_attributes_to_be_excluded |
            includeattr=space_separated_list_of_attributes_to_be_included ]
          [ compareby=remtool | ldapserver ]
          [ filename=file_name_without_extension_to_store_compare_report]
          [ entos=ignore | add | del | log2add | log2del | log ]
          [ entod=ignore | add | del | log2add | log2del | log ]
          [ atros=ignore | add | del | log2add | log2del | usenewer |
                   log2usenewer | useolder | log2useolder | usesmallguid |
                   log2usesmallguid | usebigguid | log2usebigguid | log ]
          [ atrod=ignore | add | del | log2add | log2del | usenewer |
                   log2usenewer | useolder | log2useolder | usesmallguid |
                   log2usesmallguid | usebigguid | log2usebigguid | log ]
          [ svatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest |
                     usenewer | log2usenewer | useolder | log2useolder |
                     usesmallguid | log2usesmallguid | usebigguid | log2usebigguid
                     | log ]
```

```
[ mvatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge
          | log2merge | usenewer | log2usenewer | useolder |
          log2useolder | usesmallguid | log2usesmallguid | usebigguid |
          log2usebigguid | log ]
[ dndif=ignore | usesrc | log2usesrc | usedest | log2usedest | log ]
[ odefos=ignore | add | log2add | del | log2del | log ]
[ odefod=ignore | add | log2add | del | log2del | log ]
[ odefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge |
         log2merge | log ]
[ adefos=ignore | add | log2add | del | log2del | log ]
[ adefod=ignore | add | log2add | del | log2del | log ]
[ adefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | log ]
[ verbose=t[rue] | f[alse] ]
[ force=t[rue] | f[alse] ]
[ help=t[rue] | f[alse] ]
[ paramfile=file_containing_parameters]
[ genchglog=d[efault] | t[rue] | f[alse] ]
[ contonerr = t[rue] | f[alse] ]
```

Arguments for oidcmprec

operation=compare | reconcile | merge | merge_dryrun | userdefinedcr

Required. The `operation` to perform. The `operation` argument can take the following values:

- `compare`: Compares the two directories, reports conflicts, and logs the changes that need to be applied to the destination directory to resolve conflicts.
- `reconcile`: Compares the two directories, resolves conflicts, and logs the changes applied to the destination directory to resolve conflicts.
- `merge`: Compares the two directories and synchronizes them, updates both the source and destination directories. The source directory wins in case of a conflict.
- `merge_dryrun`: Performs a dry run of the merge operation. Logs all changes that need to be made to synchronize the source and destination directories.
- `userdefinedcr`: Performs a user-defined `compare` and `reconcile` operation. Allows the user to choose the conflict resolution rules.

source=*host*:*port*/*replication_dn_password*

Required. The connection string used to bind to the source Oracle Internet Directory node. If you do not supply the argument on the command line, the tool will prompt you for the information. The connection string is composed of the following elements:

- The host name of the directory server that acts as the source directory
- The LDAP listening port of the directory server
- The password of the replication DN

destination=*host*:*port*/*replication_dn_password*

Required. The connection string used to bind to the destination Oracle Internet Directory node. If you do not supply the argument on the command line, the tool will prompt you for the information. The connection string is composed of the following elements:

- The host name of the directory server that acts as the destination directory
- The LDAP listening port of the directory server

- The password of the replication DN

base=" '*dn1*' '*dn2*' '*dn3*' ..."

Required. Specifies the Distinguished Names (DNs) from where the comparison operation begins. The `scope` argument determines if child entries and subtrees of the base DNs would be compared as well.

dns2exclude=" 'edn1' 'edn2' 'edn3' ..."

Optional. Specifies DNs that are to be excluded from the comparison operation. These DNs must be child entries or subtrees of the DNs specified in the `base` argument.

scope=base | subtree | onelevel

Optional. Specifies whether the child entries and subtrees of a base DN are also compared. The `scope` argument can take the following values:

- `base`: Only the DNs specified in the `base` argument are compared. This is the default value.
- `subtree`: Directory information trees (DITs) identified by the DNs specified in the `base` argument are compared.
- `onelevel`: Only the immediate children of the DNs specified in the `base` argument are compared.

threads=*number_of_worker_threads*

Optional. Specifies the number of worker threads that should be created. Worker threads are responsible for comparing entries, and reconciling the differences. One worker thread is created, by default.

If the `scope` is `base`, then the `threads` argument is ignored and it spawns one worker thread and one DN thread.

dnthreads=*number_of_dn_threads*

Optional. Specifies the number of DN threads that should be created. DN threads are responsible for collecting all DNs that need to be compared.

One DN thread is created, by default. The total number of DN threads and worker threads cannot exceed "6 * Number of CPUs - 2". If the total number of DN threads and worker threads exceeds the maximum value, the tool reduces both values proportionately to "6 * Number of CPUs - 2".

excludeattr=*space_separated_list_of_attributes_to_be_excluded* | includeattr=*space_separated_list_of_attributes_to_be_included*

Optional. Specifies the list of attributes to be excluded or included for comparison. You can either specify a list of attributes to be excluded, using `excludeattr`, or specify a list of attributes to be included, using `includeattr`.

All attributes are included by default, except the following operational attributes:

- `creatorsname`
- `createtimestamp`
- `modifiersname`
- `modifytimestamp`
- `orclentrydn`

- orclnormdn

> **Note:** The excludeattr and includeattr attributes cannot be used together, except when you use "*" for includeattr.

The option allows limited pattern matching. You can use *attributename** to match all attributes starting with *attributename*. You can also use *attributename;** to match all subtypes of attributename.

compareby=tool | ldapserver

Optional. Specifies whether the compare operation is performed by the tool or ldapserver. A compare operation performed by the tool is several times faster than a compare operation performed by ldapserver.

filename=*file_name*

Optional. Specifies a base name for the report files that would be generated by the tool. Do not specify an extension with the file name. The tool generates the following files:

- *file_name*.rpt: This file contains the DNs of all entries compared and the compare results. This file is known as the rpt file.
- *file_name*.s2d.ldif: This file contains all changes that were applied (or to be applied) to the destination directory. s2d stands for source directory to destination directory. This file is known as the s2d file.
- *file_name*.d2s.ldif: This file contains all changes that were applied (or to be applied) to the source directory. d2s stands for destination directory to source directory. This file is known as the d2s file.
- *file_name*.eos.rpt: This file lists DNs of entries that exist only in the source directory. eos stands for entries available only in the source directory. This file is known as the eos file.
- *file_name*.eod.rpt: This file lists DNs of entries that exist only in the destination directory. eod stands for entries available only in the destination directory. This file is known as the eod file.
- *file_name*.dif.rpt: This file lists the DNs that are different in the source and destination directories along with the names of the DN attributes that differ. This file is known as the dif file.
- *file_name*.err: This file contains all the error messages. It is known as the err file.

entos=ignore | add | del | log2add | log2del | log

Optional. Specifies the conflict resolution rule to use in case an entry exists only in the source directory. The following values are allowed:

- ignore: Ignore the conflict and take no action
- add: Add the entry to the peer directory
- del: Delete the entry from the directory
- log2add: Same as add except that the change is logged to an LDIF file and not directly effected in the peer directory
- log2del: Same as del except that the change is logged to an LDIF file and not directly effected in the directory

- `log`: Log the conflict in the report file and take no other action

The default value depends on the operation specified. Table 5–1shows the default values of the `entos` argument, corresponding to the operations specified.

Table 5–1 Default Values for the entos Argument

Operation	Default Value
`compare`	`log2add`
`reconcile`	`add`
`merge`	`add`
`merge_dryrun`	`log2add`
`userdefinedcr`	`ignore`

entod=ignore | add | del | log2add | log2del | log

Optional. Specifies the conflict resolution rule to use in case an entry exists only in the destination directory. The values allowed are the same as the `entos` argument.

The default value depends on the operation specified. Table 5–2 shows the default values of the `entod` argument, corresponding to the operations specified.

Table 5–2 Default Values for the entod Argument

Operation	Default Value
`compare`	`log2delete`
`reconcile`	`delete`
`merge`	`add`
`merge_dryrun`	`log2add`
`userdefinedcr`	`ignore`

atros=ignore | add | del | log2add | log2del | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log

Optional. Specifies the conflict resolution rule to use in case an attribute exists only in the source directory. The following values are allowed:

- `ignore`: Ignore the conflict and take no action
- `add`: Add the attribute to the corresponding entry in the peer directory
- `del`: Delete the attribute from the directory
- `log2add`: Same as `add`, except that the change is logged into an LDIF file and not directly effected in the peer directory.
- `log2del`: Same as `del` except that the change is logged into an LDIF file and not directly effected in the directory.
- `usenewer`: Check the `modifytimestamp` value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the newer `modifytimestamp` value wins. If the `modifytimestamp` values are the same, then the source directory wins.
- `log2usenewer`: Same as `usenewer` except that the change is logged into an LDIF file and not directly effected in the directory.

- useolder: Check the modifytimestamp value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the older modifytimestamp value wins. If the modifytimestamp values are the same, then the source directory wins.
- log2useolder: Same as useolder except that the change is logged to an LDIF file and not directly effected in the directory.
- usesmallguid: Check the GUID value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the smaller GUID value wins. The GUID values would be the same in the same replication group. This rule is intended for nonreplication environments. If the GUID values are the same in both directories, then the source directory wins.
- log2usesmallguid: Same as usesmallguid except that the change is logged into an LDIF file and not directly effected in the directory.
- usebigguid: Check the GUID value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the bigger GUID value wins. The GUID values would be the same in the same replication group. This rule is intended for nonreplication environments. If the GUID values are the same in both directories, then the source directory wins.
- log2usebigguid: Same as usebigguid except that the change is logged into an LDIF file and not directly effected in the directory.
- log: Log the conflict in the report file and take no other action.

The default value depends on the operation specified. Table 5–3 shows the default values of the atros argument, corresponding to the operations specified.

Table 5–3 Default Values for the atros Argument

Operation	Default Value
compare	log2add
reconcile	add
merge	add
merge_dryrun	log2add
userdefinedcr	ignore

atrod=ignore | add | del | log2add | log2del | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log

Optional. Specifies the conflict resolution rule to use in case an attribute exists only in the destination directory. The values allowed are the same as the atros argument.

The default value depends on the operation specified. Table 5–4 shows the default values of the atrod argument, corresponding to the operations specified.

Table 5–4 Default Values for the atrod Argument

Operation	Default Value
compare	log2delete
reconcile	delete
merge	add
merge_dryrun	log2add

Table 5–4 (Cont.) Default Values for the atrod Argument

Operation	Default Value
userdefinedcr	ignore

svatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log

Optional. Specifies the conflict resolution rule to use when a single-valued attribute for an entry is different in the two directories. The following values are allowed for the svatrdif argument:

- ignore: Ignore the conflict and take no action
- usesrc: Replace the value of the attribute in the destination directory with the value of the attribute in the source directory
- log2usesrc: Same as usesrc, except that the change is logged into an LDIF file and not directly effected in the destination directory
- usedest: Replace the value of the attribute in the source directory with the value of the attribute in the destination directory
- log2usedest: Same as usedest except that the change is logged into an LDIF file and not directly effected in the source directory
- usenewer: If the modifystamp value of the attribute in the source directory is newer than the destination directory, then update the attribute value in the destination directory. If the modifystamp value of the attribute in the destination directory is newer, then change the attribute value in the source directory. If the modifystamp values in both directories are the same, then the source directory wins.
- log2usenewer: Same as usenewer except that the change is logged into an LDIF file and not directly effected in the directory.
- useolder: If the modifystamp value of the attribute in the source directory is older than the destination directory, then update the attribute value in the destination directory. If the modifystamp value of the attribute in the destination directory is older, then change the attribute value in the source directory. If the modifystamp values in both directories are the same, then the source directory wins.
- log2useolder: Same as useolder except that the change is logged into an LDIF file and not directly effected in the directory.
- usesmallguid: If the source directory entry's GUID is smaller than the destination directory entry's GUID, then update the attribute in the destination directory. If the destination directory entry's GUID is smaller, then update the attribute in the source directory. If the GUID values are the same, then the source directory wins. This rule is meant for nonreplication environments, as the GUID values would be the same in the same replication group.
- log2usesmallguid: Same as usesmallguid except that the change is logged into an LDIF file and not directly effected in the directory.
- usebigguid: If the source directory entry's GUID is bigger than the destination directory entry's GUID, then update the attribute in the destination directory. If the destination directory entry's GUID is bigger, then update the attribute in the source directory. If the GUID values are the same, then the source directory wins. This

rule is meant for nonreplication environments, as the GUID values would be the same in the same replication group.

- log2usebigguid: Same as usebigguid except that the change is logged into an LDIF file and not directly effected in the directory.
- log: Log the conflict in the report file and take no other action

The default value depends on the operation specified. Table 5–5 shows the default values of the svatrdif argument, corresponding to the operations specified.

Table 5–5 Default Values for the svatrdif Argument

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	usesrc
merge_dryrun	log2usesrc
userdefinedcr	ignore

mvatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge | log2merge | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log

Optional. Specifies the conflict resolution rule to use when a multivalued attribute for an entry is different in the two directories. The values allowed are the same as the svatrdif argument. This argument also has other values that do not exist for the svatrdif argument. The following are values specific to the mvatrdif argument:

- merge: The missing attribute values in the destination directory are added from the source directory and those missing in the source directory are added from the destination directory.
- log2merge: Same as merge except that the changes are logged into an LDIF file and not directly effected in the directory.

The default value depends on the operation specified. Table 5–6 shows the default values of the mvatrdif argument, corresponding to the operations specified.

Table 5–6 Default Values for the mvatrdif Argument

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	merge
merge_dryrun	log2merge
userdefinedcr	ignore

dndif=ignore | usesrc | log2usesrc | usedest | log2usedest | log

Optional. Specifies the conflict resolution rule to use when an entry has different DNs in the source and destination directories. The following values are allowed for the dndif argument:

- ignore: Ignore the conflict and take no action

- usesrc: Change the DN of the entry in the destination directory to that of the source directory
- log2usesrc: Same as usesrc except that the change is logged into an LDIF file, and not directly effected in the destination directory
- usedest: Change the DN of the entry in the source directory to that of the destination directory
- log2usedest: Same as usedest except that the change is logged into an LDIF file, and not directly effected in the source directory

The default value depends on the operation specified. Table 5–7 shows the default values of the mvatrdif argument, corresponding to the operations specified.

Table 5–7 Default Values for the mvatrdif Argument

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	log2usesrc
merge_dryrun	usesrc
userdefinedcr	ignore

odefos=ignore | add | log2add | del | log2del | log

Optional. Specifies the conflict resolution rule to use when an object class definition exists only in the source directory. The following values are allowed for the odefos argument:

- ignore: Ignore the conflict and do not take any action
- add: Add the object class definition to the peer directory
- log2add: Same as add except that the changes are logged into an LDIF file and not directly effected in the directory.
- del: Delete the object class definition from the directory
- log2del: Same as del except that the changes are logged into an LDIF file and not directly effected in the directory
- log: Log the conflict in the report file and take no other action

The default value depends on the operation specified. Table 5–8 shows the default values of the odefos argument, corresponding to the operations specified.

Table 5–8 Default Values for the odefos Argument

Operation	Default Value
compare	log2add
reconcile	add
merge	add
merge_dryrun	log2add
userdefinedcr	ignore

odefod=ignore | add | log2add | del | log2del | log

Optional. Specifies the conflict resolution rule to use when an object class definition exists only in the destination directory. The values allowed for the `odefod` argument are the same as the `odefos` argument.

The default value depends on the operation specified. Table 5–9 shows the default values of the `odefod` argument, corresponding to the operations specified.

Table 5–9 Default Values for the odefod Argument

Operation	Default Value
`compare`	`log2del`
`reconcile`	`del`
`merge`	`add`
`merge_dryrun`	`log2add`
`userdefinedcr`	`ignore`

odefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge | log2merge | log

Optional. Specifies the conflict resolution rule to use when an object class definition is different in the source and destination directories. The following values are allowed for the `odefdif` argument:

- `ignore`: Ignore the conflict and take no action
- `usesrc`: Replace the object class definition in the destination directory with the object class definition in the source directory
- `log2usesrc`: Same as `usesrc` except that the changes are logged in an LDIF file and not directly effected in the destination directory
- `usedest`: Replace the object class definition in the source directory with the object class definition in the destination directory
- `log2usedest`: Same as `usedest` except that the changes are logged in an LDIF file and not directly effected in the source directory
- `merge`: Merge the object class definitions. This involves adding optional and mandatory attributes available in one directory to the other directory
- `log2merge`: Same as merge except that the changes are logged into an LDIF file and not directly effected in the directory
- `log`: Log the conflicts in the report file and take no other action

The default value depends on the operation specified. Table 5–10 shows the default values of the `odefdif` argument, corresponding to the operation specified.

Table 5–10 Default Values for the odefdif Argument

Operation	Default Value
`compare`	`log2usesrc`
`reconcile`	`usesrc`
`merge`	`merge`
`merge_dryrun`	`log2merge`
`userdefinedcr`	`ignore`

adefos=ignore | add | log2add | del | log2del | log

Optional. Specifies the conflict resolution rule to use when an attribute definition exists only in the source directory. The following values are allowed for the `adefos` argument:

- `ignore`: Ignore the conflict and do not take any action
- `add`: Add the attribute definition to the peer directory
- `log2add`: Same as add except that the changes are logged into an LDIF file and not directly effected in the directory.
- `del`: Delete the attribute definition from the directory
- `log2del`: Same as del except that the changes are logged into an LDIF file and not directly effected in the directory
- `log`: Log the conflict in the report file and take no other action

The default value depends on the operation specified. Table 5–11 shows the default values of the `adefos` argument, corresponding to the operation specified.

Table 5–11 Default Values for the adefos Argument

Operation	Default Value
`compare`	`log2add`
`reconcile`	`add`
`merge`	`add`
`merge_dryrun`	`log2add`
`userdefinedcr`	`ignore`

adefod=ignore | add | log2add | del | log2del | log

Optional. Specifies the conflict resolution rule to use when an attribute definition exists only in the destination directory. The values allowed for the `adefod` argument are the same as the `adefos` argument.

The default value depends on the operation specified. Table 5–12 shows the default values of the `adefod` argument, corresponding to the operation specified.

Table 5–12 Default Values for the adefod Argument

Operation	Default Value
`compare`	`log2del`
`reconcile`	`del`
`merge`	`add`
`merge_dryrun`	`log2add`
`userdefinedcr`	`ignore`

adefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | log

Optional. Specifies the conflict resolution rule to use when an attribute definition is different in the source and destination directories. The following values are allowed for the `adefdif` argument:

- `ignore`: Ignore the conflict and take no action

- `usesrc`: Replace the attribute definition in the destination directory with the attribute definition in the source directory
- `log2usesrc`: Same as `usesrc` except that the changes are logged in an LDIF file and not directly effected in the destination directory
- `usedest`: Replace the attribute definition in the source directory with the attribute definition in the destination directory
- `log2usedest`: Same as `usedest` except that the changes are logged in an LDIF file and not directly effected in the source directory
- `log`: Log the conflicts in the report file and take no other action

The default value depends on the operation specified. Table 5–13 shows the default values of the `adefdif` argument, corresponding to the operation specified.

Table 5–13 Default Values for the adefdif Argument

Operation	Default Value
`compare`	`log2usesrc`
`reconcile`	`usesrc`
`merge`	`usesrc`
`merge_dryrun`	`log2usesrc`
`userdefinedcr`	`ignore`

verbose=t[rue] | f[alse]

Optional. Determines whether the `rpt` file is shown on the screen. The default value is `false`. When set to `true`, `verbose` displays the report file on the screen as it is generated. When `verbose` is set to `false`, the tool shows its progress on the screen by displaying the count of entries it has processed.

force=t[rue] | f[alse]

Optional. Determines whether the tool prompts the user for confirmation before performing the specified operation. The default value is `false`. When set to `true`, the tool will not prompt the user for confirmation before performing the specified operation.

help=t[rue] | f[alse]

Optional. When set to `true`, the tool displays help on the `oidcmprec` command. The default value is `false`.

paramfile=*filename_that_contains_the_above_parameters*

Optional. Specifies a parameter file to supply argument values. A parameter file can be used to supply arguments that are normally entered at the command line. The file should contain `argument=`*`value`* pairs either separated by whitespace characters or entered on separate lines. If an argument is contained in the parameter file and also supplied through the command line, then the command line value overrides the parameter file value for that argument.

genchglog=d[efault] | t[rue] | f[alse]

Optional. Determines whether a change log is created for the changes made by the `oidcmprec` tool. The `genchglog` argument can have the following values:

- `default`: The OID server settings decide whether a change log is generated or not. Change logs are generated if the root entry's `orcldiprepository` attribute is set to `true`. A value of `false` means that change logs are not generated. The same rule applies for both the source and destination directories. `default` is the default value for `gechglog`.
- `true`: Change logs are always generated irrespective of the settings on the source and destination directories.
- `false`: Change logs are never generated irrespective of the settings on the source and destination directories.

contonerr=t[rue] | f[alse]

Optional. Determines whether the tool shall continue when it encounters an error. The `contonerr` argument can have the following values:

- `true`: The tool continues to process other entries even if there is an error. This is the default value for `contonerr`.
- `false`: The tool stops if it encounters an error.

> **Note:** If the tool encounters a critical error, it stops irrespective of the value passed to `contonerr`.

Tasks and Examples for oidcmprec

This section provides examples for tasks that can be performed using the `oidcmprec` command. The following examples discuss various operations that can be performed with the `oidcmprec` tool:

- Comparing and Reconciling Individual Entries in Two Directories
- Comparing and Reconciling Subtrees in Two Directories
- Comparing and Reconciling Entire Directories
- Performing User-Defined Compare and Reconcile Operations
- Merging Two Directories
- Including and Excluding Attributes
- Overriding Default Conflict Resolution Rules
- Using a Parameter File
- Generating Change Logs
- Performing Directory Schema Operations

Comparing and Reconciling Individual Entries in Two Directories

This example compares the DN, `"cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com"`, in the source and destination directories. The default conflict resolution rules for the `compare` operation are used. You are prompted for the source directory and destination directory passwords, if you do not enter these on the command line.

Example

```
oidcmprec base="'cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com'" \
          operation=compare \
```

```
          source=myhost1.acme.com:389 \
          destination=myhost2.acme.com:389

Enter replication DN password of the source directory      :
Enter replication DN password of the destination directory :
```

The following example compares the DN, `cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com`, in the source and destination directories. It resolves the conflicts that are detected. The default conflict resolution rules for the `reconcile` operation are used.

Example

```
oidcmprec base="'cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com'" \
          operation=reconcile \
          source=myhost1.acme.com:389/secret1 \
          destination=myhost2.acme.com:389/secret2
```

Comparing and Reconciling Subtrees in Two Directories

This example compares the naming context, `dc=com`, in the two directories. The `scope` attribute has been set to subtree. This allows the entire directory information tree (DIT) under the `base` DN, `dc=com`, to be compared. The `threads` and `dnthreads` arguments specify the number of worker threads and DN threads. The `cmpres` file is used to store the report for the operation.

Example

```
oidcmprec base="'dc=com'" \
          operation=compare scope=subtree \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          threads=5 dnthreads=2 filename=cmpres
```

The following example performs the reconcile operation on two subtrees namely, `dc=com` and `dc=org`. The `dns2exclude` argument is used to exclude the `c=us,dc=mycom,dc=com` and `c=uk,dc=myorg,dc=org` subtrees from the operation.

Example

```
oidcmprec base="'dc=com'  'dc=org'" \
          dns2exclude="'c=us,dc=mycom,dc=com' 'c=uk,dc=myorg,dc=org'"
          operation=reconcile scope=subtree \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
```

Comparing and Reconciling Entire Directories

The following example compares a directory residing on `host1` with another directory residing on `host2`. The `base` argument is set to " " and the `scope` argument is set to subtree.

Example

```
oidcmprec operation=compare source=host1:3060/secret1 \
          destination=host2:3070/secret2 \
          base="' '" scope=subtree
```

The following example reconciles a directory residing on myhost1 with another directory residing on myhost2. Entire directories are compared except the DN, c=us,dc=mycom,dc=com.

Example

```
oidcmprec base="' '" \
          dns2exclude="'c=us,dc=mycom,dc=com'" 
          operation=reconcile scope=subtree \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          threads=5 dnthreads=2 file=cmpres
```

Note: When you compare entire directories, the following DNs and their subtrees are excluded:

- root DSE entry
- cn=auditlog
- cn=baseschema
- cn=catalogs
- cn=events
- cn=oracle internet directory
- cn=replication configuration
- cn=server configuration
- cn=subconfigsubentry
- cn=subregistrysubentry
- cn=subschemasubentry

You can include these entries by specifying them explicitly in the base argument.

Performing User-Defined Compare and Reconcile Operations

This example makes use of user-defined values for the entos, entod, atros, svatrdif, mvatrdif, and dndif arguments. Conflict resolution arguments not specified on the command line, like atrod, are set to ignore.

Example

```
oidcmprec operation=userdefinedcr scope=subtree \
          base="'dc=com'  'dc=org'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          entos=add entod=ignore atros=add \
          svatrdif=usesrc mvatrdif=usesrc dndif=ignore \
          threads=5 dnthreads=2 file=myreconcile
```

Merging Two Directories

This example synchronizes the dc=com subtree in two directories. The merge operation updates both the source and destination directories.

Example

```
oidcmprec operation=merge scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          file=merge
```

Including and Excluding Attributes

The following example performs a `compare` operation. It uses the `exclattr` argument to exclude the `orclguid`, `category`, `userpassword`, and `authpassword` attributes. The example makes use of wildcard pattern matching to exclude the `authpassword` attribute subtypes.

Example

```
oidcmprec operation=compare scope=subtree base="'dc=com'  'dc=org'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          exclattr="userpassword authpassword authpassword;* orclguid category"
          threads=5 dnthreads=2 file=compare
```

The following example makes use of the `inclattr` argument to include the `userpassword`, `cn`, `sn` `givenname`, and `mail` attributes.

Example

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          inclattr="userpassword cn sn givenname mail"
          file=cmpr
```

The following example includes all attributes for the compare operation except `orclguid`, `creatorsname`, and `modifiersname` attributes.

Example

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          inclattr="*" exclattr="orclguid creatorsname modifiersname"
          file=compare
```

Overriding Default Conflict Resolution Rules

This example performs a compare operation on two directories. It overrides the default conflict resolution rules used for the `dndif` and `mvatrdif` arguments. The conflict resolution rule for these arguments is set to `ignore`.

Example

```
oidcmprec source=host1:3060/secret1 destination=host2:3070/secret2 \
          base="' '" scope=subtree file=temp operation=compare \
          dndif=ignore mvatrdif=ignore
```

Using a Parameter File

This example performs a `compare` operation on two directories. It uses a parameter file, `comp_param` to specify command-line arguments. The `dnthreads` argument is specified both in the file and at the command line. The command-line value of `dnthreads` overrides the value specified in the parameter file.

Example

```
oidcmprec paramfile=comp_param dnthreads=3
```

The following displays the parameter file that is used:

```
##########################################
#Parameter file for compare and reconcile tool
#Creator   : John
#Date      : 21-Mar-2006
#File Name : comp_param
##########################################
operation=compare
source=staqj13:3060/ods
destination=staqj13:3070/ods
base="cn=oraclecontext"
base="c=uk,dc=mycom,dc=com"
base="c=us,dc=mycom,dc=com"
verbose=false
force=true
threads=6
dnthreads=2
exclattr="orclguid userpassword authpassword authpassword;*"
filename=cmp2006Feb01
```

Generating Change Logs

The following example uses the `genchglog` argument to ensure that change logs are generated for the operation. When `genchglog` is set to `true`, change logs are generated at both the source and destination directories.

Example

```
oidcmprec operation=merge scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          inclattr="*" exclattr="orclguid creatorsname modifiersname"
          file=merge  genchglog=true
```

Performing Directory Schema Operations

The following example includes the schema for the selected operation by adding the `cn=subschemasubentry` DN to the `base` argument.

Example

```
oidcmprec operation=merge scope=subtree \
          base="'dc=com' 'cn=subschemasubentry'" \
          source=myhost1.mycom.com:389/secret1 \
          destination=myhost2.mycom.com:389/secret2 \
          inclattr="*" exclattr="orclguid creatorsname modifiersname"
          file=merge genchglog=false
```

remtool

The Replication Environment Management Tool is used to manage Oracle Internet Directory replication configuration activities.

More specifically, the Replication Environment Management tool:

- Configures **Oracle Database Advanced Replication**-based **multimaster replication**.
- Scans the replication environment and verifies an Oracle Database Advanced Replication-based directory replication group (DRG).
- Rectifies any problems in an Advanced Replication-based DRG. If the tool cannot rectify a problem, it reports the point or points of failure, which you can then fix manually.
- Reports queue statistics, deferred transactions errors, and administrative request errors of an Advanced Replication-based DRG.
- Reconfigures the Advanced Replication-based DRG.
- Configures LDAP-based replication.
- Reconfigures an LDAP-based directory replication group (DRG).

Syntax for remtool

```
remtool {operation} [-v]
```

Arguments for remtool

operation

Required. The name of the operation to perform using `remtool`. See the appropriate operation documentation for operation specific syntax, arguments, and usage. The following operations are available:

- addnode - Adds a new node to an Oracle Database Advanced Replication-based directory replication group (DRG). See "The remtool -addnode Operation" on page 5-24 for more information about this operation.
- asrcleanup - Cleans up the set up of an Oracle Database Advanced Replication-based DRG. See "The remtool -asrcleanup Operation" on page 5-26 for more information about this operation.
- asrrectify - Verifies the setup of Oracle Database Advanced Replication-based DRG, and corrects any problems found. See "The remtool -asrrectify Operation" on page 5-28 for more information about this operation.
- asrsetup - Creates a new directory replication group (DRG) by configuring Oracle Database Advanced Replication. See "The remtool -asrsetup Operation" on page 5-30 for more information about this operation.
- asrverify - Verifies the setup of Oracle Database Advanced Replication-based DRG, and reports any problems found. See "The remtool -asrverify Operation" on page 5-32 for more information about this operation.
- backupmetadata - Adds the metadata of a pilot replica to a master replica or backs up the metadata of a pilot replica into a file. This operation must be executed at the pilot replica. See "The remtool -backupmetadata Operation" on page 5-35 for more information about this operation.
- chgpwd - Changes the replication administrator's database account password on all nodes of an Oracle Database Advanced Replication-based DRG. See "The remtool -chgpwd Operation" on page 5-36 for more information about this operation.

- delnode - Deletes a node from an existing Oracle Database Advanced Replication-based DRG. See "The remtool -delnode Operation" on page 5-37 for more information about this operation.
- dispasrerr - Displays all deferred transaction errors and administrative request errors for an Oracle Database Advanced Replication-based DRG. See "The remtool -dispasrerr Operation" on page 5-39 for more information about this operation.
- dispqstat - Displays the queue statistics of all nodes in an Oracle Database Advanced Replication-based DRG. See "The remtool -dispqstat Operation" on page 5-41 for more information about this operation.
- paddnode - Adds a partial replica to an LDAP-based DRG. See "The remtool -paddnode Operation" on page 5-42 for more information about this operation.
- pchgmaster- Breaks agreement with the old supplier (master copy of the naming context) and reestablishes agreement with a new supplier. See "The remtool -pchgmaster Operation" on page 5-46 for more information about this operation.
- pchgpwd - Changes the password of a replication DN for a replica in an LDAP-based DRG. See "The remtool -pchgpwd Operation" on page 5-49 for more information about this operation.
- pchgwalpwd - Changes the wallet password of a replication DN for a replica in an LDAP-based DRG. See "The remtool -pchgwalpwd Operation" on page 5-50 for more information about this operation.
- pcleanup - Cleans up the partial replication setup of an LDAP-based DRG. See "The remtool -pcleanup Operation" on page 5-51 for more information about this operation.
- pdelnode - Deletes a partial replica from an LDAP-based DRG. See "The remtool -pdelnode Operation" on page 5-53 for more information about this operation.
- pdispqstat - Displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. See "The remtool -pdispqstat Operation" on page 5-55 for more information about this operation.
- pilotreplica - Begins or ends pilot mode for a replica. See "The remtool -pilotreplica Operation" on page 5-56 for more information about this operation.
- presetpwd - Resets the password of a replication DN for a replica in an LDAP-based DRG. See "The remtool -presetpwd Operation" on page 5-57 for more information about this operation.
- pverify - Verifies the replication configuration for a DRG node that uses LDAP-based replication. See "The remtool -pverify Operation" on page 5-58 for more information about this operation.
- resumeasr - Resumes replication activity for an Oracle Database Advanced Replication-based DRG. See "The remtool -resumeasr Operation" on page 5-61 for more information about this operation.
- suspendasr - Suspends replication activity for an Oracle Database Advanced Replication-based DRG. See "The remtool -suspendasr Operation" on page 5-62 for more information about this operation.

-v

Optional. Runs the command in verbose mode. Shows detailed output for the command on the screen and also logs all operations in the `remtool.log` file created in `$`*`ORACLE_HOME`*`/ldap/log`.

The remtool -addnode Operation

The `addnode` operation adds a new node to an existing directory replication group (DRG). You must first create the DRG using "The remtool -asrsetup Operation" on page 5-30. The following usage rules apply to this operation:

- The node to be added must be empty.
- You will need to know the SYSTEM user password of the new node.
- Oracle Internet Directory processes on the master definition site (MDS) and other remote master sites (RMSs) must be down.
- After the `addnode` operation is complete, Oracle Internet Directory processes can be restarted.

Syntax for remtool -addnode

```
remtool -addnode [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -addnode

The tool will also prompt you for the database global name (as defined in the `tnsnames.ora` file) and SYSTEM password for each node to be added.

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -addnode

Using the `addnode` operation you can perform the following tasks:

- Adding a New Node to an Oracle Database Advanced Replication-based DRG

Adding a New Node to an Oracle Database Advanced Replication-based DRG In this example, `MY_HOST3.MY_COMPANY.COM` is added to a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

Example:

```
remtool -addnode -v -connect repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------- ------------- ----
Instance Host Name     Global Name            Version       Replicaid     Site
Name                                                                      Type
-------- ------------ ---------------------- ------------- ------------- ----
rid2      my_host      MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0 my_host_rid1  MDS
```

```
rid2      my_host      MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0 my_host_rid2  RMS
--------- ------------ ---------------------- ------------- ------------- ----
Do you want to continue? [y/n] : y

--------------------------------------------------------------------------------
WARNING:
Make sure that the replication administrator database
account does not exist already in the new node to be
added to the DRG. If the account exists, that
account will be dropped and will be created newly.
--------------------------------------------------------------------------------
Enter global name of new node to be added          : MY_HOST3.MY_COMPANY.COM

Enter SYSTEM user password of new node to be added :
--------------------------------------------------------------------------------
Adding a new node...

MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Creating purge job...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST3.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
```

```
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST3.MY_COMPANY.COM : Verifying initialization parameter...
------------------------------------------------------------------------------
Node MY_HOST3.MY_COMPANY.COM has been added to this DRG.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1     my_host      MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
rid3     my_host      MY_HOST3.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid3  RMS
-------- ------------ ---------------------- ------------ ------------ ----
```

The remtool -asrcleanup Operation

The `asrcleanup` operation cleans up an existing Oracle Database Advanced Replication setup. You must know the system password of all nodes taking part in the directory replication group (DRG) to run this operation.

Syntax for remtool -asrcleanup

```
remtool -asrcleanup [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -asrcleanup

The tool will prompt you for the SYSTEM user password for each MDS and RMS node in the DRG

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -asrcleanup

Using the `asrcleanup` operation you can perform the following tasks:

- Cleaning Up an Oracle Database Advanced Replication-based DRG Setup

Cleaning Up an Oracle Database Advanced Replication-based DRG Setup In this example, setup is cleaned up for a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`. The tool prompts you to enter the system password for each site.

Example:

```
remtool -asrcleanup -v
```

The results are:

```
Enter replication administrator's name       : repadmin

Enter replication administrator's password   :
Enter global name of MDS                     : my_host1.my_company.com

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type

-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host       MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host       MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Do you want to continue? [y/n] : y

------------------------------------------------------------------------------
Cleaning up...

MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST2.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
```

```
host :
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MYCOMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST1.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
-------------------------------------------------------------------------------
ASR setup has been cleaned up.
-------------------------------------------------------------------------------
```

The remtool -asrrectify Operation

The `asrrectify` operation is used for detecting and rectifying problems in an Oracle Database Advanced Replication-based DRG setup. It reports on errors and corrects them. Oracle Corporation recommends that, before running this operation, you stop Oracle Internet Directory servers.

To use the `asrrectify` operation, all nodes in the DRG must be up and running. The operation will fail if any of the nodes are not running.

If necessary, the `asrrectify` operation prompts for the SYSTEM user password.

Syntax for remtool -asrrectify

```
remtool -asrrectify [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -asrrectify

The tool may also prompt you for the SYSTEM user password for each MDS and RMS node in the DRG.

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -asrrectify

Using the `asrrectify` operation you can perform the following tasks:

- Detecting and Correcting Errors in an Oracle Database Advanced Replication DRG Setup

Detecting and Correcting Errors in an Oracle Database Advanced Replication DRG Setup In this example, setup errors are deducted and rectified in a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`. The tool detects that a user has changed global name of `MY_HOST2.MY_COMPANY.COM` to

NEWNAME.MY_COMPANY.COM after setting up Advanced Replication. It rectifies this error first before continuing with other checks.

Example:

```
remtool -asrrectify -v -conn repadmin/repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
NEWNAME.MY_COMPANY.COM : Renaming global name to MY_HOST2.MY_COMPANY.COM (instance
name : rid2, hostname : my_host)
CORRECTED:
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has
been changed to MY_HOST2.MY_COMPANY.COM.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
CORRECTED:
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has
been changed to MY_HOST2.MY_COMPANY.COM.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version       Replicaid     Site
Name                                                                     Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Do you want to continue? [y/n] : y

------------------------------------------------------------------------------
Rectifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

--------------------  -----  -----  -----  -----  -----  -----  -----
DB Name               Init   Repl   DB     Purge  Sch.   Repl   Repl
                      Param  Admin  Links  Job    Links  Group  Agrmt
                             Role                             Entry
--------------------  -----  -----  -----  -----  -----  -----  -----
```

```
MY_HOST1.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   Chkd   Chkd
MY_HOST2.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   Chkd   Chkd
--------------------  -----  -----  -----  -----  -----  -----  -----
Legends :
  Chkd  - Checked. No errors.
  Crtd  - ASR setup errors were found and corrected.
  Err   - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
--------------------------------------------------------------------------------
```

The remtool -asrsetup Operation

The `asrsetup` operation is used to create a new Oracle Database Advanced Replication-based directory replication group (DRG). A DRG consists of a master definition site (MDS) and one or more remote master sites (RMS).

Before you begin, stop all Oracle Internet Directory server processes on the MDS and RMS sites. After the setup operation is completed, you can restart all Oracle Internet Directory processes and replication server processes.

Syntax for remtool -asrsetup

```
remtool -arssetup [-v]
```

Arguments for remtool -asrsetup

Only the optional `-v` argument is specified on the command-line. The tool will prompt you for the following information.

- The database global name of the MDS (as defined in the `tnsnames.ora` file).
- A replication administrator password for the MDS
- The SYSTEM password for the MDS
- The database global for each RMS (as defined in the `tnsnames.ora` file).
- The SYSTEM password for each RMS

Tasks and Examples for remtool -asrsetup

Using the `asrsetup` operation you can perform the following tasks:

- Creating an Oracle Database Advanced Replication-based DRG

Creating an Oracle Database Advanced Replication-based DRG In this example, a DRG is created consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

Example:

```
remtool -asrsetup -v
```

The results are as follows:

```
--------------------------------------------------------------------------------
ASR Setup for OID Replication
WARNING:
Make sure that the replication administrator that you
enter below does not exist already in any of the nodes
that will be part of the DRG to be created now. If the
user exists, that user will be dropped and will be
created newly.
```

```
-------------------------------------------------------------------------------
Enter replication administrator's name       : repadmin

Enter replication administrator's password   :
Reenter replication administrator's password :
Enter Master Definition Site (MDS) details   :
Enter global name of MDS                     : MY_HOST1.MY_COMPANY.COM

Enter SYSTEM user password of MDS            :
Enter Remote Master Site (RMS) details       :
Enter global name of RMS #  1                : MY_HOST2.MY_COMPANY.COM

Enter SYSTEM user password of MDS            :
Are there more Remote Master Sites in the group? [y/n/q] : n

Verify the details you had entered.
-------------------------------------------------------------------------------
Replication administrator's name   : repadmin
Master Definition Site             : MY_HOST1.MY_COMPANY.COM
Remote Master Site #  1            : MY_HOST2.MY_COMPANY.COM
Are these details correct? [y/n/q] : y

-------------------------------------------------------------------------------
ASR setup in progress...

MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Creating purge job...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Creating purge job...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Creating replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ASR_CHG_LOG to replication group
```

```
LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE
ODS.ASR_CHG_LOG...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ODS_CHG_STAT to replication
group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE
ODS.ODS_CHG_STAT...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST2.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid1" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
--------------------------------------------------------------------------------
ASR setup has been configured successfully.
--------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------- ---------------------- ------------- ------------- ----
Instance Host Name     Global Name            Version       Replicaid     Site
Name                                                                      Type
-------- ------------- ---------------------- ------------- ------------- ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------- ---------------------- ------------- ------------- ----
```

The remtool -asrverify Operation

This `asrverify` operation detects and reports on problems found in an Oracle Database Advanced Replication-based directory replication group (DRG). This operation reports errors, but does not correct them. To run this operation, all nodes in

the DRG must be up and running. You do not have to stop your Oracle Internet Directory server processes to run this operation.

The `asrverify` operation will fail or report errors for the following situations. You can use the `asrrectify` operation to correct these errors. See "The remtool -asrrectify Operation" on page 5-28 for more information about that operation.

- If, by mistake, the replication administrator account is dropped in any of the nodes, the `asrverify` operation fails. Use `asrrectify` to re-create the replication administrator account and add it back to the DRG.
- If, by mistake, the password for the replication administrator account has changed on any of the nodes in the DRG, the `asrverify` operation fails. Usremtoole `asrrectify` to change the replication administrator account and add it back to the DRG.
- If the global database name of any node has changed after Advanced Replication setup, `asrverify` reports an error and does not proceed further. Use `asrrectify` to revert back to the previous global name and rectify other issues.

Syntax for remtool -asrverify

```
remtool -asrverify [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -asrverify

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -asrverify

Using the `asrverify` operation you can perform the following tasks:

- Detecting Errors in an Oracle Database Advanced Replication DRG Setup

Detecting Errors in an Oracle Database Advanced Replication DRG Setup In this example, errors are found in a DRG consisting of two nodes.

Example:

```
remtool -asrverify -v -conn repadmin/repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------------------- ---------------------- ------------- ------------- ----
Instance Host Name     Global Name             Version       Replicaid     Site
Name                                                                       Type
```

```
-------------------- ---------------------- ------------ ------------ ----
rid1     my_host      MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1   MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2   RMS
------------------------------------------- ------------ -----------------
--------------------------------------------------------------------------------
Verifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

--------------------  -----  -----  -----  -----  -----  -----  -----
DB Name               Init   Repl   DB     Purge  Sch.   Repl   Repl
                      Param  Admin  Links  Job    Links  Group  Agrmt
                             Role                              Entry
--------------------  -----  -----  -----  -----  -----  -----  -----
MY_HOST1.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   NCrtd  Chkd
MY_HOST2.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   NCrtd  Chkd
--------------------  -----  -----  -----  -----  -----  -----  -----
Legends :
  Chkd  - Checked. No errors.
  Crtd  - ASR setup errors were found and corrected.
  Err   - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
--------------------------------------------------------------------------------
Summary of findings:
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.

ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.
```

```
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.

ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.
--------------------------------------------------------------------------------
```

The remtool -backupmetadata Operation

The `backupmetadata` operation adds the metadata of a pilot replica to the master replica, or backs up the metadata of a pilot replica into a file.

> **Note:** The `-backupmetadata` option will not work if anonymous bind is disabled at the pilot replica or master replica.

Syntax for remtool -backupmetadata

`remtool -backupmetadata -replica` *`pilot_hostname`*`:`*`port`*`/`*`pilot_repldnpwd`* `{-master` *`master_hostname`*`:`*`port`*`/`*`master_replrdnpwd`* `| -bkup` *`file_name`*`}`

Arguments for remtool -backupmetadata

-replica *pilot_hostname:port/pilot_repldnpwd*

Required. The connection string for the pilot replica. The string is comprised of the following elements:

- The host name where the pilot replica's LDAP server is running.
- The pilot replica's LDAP listening port, for example 389.
- The password for the replication DN of the pilot replica.

-master *master_hostname:port/master_repldnpwd*

Either `-master` or `-bkup` argument is required. The connection string for the master replica. The string is comprised of the following elements:

- The host name where the master replica's LDAP server is running.
- The master replica's LDAP listening port, for example 389.
- The password for the replication DN of the master replica.

-bkup *file_name*

Either `-master` or `-bkup` argument is required. The full path and file name of the LDIF output file. The metadata entries are written to this file in LDIF format.

Tasks and Examples for remtool -backupmetadata

Using the `backupmetadata` operation you can perform the following tasks:

- Adding the Metadata of a Pilot Replica to a Master Replica
- Backing Up the Metadata of a Pilot Replica to an LDIF File

Adding the Metadata of a Pilot Replica to a Master Replica This example shows how to add the metadata entries from a pilot replica to a master replica.

Example:

```
remtool -backupmetadata -replica mypilot.company.com:389/mypassword -master
mymaster.company.com:389/mypassword
```

Note: If Oracle Delegated Administration Services is not configured, then you might see an error message similar to this when you run `remtool` with the `-backupmetadata` option:

```
Failed to add "orclApplicationCommonName=ias.acme.com,
cn=IAS Instances, cn=IAS, cn=Products, cn=OracleContext"
as "uniquemember" to entry "cn=Associated Mid-tiers,
orclapplicationcommonname=DASApp, cn=DAS,cn=products,
cn=OracleContext at replica ldap://myhost:389
```

Please ignore this error message.

Backing Up the Metadata of a Pilot Replica to an LDIF File This example shows how to back up the metadata entries for a pilot replica into an LDIF file.

Example:

```
remtool -backupmetadata -replica mypilot.company.com:389/mypassword -bkup
/home/myfiles/metadata.ldi
```

The remtool -chgpwd Operation

The `chgpwd` operation is used to change the replication administrator password for an Oracle Database Advanced Replication-based directory replication group (DRG) that has already been setup using `asrsetup`.

The replication administrator password is the same for all nodes in an Advanced Replication DRG. This operation will change the password for all nodes in the DRG.

Syntax for remtool -chgpwd

```
remtool -chgpwd [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -chgpwd

The tool will also prompt you to enter the new password for the replication administrator.

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The current password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -chgpwd

Using the `chgpwd` operation you can perform the following task:

- Changing the Replication Administrator Password for an Advanced Replication-based DRG

Changing the Replication Administrator Password for an Advanced Replication-based DRG In this example, the password of the replication administrator of a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` is changed.

Example:

```
remtool -chgpwd -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1       my_host     MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2       my_host     MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Enter new password of the replication administrator   :
Reenter new password of the replication administrator :
------------------------------------------------------------------------------
Changing the password of all nodes...

MY_HOST1.MY_COMPANY.COM : Changing password of replication administrator
repadmin...
MY_HOST2.MY_COMPANY.COM : Changing password of replication administrator
repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
------------------------------------------------------------------------------
Password has been changed.
------------------------------------------------------------------------------
```

The remtool -delnode Operation

The `delnode` operation removes a remote master site (RMS) node from an existing directory replication group (DRG). You must first create the DRG using "The remtool -asrsetup Operation" on page 5-30. The following usage rules apply to this operation:

- You can only delete RMS nodes from a DRG, not the master definition site (MDS).
- Oracle Internet Directory processes on the master definition site (MDS) and other remote master sites (RMSs) in the DRG must be stopped before running the operation.
- If the RMS node being deleted is down when the `delnode` operation is invoked, it will be selected for deletion.

- After the `delnode` operation is complete, Oracle Internet Directory processes can be restarted.

Syntax for remtool -delnode

```
remtool -delnode [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -delnode

The tool will also prompt you for the global database name (as defined in the `tnsnames.ora` file of the RMS node to be deleted from the DRG.

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -delnode

Using the `delnode` operation you can perform the following task:

- Removing a RMS Node from an Oracle Database Advanced Replication-based DRG

Removing a RMS Node from an Oracle Database Advanced Replication-based DRG In this example, `MY_HOST3.MY_COMPANY.COM` is removed from a DRG consisting of `MY_HOST1.MY_COMPANY.COM`, `MY_HOST2.MY_COMPANY.COM` and `MY_HOST3.MY_COMPANY.COM`

Example:

```
remtool -delnode -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
MY_HOST3.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
rid3      my_host      MY_HOST3.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid3  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Do you want to continue? [y/n] : y

Enter globalname of node to be deleted : MY_HOST3.MY_COMPANY.COM

------------------------------------------------------------------------------
```

```
Deleting an existing node...

MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST3.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST3.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from
replication agreement entry as it is not part of DRG or was repeated.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from
replication agreement entry as it is not part of DRG or was repeated.
-------------------------------------------------------------------------------
Node MY_HOST3.MY_COMPANY.COM has been deleted from this DRG.
-------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1     my_host       MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2     my_host       MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----

===============================================================================
```

The remtool -dispasrerr Operation

The `dispasrerr` operation displays errors for an Oracle Database Advanced Replication-based directory replication group (DRG). It shows both administrative request errors and deferred transaction errors.

Syntax for remtool -dispasrerr

```
remtool -dispasrerr [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -dispasrerr

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -dispasrerr

Using the `dispasrerr` operation you can perform the following task:

- Displaying Errors for an Advanced Replication-based DRG

Displaying Errors for an Advanced Replication-based DRG In this example, the tool reports Advanced Replication errors for a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

Example:

```
remtool -dispasrerr -v -conn repadmin/repadmin@my_host1.my_company.com

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid      my_host       MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2     my_host       MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
------------------------------------------------------------------------------
Following administrative request errors were found at MY_HOST1.MY_COMPANY.COM

--------------------  --------------------  --------------------------------
Admin request         Request raised at     Error
raised by
--------------------  --------------------  --------------------------------
REPADMIN              MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ASR_CHG_L
REPADMIN              MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ODS_CHG_S
REPADMIN              MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ODS_CHG
REPADMIN              MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ODS_CHG_S
REPADMIN              MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ASR_CHG
REPADMIN              MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ASR_CHG_L
--------------------  --------------------  --------------------------------
------------------------------------------------------------------------------
Following deferred transaction errors were found at MY_HOST1.MY_COMPANY.COM
```

```
--------------  --------------  --------------  ----------------------------
Deferred        Deferred Trans  Destination     Error
Transaction ID  Origin DB
--------------  --------------  --------------  ----------------------------
1.2.3733        MY_HOST1.MY_COM  MY_HOST1.MY_COM  ORA-01403: no data found

--------------  --------------  --------------  ----------------------------
No deferred transaction errors were found at MY_HOST2.MY_COMPANY.COM
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

The remtool -dispqstat Operation

The `dispqstat` operation displays the queue statistics for a directory replication group (DRG) that uses Oracle Database Advanced Replication. This operation cannot be used for DRGs that use LDAP-based replication. If a DRG uses both Advanced and LDAP-based replication, this operation displays queue statistics for nodes that use Advanced Replication only.

Syntax for remtool -dispqstat

```
remtool -dispqstat [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -dispqstat

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -dispqstat

Using the `dispqstat` operation you can perform the following tasks:

- Displaying Queue Statistics for an Advanced Replication-Based DRG

Displaying Queue Statistics for an Advanced Replication-Based DRG In this example, queue statistics for an Advanced Replication-based DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` are reported.

Example:

```
remtool -dispqstat -v -conn repadmin/repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------- ------------- ----
Instance Host Name     Global Name            Version       Replicaid     Site
```

```
Name                                                                                                Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1     my_host       MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2     my_host       MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Queue Statistics :
-------------- -------------- --------- --------- --------- --------- ---------
   Supplier       Consumer       New      Retry     Purge      HIQ    Change #
-------------- -------------- --------- --------- --------- --------- ---------
MY_HOST1.MY CO MY_HOST1.MY CO     3         9         10         6      2003
MY_HOST1.MY CO MY HOST2.MY CO     2         7         8          5      2001
MY_HOST2.MY CO MY_HOST1.MY CO     2         8         5          8      2002
MY_HOST2.MY CO MY_HOST2.MY CO     2        10         7          8      2000
-------------- -------------- --------- --------- --------- --------- ---------
Legends
  New: No. of new change logs
  Retry: No. of change logs in retry queue
  Purge: No. of change logs in purge queue
  HIQ: No. of change logs in Human Intervention Queue (HIQ)
  Change # : Last applied change log no.
```

The remtool -paddnode Operation

The `paddnode` operation adds a replica or partial replica to a directory replication group (DRG). This operation has the following usage rules:

- The supplier node (the master copy) can be part of a DRG that uses Advanced Replication, LDAP-based replication, or both.
- If you want to specify a supplier node that uses Advanced Replication, you must bind using that node's connection information.
- The new replica to be added should not be a member of any DRG.
- A consumer node (the destination of replication updates) can be any node that uses LDAP-based replication.
- After adding a replica, you can choose the naming context(s) to participate in replication, or choose the entire directory by selecting `*` (asterisk). Choosing specific naming contexts replicates only that portion of the directory. Choosing the entire directory will replicate all directory data except for directory-specific entries (DSE).
- The `cn=oraclecontext` naming context is included for replication whether or not any naming contexts are specified by the user.

Syntax for remtool -paddnode

```
remtool -paddnode [-bind supplier_hostname:ldap_port/replication_dn_password] [-v]
```

Arguments for remtool -paddnode

In addition to the arguments specified on the command-line, the tool will prompt you for the following information:

- Consumer Host Name of Host Running OID Server - The host name of the Oracle Internet Directory server where you want to create the replica. This node can be added to the DRG as a read-only or updateable replica.
- Consumer Port - The LDAP listening port of the consumer node.

- Consumer Replication DN Password - The password for the replication DN on the consumer node.
- **Replica ID of Supplier** - If the DRG contains multiple nodes that can be used as the supplier, you will be prompted to enter the replica ID of the one you want to use.
- **Naming Context** - For a partial replica, you can enter the name(s) of the naming context you want to replicate. To select the entire directory, enter `*` (asterisk). To select none, enter `e` (end).

-bind *supplier_hostname:ldap_port/replication_dn_password*

The connection string used to bind to the LDAP directory server of the supplier node. If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The host name of the supplier node.
- The LDAP listening port of the supplier node.
- The password for the replication DN on the supplier node.

Tasks and Examples for remtool -paddnode

Using the `paddnode` operation you can perform the following tasks:

- Adding a Read-Only Replica to a DRG
- Adding a Partial Replica to a DRG

Adding a Read-Only Replica to a DRG In this example, directory server `ldap://my_host:3060` is added as a replica to directory server `ldap://my_host:3040`, which is part of the DRG consisting of `ldap://my_host:3040` and `ldap://my_host:3080`, which both use LDAP-based replication.

Example:

```
remtool -paddnode -v -bind my_host:3040/ods
```

The results are:

```
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040            --                     RW

002 my_host_rid3       my_host:3080            my_host_rid1           RO

--- ------------------ ---------------------- ---------------------- -----
Enter consumer directory details:
Enter hostname of host running OID server    : my_host

Enter port on which OID server is listening  : 3060

Enter replication dn password                :
Enter replica type [1 - LDAP read-only replica; 2 - LDAP updateable replica] : 1
Enter replicaid of the supplier              : my_host_rid1
-------------------------------------------------------------------------------
```

```
ldap://my_host:3060 [my_host_r[my_host_rid1]id2] : Modifying entry
orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry
orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
--------------------------------------------------------------------------------
Replica ldap://my_host:3060(my_host_rem2) has been added to this DRG.
--------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1        my_host:3040               --                    RW

002 my_host_rid2       my_host:3060               my_host_rid1           RO

003 my_host_rid3       my_host:3080               my_host_rid1           RO

--- ------------------ ---------------------- ---------------------- -----
Replica ldap://my_host:3060 (my_host_rid2) can be made partial replica by
specifying naming contexts to be replicated.
--------------------------------------------------------------------------------

List of available naming contexts in supplier replica ldap://my_host:3040
(my_host_rid1) :

    1. *  [replicate whole directory]
Enter naming context (e-end, q-quit) : e

--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
```

Adding a Partial Replica to a DRG In this example, the directory server `ldap://my_host:3060` is added as a partial replica by specifying the naming contexts to be replicated to directory server `ldap://my_host:3040`.

Example:

```
remtool -paddnode -v -bind my_host:3040/ods
```

The results are:

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid       my_host:3040            --                     RW

--- ----------------- ---------------------- ---------------------- -----
Enter consumer directory details:
Enter hostname of host running OID server    : my_host

Enter port on which OID server is listening  : 3060

Enter replication dn password                :
Enter replica type [1 - LDAP read-only replica; 2 - LDAP updateable replica] : 2
------------------------------------------------------------------------------
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry
orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_prep
,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_prep
,cn=replication configuration...
------------------------------------------------------------------------------
Replica ldap://my_host:3060(my_host_rid2) has been added to this DRG.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040            --                     RW
```

```
002 my_host_rid2        my_host:3060            my_host_rid1            RW

--- ------------------ ---------------------- ---------------------- -----
Replica ldap://my_host:3060 (my_host_rem2) can be made partial replica by
specifying naming contexts to be replicated.

-------------------------------------------------------------------------------
List of available naming contexts in supplier replica ldap://my_host:3040
(my_host_rid1) :

    1. * [replicate whole directory]
    2. dc=com
    3. dc=org
    4. dc=net
    5. dc=edu
Enter naming context (e-end, q-quit) : dc=org

Enter naming context (e-end, q-quit) : dc=edu

Enter naming context (e-end, q-quit) : e

Following naming contexts will be included for replication:
-------------------------------------------------------------------------------
    1. dc=org
    2. dc=edu
Do you want to continue? [y/n] : y

ldap://my_host:3040 [my_host_rid1] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_rid,cn
=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_rid,cn
=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_rid,cn
=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_rid,cn
=replication configuration...

-------------------------------------------------------------------------------
Selected naming contexts have been included for replication.
-------------------------------------------------------------------------------
```

The remtool -pchgmaster Operation

The `pchgmaster` operation is used to break the agreement with the old supplier and reestablish the agreement with a new supplier. This operation is part of configuring replication failover.

> **See Also:** "Configuring Replication Failover" in *Oracle Internet Directory Administrator's Guide* for details on performing the replication failover process

The `pchgmaster` operation has the following usage rules:

1. If you do not supply consumer directory details using the `-bind` option, then you are prompted to specify consumer details.

2. If the consumer details are valid, then `remtool` identifies all nodes in the DRG, if any, and displays their details.
3. You are next prompted for the retiring and new supplier details.
4. After the change master operation completes successfully, you may need to use `remtool -pcleanup -agrmt` on the old supplier to remove the old agreement. This would be the case if the old supplier was offline during the change master operation. See "The remtool -pcleanup Operation" on page 5-51 for details about the `pcleanup` operation.

Syntax for remtool -pchgmaster

```
remtool -pchgmaster [-bind replica_hostname:ldap_port/replication_dn_password]
[-v]
```

Arguments for remtool -pchgmaster

The tool will prompt you for the host names and port numbers of the retiring supplier and the new supplier.

-bind *replica_hostname*:*port_number*/*replication_dn_password*

The connection string used to bind to the consumer whose supplier you wish to change. If you do not supply the argument on the command-line, the tool will prompt you for the information. The connection string is composed of the following elements:

- The host name of the Oracle Internet Directory server hosting the consumer replica
- The LDAP listening port of the Oracle Internet Directory server hosting the consumer replica
- The current password for the replication DN

Tasks and Examples for remtool -pchgmaster

Using the `pchgmaster` operation, you can perform the following tasks:

- Breaking a Supplier Agreement and Creating a New Supplier Agreement for a Consumer

Breaking a Supplier Agreement and Creating a New Supplier Agreement for a Consumer In this example, the supplier of directory server `ldap://my_host:3060` is changed from directory server `ldap://my_host:3040` to directory server `ldap://my_host:3080`.

Example:

```
remtool -pchgmaster -v -bind my_host:3060/ods
```

The results are:

```
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl   Replicaid         Directory Information    Supplier Information   Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid2        my_host:3060            my_host_rid1           RW

002 my_host_rid3        my_host:3080            my_host_rid1           RW
```

```
003 my_host_rid1        my_host:3040            my_host_rid3            RW
                                                my_host_rid2

--- ------------------ ---------------------- ---------------------- -----

Enter replica ID of the retiring supplier                  : my_host_rid1

-------------------------------------------------------------------------------
Enter hostname of the new supplier                          : my_host

Enter port number of the new supplier                      : 3080

Enter replication DN password of the new supplier :
* WARNING *: Moving my_host_rid1 to be consumer of my_host_rid3 might cause
discrepancy in data.
Do you want to continue? [y/n]: y
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000002,cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000001,cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
-------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid2        my_host:3060            my_host_rid3            RW

002 my_host_rid3        my_host:3080            my_host_rid1            RW
                                                my_host_rid2

003 my_host_rid1        my_host:3040            my_host_rid3            RW
```

```
--- ----------------- ---------------------- ---------------------- -----
Change master of my_host_rid2 to my_host_rid3 successfully.
```

The remtool -pchgpwd Operation

This `pchgpwd` operation changes the replication DN password for an Oracle Internet Directory server. The password is changed in both the directory and in wallet.

If the replica is taking part in replication, then password will be changed in other replicas for the local replica's replication DN. Note that, unlike Advanced Replication, the replication DN password for each replica can be different.

The operation must be run on the host of the Oracle Internet Directory server whose password you are changing in order to update the wallet password at the same time. You can also update the wallet password separately using "The remtool -pchgwalpwd Operation" on page 5-50.

Syntax for remtool -pchgpwd

```
remtool -pchgpwd [-bind oid_hostname:ldap_port/replication_dn_password] [-v]
```

Arguments for remtool -pchgpwd

In addition to the arguments specified on the command-line, the tool will also prompt you for the new replication DN password for the host specified in the bind connection string.

-bind *supplier_hostname:ldap_port/replication_dn_password*

The connection string used to bind to the Oracle Internet Directory server whose password you want to change. You must run this operation on that host in order to update the wallet password as well. If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The host name of the Oracle Internet Directory server.
- The LDAP listening port of the Oracle Internet Directory server.
- The current password for the replication DN.

Tasks and Examples for remtool -pchgpwd

Using the `pchgpwd` operation you can perform the following tasks:

- Changing the Replication DN Password Used for LDAP-Based Replication

Changing the Replication DN Password Used for LDAP-Based Replication In this example, the replication DN password of the Oracle Internet Directory server `ldap://my_host:3040/ods` is changed.

Example:

```
remtool -pchgpwd -v -bind my_host:3040/ods
```

The results are:

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
```

```
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040            --                     RW

002 my_host_rid3      my_host:3080            my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid' will be changed.
Do you want to continue? [y/n] : y

Enter new password of replication DN         :
Reenter new password of replication DN       :
------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
------------------------------------------------------------------------------
Password has been changed.
------------------------------------------------------------------------------
```

The remtool -pchgwalpwd Operation

The `pchgwalpwd` operation is used to change the replication DN password only in the wallet of an Oracle Internet Directory server. It sets the wallet password to the same replication DN password stored in the Oracle Internet Directory repository for the host specified in the bind connection string.

Syntax for remtool -pchgwalpwd

```
remtool -pchgwalpwd [-bind oid_hostname:ldap_port/replication_dn_password] [-v]
```

Arguments for remtool -pchgwalpwd

-bind *supplier_hostname:ldap_port/replication_dn_password*

The connection string used to bind to the Oracle Internet Directory server whose wallet password you want to change. If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The host name of the Oracle Internet Directory server.
- The LDAP listening port of the Oracle Internet Directory server.
- The current password for the replication DN.

Tasks and Examples for remtool -pchgwalpwd

Using the `pchgwalpwd` operation you can perform the following task:

- Changing the Replication DN Password in the Oracle Internet Directory Wallet

Changing the Replication DN Password in the Oracle Internet Directory Wallet In this example, the replication DN password for Oracle Internet Directory server `ldap://my_host:3040` is set in wallet to match the password in the repository.

Example:

```
remtool -pchgwalpwd -v -bind my_host:3040/ods
```

The results are:

```
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           --                     RW

002 my_host_rid3       my_host:3080           my_host_rid1           RO

--- ------------------ ---------------------- ---------------------- -----
--------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rid1) associated with
database 'rid' will be set in wallet.
Do you want to continue? [y/n] : y
```

The remtool -pcleanup Operation

The `pcleanup` operation is used to clean up an LDAP-based directory replication group (DRG) setup. It will clean up a replica which has incomplete or flawed LDAP-based DRG setup. It will only clean up the replica identified by the bind connection string.

If replication configuration information is corrupted, or the replication DN entry is not available, then the tool will prompt for the Oracle Internet Directory super user DN and password.

This operation only cleans up LDAP-based DRG setup. For clean up of an Oracle Database Advanced Replication-based DRG setup, see "The remtool -asrcleanup Operation" on page 5-26.

Syntax for remtool -pcleanup

```
remtool -pcleanup [-bind oid_hostname:ldap_port/replication_dn_password] [-agrmt]
[-v]
```

Arguments for remtool -pcleanup

-bind *supplier_hostname:ldap_port/replication_dn_password*

The connection string used to bind to the Oracle Internet Directory server whose DRG configuration you want to clean. If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The host name of the Oracle Internet Directory server.
- The LDAP listening port of the Oracle Internet Directory server.
- The current password for the replication DN.

-agrmt

Optional. Use this option to clean specific LDAP agreements associated with an LDAP node.

Tasks and Examples for remtool -pcleanup

Using the `pcleanup` operation you can perform the following tasks:

- Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup
- Cleaning Up Specific LDAP Agreements

Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup In this example, the tool cleans up the replication setup of a DRG that has three replicas taking part in LDAP based replication.

Example:

```
remtool -pcleanup -v -bind my_host:3040/ods
```

The results are:

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040             --                     RW

002 my_host_rid3      my_host:3080            my_host_rid1            RO

003 my_host_rid2      my_host:3060            my_host_rid1            RO

--- ----------------- ---------------------- ---------------------- -----
DRG identified by replica ldap://my_host:3040 (my_host_rid1) will be cleaned up.
Do you want to continue? [y/n] : y

-------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry
orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Deleting entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Deleting entry cn=replication
```

```
dn,orclreplicaid=my_host_rem3,cn=replication configuration...
------------------------------------------------------------------------------
Replica ldap://my_host:3040(my_host_rid1) has been cleaned up.
------------------------------------------------------------------------------
```

Cleaning Up Specific LDAP Agreements In this example, the agreement between directory servers `ldap://my_host:3040` and `ldap://my_host:3060` is cleaned up. The agreement between directory servers `ldap://my_host:3040` and `ldap://my_host:3080` is also cleaned up.

Example:

```
remtool -pcleanup -v -agrmt -bind my_host:3040/ods

Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001  my_host_rid1       my_host:3040            my_host_rid2           RW
                                                my_host_rid3

002  my_host_rid3       my_host:3080            my_host_rid1           RW

003  my_host_rid2       my_host:3060            my_host_rid1           RW
--- ------------------ ---------------------- ---------------------- -----

Enter replica ID of replica(s) for which its(their) agreement(s) with replica
ldap://my_host:3040 (my_host_rid1) will be cleaned up.
Enter replica ID [Enter "e" to end selection] : my_host_rid2

Enter replica ID [Enter "e" to end selection] : my_host_rid3

Enter replica ID [Enter "e" to end selection] : e

------------------------------------------------------------------------------
Agreement(s) with the following replica(s) would be cleaned up:
    0. my_host_rid2
    1. my_host_rid3
Do you want to continue? [y/n] : y

------------------------------------------------------------------------------
Successfully cleaned up agreement between my_host_rid1 and my_host_rid2.
Successfully cleaned up agreement between my_host_rid1 and my_host_rid3.
------------------------------------------------------------------------------
Replica ldap://my_host:3040(my_host_rid1) has been cleaned up.
------------------------------------------------------------------------------
```

The remtool -pdelnode Operation

The `pdelnode` operation deletes an LDAP-based replica or partial replica from a directory replication group (DRG). To delete an Advanced Replication-based replica, used the "The remtool -delnode Operation" on page 5-37.

Syntax for remtool -pdelnode

```
remtool -pdelnode [-bind hostname:ldap_port/replication_dn_password] [-v]
```

Arguments for remtool -pdelnode

In addition to the arguments specified on the command-line, the tool will prompt you for the following information:

- The replica ID of the replica to be deleted - The replica ID of the LDAP-based replica you want to delete.

-bind *hostname:ldap_port/replication_dn_password*

The connection string used to bind to the LDAP directory server of an LDAP-based replication node of a DRG. If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The host name of an LDAP-based replica node.
- The LDAP listening port.
- The password for the replication DN.

Tasks and Examples for remtool -pdelnode

Using the `pdelnode` operation you can perform the following tasks:

- Deleting a Read-Only Replica from a DRG

Deleting a Read-Only Replica from a DRG In this example, replica `ldap://my_host:3080` is removed from the DRG. This DRG consists of three replicas: `ldap://my_host:3040`, `ldap://my_host:3060`, and `ldap://my_host:3080`, of which `ldap://my_host:3040` and `ldap://my_host:3060` uses Advanced Replication and `ldap:my_host:3040` and `ldap://my_host:3080` uses LDAP-based replication. To delete replica `ldap://my_host:3080`, user has to give bind details of either `ldap://my_host:3040` or `ldap://my_host:3080`.

Example:

```
remtool -pdelnode -v -bind my_host:3040/ods
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :
--- ----------------- ---------------------- ---------------------- -----
Sl   Replicaid         Directory Information    Supplier Information   Repl.
No.                                                                   Type
--- ----------------- ---------------------- ---------------------- -----
001  my_host_rid1       my_host:3040           my_host_rid2           RW

002  my_host_rid2       --                     my_host_rid1           RW

003  my_host_rid3       my_host:3080           my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
Enter replicaid of the replica to be deleted : my_host_rid3

------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry
orclreplicaid=my_host_rem3,cn=replication configuration...
```

```
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclreplicaid=my_host_rem,cn=replication configuration...
------------------------------------------------------------------------------
Replica ldap://my_host:3080(my_host_rid3) has been deleted from this DRG.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           my_host_rid2            RW

002 my_host_rid2       --                     my_host_rid1            RW

--- ------------------ ---------------------- ---------------------- -----
```

The remtool -pdispqstat Operation

The `pdispqstat` operation displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. This operation cannot be used for DRGs that use ASR-based (advanced) replication. If a DRG uses both ASR and LDAP-based replication, the `pdispqstat` operation displays queue statistics for nodes that use LDAP-based replication only.

> **Note:** The `dispqstat` operation is used to display the queue statistics for a DRG that uses ASR-based replication.

> **See Also:** "The remtool -dispqstat Operation" for more details on displaying the queue statistics for a DRG that uses ASR-based replication

Syntax for remtool -pdispqstat

```
remtool -pdispqstat [-bind hostname:ldap_port/replication_dn_password] [-v]
```

Arguments for remtool -pdispqstat

-bind *hostname:ldap_port/replication_dn_password*

Required. The connection string used to bind to an LDAP-based replication node. The connection string is composed of three elements:

- The host name of the LDAP-based replication node.
- The LDAP listening port for the node.
- The password for the replication DN.

Tasks and Examples for remtool -pdispqstat

Using the `pdispqstat` operation, you can perform the following tasks:

- Display queue statistics for LDAP-based replicas

Display queue statistics for LDAP-based replicas In this example, queue statistics for a DRG consisting of directory servers `ldap://my_host:3040` and `ldap://my_host:3060` are displayed.

Example:

```
remtool -pdispqstat -v -bind my_host:3040/ods

Directory Replication Group (DRG) details :
--- ------------------ ---------------------- ---------------------- -----
Sl   Replicaid         Directory Information    Supplier Information   Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001  my_host_rid1       my_host:3040             my_host_rid2           RW
002  my_host_rid2       my_host:3060             my_host_rid1           RW
--- ------------------ ---------------------- ---------------------- -----
Queue Statistics:
--------     --------     ----- --- ----- ----- --- ------- -------- -------
Supplier     Consumer     PROTO New Retry Purge HIQ LA Chg# Logs TBP LT Chg#
--------     --------     ----- --- ----- ----- --- ------- -------- -------
my_host_rid2 my_host_rid1 LDAP  0   0     1     2   2001     0        2001
my_host_rid1 my_host_rid2 LDAP  0   0     2     3   2082     3        70335
--------     --------     ----- --- ----- ----- --- ------- -------- -------
Legends:
  New      : No. of new change logs
  Retry    : No. of change logs in retry queue
  Purge    : No. of change logs in purge queue
  HIQ      : No. of change logs in Human Intervention Queue (HIQ)
  LA Chg # : Last applied change log no.
  Logs TBP : Logs to be transported.
  LT Chg # : Last transported change log no.
```

The remtool -pilotreplica Operation

The `pilotreplica` operation begins or ends pilot mode for a replica.

Syntax for remtool -pilotreplica

```
remtool -pilotreplica {begin|end} -bind hostname:ldap_port/replication_dn_password
[-bkup file_name]
```

Arguments for remtool -pilotreplica

begin | end

Required. Begin or end pilot mode.

-bind *hostname*:*ldap_port*/*replication_dn_password*

Required. The connection string used to bind to the LDAP-based replica for which to begin or end pilot mode. The connect string is composed of three elements:

- The host name of an LDAP-based pilot replica.
- The LDAP listening port of the pilot replica.
- The password for the replication DN.

-bkup *file_name*

Name of backup file in which entries modified after pilot mode is started are to be stored in LDIF format.

Tasks and Examples for remtool -pilotreplica

Using the `pilotreplica` operation you can perform the following tasks:

- Beginning Pilot Mode for a Replica
- Ending Pilot Mode for a Replica

Beginning Pilot Mode for a Replica

Example:

```
remtool -pilotreplica begin -bind myhost:389/mypassword -bkup
/home/myfiles/pilot.ldif
```

Ending Pilot Mode for a Replica

Example:

```
remtool -pilotreplica end -bind myhost:389/mypassword
```

The remtool -presetpwd Operation

This `presetpwd` operation resets the replication DN password for the given Oracle Internet Directory server in both the directory repository and wallet. It will not reset the passwords for any other directories of the directory replication group (DRG) of which this directory is a member.

You will need the Oracle Internet Directory super user DN and password to reset the replication DN password.

Syntax for remtool -presetpwd

```
remtool -presetpwd -bind hostname:ldap_port/replication_dn_password [-v]
```

Arguments for remtool -presetpwd

In addition to the arguments supplied on the command-line, the tool will prompt you for the following information:

- The super user DN, for example `cn=orcladmin`.
- The super user password.
- The new replication DN password.

-bind *hostname:ldap_port/replication_dn_password*

Required. The connection string used to bind to the Oracle Internet Directory server for which to reset the replication DN password. The connect string is composed of three elements:

- The host name of the Oracle Internet Directory server.
- The LDAP listening port of the Oracle Internet Directory server.
- The current password for the replication DN.

Tasks and Examples for remtool -presetpwd

Using the `presetpwd` operation you can perform the following tasks:

- Resetting the Replication DN Password for a Single Directory

Resetting the Replication DN Password for a Single Directory In this example, the replication DN password is reset for replica `my_host:3040`.

Example:

```
remtool -presetpwdd -v -bind my_host:3040/ods
```

The results are:

```
Enter superuser DN                          : cn=orcladmin

Enter superuser password                    :
-------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid1' will be reset.
Do you want to continue? [y/n] : y

Enter new password of replication DN        :
Reenter new password of replication DN      :
-------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rid1,cn=replication configuration...
-------------------------------------------------------------------------------
Password has been changed.
-------------------------------------------------------------------------------
```

The remtool -pverify Operation

The `pverify` operation verifies the replication configuration for a directory replication group (DRG) that uses LDAP-based replication. This operation cannot be used for a DRG that uses ASR based replication. If a DRG uses both ASR and LDAP-based replication, then this option verifies the replication configuration between nodes that use LDAP-based replication only.

The `pverify` operation has the following usage rules:

- This option only verifies agreements that involve the node specified in the command argument.
- The `REMTOOL_VERIFY_LOG.rpt` report contains the verification results.

Syntax for remtool -pverify

```
remtool -pverify [-bind hostname:ldap_port_number/replication_dn_password]
[-hiqmax hiqmax] [-tbtmax tbtmax] [-v]
```

Arguments for remtool -pverify

-bind *hostname*:*ldap_port_number*/*replication_dn_password*

Required. The connection string used to bind to an LDAP-based replication node. The connection string is composed of three elements:

- The host name of the LDAP-based replication node.
- The LDAP listening port for the node.
- The password for the replication DN.

-hiqmax *hiqmax*

The maximum number of change logs in the Human Intervention Queue (HIQ) after which warnings are generated.

-tbtmax *tbtmax*

The maximum number of logs to be transported (tbt) after which warnings are generated.

Tasks and Examples for remtool -pverify

Use the `pverify` operation to perform the following tasks:

- Verify Replication Configuration for an LDAP-Based DRG

Verify Replication Configuration for an LDAP-Based DRG In this example, the replication configuration for a DRG comprising of directory servers `ldap://my_host:3040`, `ldap://my_host:3060`, and `ldap://my_host:3080` is verified.

Example

```
remtool -pverify -v -bind my_host:3040/ods

Node ID: my_host_rid1
  Test Category: Connection
    Test Against: my_host_rid1
      Test: Wallet
        Check: Corruption passed
        Check: Authentication passed
        Check: Replicationdn passed

    Test Against: my_host_rid2
      Test: URL
        Check: Format (Primary) passed
        Check: Format (Secondary) passed

    Test Against: my_host_rid3
      Test: URL
        Check: Format (Primary) passed
        Check: Format (Secondary) passed

    Test Against: my_host_rid1
      Test: URL
        Check: Format (Primary) passed
        Check: Format (Secondary) passed

  Test Category: Agreements
    Test Against: Agrmt 000002
      Test: orclreplicadn
        Check: Validity passed
        Check: Match agreement type passed

      Test: agreement DN
        Check: Format passed

    Test Against: Agrmt 000002 with my_host_rid2
      Test: lastAppliedChangeNumber (my_host_rid2 to my_host_rid1)
        Check: Format (transport) passed
        Check: Logs TBP passed
        Check: Format (apply) passed
        Check: HIQ passed

      Test: Filtering (my_host_rid2 to my_host_rid1)
        Check: Format passed
        Check: Configuration passed
```

```
Test Against: Agrmt 000002 with my_host_rid2
  Test: Connection
    Check: Authentication passed

  Test: Replica Pair
    Check: Validity passed
    Check: Consistency passed

  Test: orclreplicationid
    Check: Availability passed

  Test: Replication Protocol
    Check: Availability passed

  Test: lastAppliedChangeNumber (my_host_rid1 to my_host_rid2)
    Check: Format (transport) passed
    Check: Logs TBP passed
    Check: Format (apply) passed
    Check: HIQ passed

  Test: Filtering (my_host_rid1 to my_host_rid2)
    Check: Format passed
    Check: Configuration passed

Test Against: Agrmt 000003
  Test: orclreplicadn
    Check: Validity passed
    Check: Match agreement type passed

  Test: agreement DN
    Check: Format passed

Test Against: Agrmt 000003 with my_host_rid3
  Test: lastAppliedChangeNumber (my_host_rid3 to my_host_rid1)
    Check: Format (transport) passed
    Check: Logs TBP passed
    Check: Format (apply) passed
    Check: HIQ passed

  Test: Filtering (my_host_rid3 to my_host_rid1)
    Check: Format passed
    Check: Configuration failed

Test Against: Agrmt 000003 with my_host_rid3
  Test: Connection
    Check: Authentication passed

  Test: Replica Pair
    Check: Validity passed
    Check: Consistency passed

  Test: orclreplicationid
    Check: Availability passed

  Test: Replication Protocol
    Check: Availability passed

  Test: lastAppliedChangeNumber (my_host_rid1 to my_host_rid3)
    Check: Format (transport) passed
```

```
        Check: Logs TBP passed
        Check: Format (apply) passed
        Check: HIQ passed

      Test: Filtering (my_host_rid1 to my_host_rid3)
        Check: Format passed
        Check: Configuration failed


Verify replication configuration for my_host_rid1 successfully.

Refer to REMTOOL_VERIFY_LOG.rpt for details.

2 checks failed.
```

The remtool -resumeasr Operation

The `resumeasr` operation resumes replication activity for an Oracle Database Advanced Replication-based directory replication group (DRG) that was previously suspended using the "The remtool -suspendasr Operation" on page 5-62.

Syntax for remtool -resumeasr

```
remtool -resumeasr [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -resumeasr

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -resumeasr

Using the `resumeasr` operation you can perform the following tasks:

- Resuming Replication Activity for an Advanced Replication-based DRG

Resuming Replication Activity for an Advanced Replication-based DRG In this example, replication activity of DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` is resumed.

Example:

```
remtool -resumeasr -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
```

```
Instance Host Name     Global Name             Version       Replicaid     Site
Name                                                                       Type
-------- ------------- ---------------------- ------------- ------------- ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------- ---------------------- ------------- ------------- ----
--------------------------------------------------------------------------------
Altering replication status...

MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
--------------------------------------------------------------------------------
Replication status has been altered successfully.
--------------------------------------------------------------------------------
```

The remtool -suspendasr Operation

The `suspendasr` operation suspends Oracle Database Advanced Replication activity for a directory replication group (DRG) that uses it for replication. While Advanced Replication activity is suspended, replication will not take place.

Syntax for remtool -suspendasr

```
remtool -suspendasr [-connect repl_admin_name/password@net_service_name] [-v]
```

Arguments for remtool -suspendasr

-connect *repl_admin_name/password@net_service_name*

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). If you do not supply the argument on the command-line, the tool will prompt you for the information. The connect string is composed of three elements:

- The name of the replication administrator.
- The password for the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located in `$ORACLE_HOME/network/admin`.

Tasks and Examples for remtool -suspendasr

Using the `suspendasr` operation you can perform the following tasks:

- Suspending Replication Activity for an Advanced Replication-based DRG

Suspending Replication Activity for an Advanced Replication-based DRG n this example, replication activity of a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` is suspended.

Example:

```
remtool -suspendasr -v -conn repadmin/repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------- ---------------------- ------------- ------------- ----
```

```
Instance Host Name     Global Name             Version       Replicaid     Site
Name                                                                       Type
-------- ------------- ----------------------- ------------- ------------- ----
rid      my_host       MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2     my_host       MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-------- ------------- ----------------------- ------------- ------------- ----
-------------------------------------------------------------------------------
Altering replication status...

MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
-------------------------------------------------------------------------------
Replication status has been altered successfully.
-------------------------------------------------------------------------------
```

Related Command-Line Tools for remtool

- See "oidctl" on page 2-8
- See "opmnctl" on page 2-18

6

Oracle Directory Integration Platform Tools

This chapter describes the following command-line tools used to administer Oracle Directory Integration Platform:

- dipassistant (Directory Integration Platform Assistant)
- odisrvreg (Oracle Directory Integration Platform Server Registration)
- oidprovtool (Provisioning Registration Tool)
- schemasync (Schema Synchronization Tool)

dipassistant

The Directory Integration Platform Assistant (`dipassistant`) is a command-line tool for administering the Oracle Directory Integration Platform server.

Syntax for dipassistant

```
dipassistant {operation | -gui} [-help]
```

Arguments for dipassistant

operation

The name of the operation to perform using `dipassistant`. See the appropriate operation documentation for operation specific syntax, arguments, and usage. The following operations are available:

- bootstrap (bs) - Performs the initial migration of data between a connected directory and Oracle Internet Directory. See "The dipassistant bootstrap Operation" on page 6-2 for more information about this operation.
- bulkprov (bp) - Creates user entries and provisions or de-provisions them to applications in bulk. See "The dipassistant bulkprov Operation" on page 6-7 for more information about this operation.
- chgpasswd (cpw) - Changes the password for the `dipadmin` account. See "The dipassistant chgpasswd Operation" on page 6-9 for more information about this operation.
- createprofile (cp) - Creates a new synchronization profile from. See "The dipassistant createprofile Operation" on page 6-10 for more information about this operation.

- createprofilelike (cpl) - Creates a new synchronization profile by using an existing profile as a template. See "The dipassistant createprofilelike Operation" on page 6-13 for more information about this operation.
- deleteprofile (dp) - Deletes a synchronization profile. See "The dipassistant deleteprofile Operation" on page 6-14 for more information about this operation.
- expressconfig (ec) - Performs an express configuration of the third-party directory connector. See "The dipassistant expressconfig Operation" on page 6-15 for more information about this operation.
- listprofiles (lp) - Shows a list of all synchronization profile names in Oracle Internet Directory. See "The dipassistant listprofiles Operation" on page 6-16 for more information about this operation.
- loaddata (ld) - See "The dipassistant loaddata Operation" on page 6-17 for more information about this operation.
- modifyprofile (mp) - Modifies an existing synchronization profile. See "The dipassistant modifyprofile Operation" on page 6-21 for more information about this operation.
- reassociate (rs) - Moves and reassociates directory integration profiles from one Oracle Internet Directory server to another. See "The dipassistant reassociate Operation" on page 6-22 for more information about this operation.
- showprofile (sp) - See "The dipassistant showprofile Operation" on page 6-24 for more information about this operation.
- wpasswd (wp) - See "The dipassistant wpasswd Operation" on page 6-25 for more information about this operation.
- extauth (ea) - Configures external authentication plug-in for the connected directory. See "The dipassistant extauth Operation" on page 6-26 for more information about this operation.

-gui

Launches the Oracle Directory Integration Platform Server Administration Tool, which is a graphical user interface that enables you to perform the same operations as `dipassistant`. See the *Oracle Identity Management Integration Guide* for more information about the Oracle Directory Integration Platform Server Administration Tool.

-help

Displays the command-line help for the `dipassistant` tool. To see a list of all operations, type:

```
dipassistant -help
```

To see the arguments and syntax for a particular operation, type:

```
dipassistant operation_name -help
```

The dipassistant bootstrap Operation

The `bootstrap (bs)` operation performs the initial migration of data between a connected directory and Oracle Internet Directory.

Syntax for dipassistant bootstrap

```
dipassistant bootstrap {-profile profile_name [-h oid_hostname] [-p port] [-U
```

```
ssl_mode][-D "bindDN"] [-w password][-log log_file] [-logseverity 1-15] [-trace
trace_file] [-tracelevel level] [-loadparallelism number_threads] [-loadretry
retry_count]}|{-f config_file}
```

Arguments for dipassistant bootstrap

-profile *profile_name*

Either `-f` or `-profile` is required. The name of the synchronization profile to use when performing the bootstrap operation. If you do not provide a synchronization profile, you can provide the name of a configuration file instead. If a profile is provided, then the following optional arguments may be supplied on the command-line.

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-log *log_file*

Optional. The path and file name of the log file. The default is *ORACLE_HOME*`/ldap/odi/bootstrap.log`.

-logseverity

Optional. A number between 1 and 15 that corresponds to the level of events that should be logged. The levels are as follows.

- 1 – INFO
- 2 – WARNING
- 4 – DEBUG
- 8 – ERROR

To specify multiple levels, add the numbers together. For example, the default log severity is 9, INFO and ERROR (1+8=9).

-trace *trace_file*

Optional. The full path and file name of the trace logging file. The default location is *ORACLE_HOME*/ldap/odi/log/bootstrap.trc. If the file exists it will be overwritten.

-tracelevel *level*

Optional. The number that corresponds to the level of information to write to the trace logging file. To specify multiple levels, add the numbers together. The default trace level is 3 (1+2=3).

- 1 - Starting and stopping of threads
- 2 - Refreshing of profiles
- 4 - Initialization, execution, and end
- details of connectors
- 8 - Details during connector execution
- 16 - Change record of the connector
- 32 - Mapping details of the connector
- 64 - Execution time details of the connector

-loadparallelism *number_threads*

Optional. The number of concurrent threads for loading data into Oracle Internet Directory. The default is 5.

-loadretry *retry_count*

Optional. If the loading of an entry fails, the number of times to retry to load the entry before the entry is marked as a bad entry. The default is 5.

-f *config_file*

Either -f or -profile is required. The full path and file name of a configuration file containing the properties described in "Configuration File Properties for dipassistant bootstrap" on page 6-4. If you do not provide a configuration file, you can provide the name of a synchronization profile instead.

Configuration File Properties for dipassistant bootstrap

odip.bootstrap.srctype

Required. The source of the bootstrap data. Valid values are LDAP or LDIF.

odip.bootstrap.desttype

Required. The destination for the bootstrap data. Valid values are LDAP or LDIF.

odip.bootstrap.srcurl

Required. For LDAP, the host_name:port of the directory server that is the source of the bootstrap data. For LDIF, the absolute path of the file that contains the bootstrap source data.

odip.bootstrap.desturl

Required. For `LDAP`, the `host_name:port` of the directory server that is the destination for the bootstrap data. For `LDIF`, the absolute path of the destination LDIF file.

odip.bootstrap.srcsslmode

Optional. Set to `TRUE` to require SSL-based authentication to the to connect to the source of the bootstrapping data. The default is `FALSE` (SSL not used).

odip.bootstrap.destsslmode

Optional. Set to `TRUE` to require SSL-based authentication to the to connect to the destination for the bootstrapping data. The default is `FALSE` (SSL not used).

odip.bootstrap.srcdn

Required for LDAP only. The source DN used to bind to the source directory. The default is the DN of the Oracle Directory Integration Platform administrator, for example `"cn=dipadmin"`.

odip.bootstrap.destdn

Required for LDAP only. The destination DN used to bind to the destination directory. The default is the DN of the Oracle Directory Integration Platform administrator, for example `"cn=dipadmin"`.

Note: If the source DN or the destination DN contains multibyte character-set characters, then these need to be supplied in the `UTF-16` format. For example:

```
odip.bootstrap.srcdn =
CN=nlstest1,ou=\u7F8E\u56FD\u5730\u533A,dc=idm2003,dc=net
```

---

odip.bootstrap.srcpasswd

Optional. The password used to bind to the source directory. In the case of LDAP binding, this is used as a security credential. Oracle Corporation recommends that you not specify the password in this file.

odip.bootstrap.destpasswd

Optional. The password used to bind to the destination directory. In the case of LDAP binding, this is used as a security credential. Oracle Corporation recommends that you not specify the password in this file.

odip.bootstrap.mapfile

Optional. Location of the map file that contains the attribute and domain mappings.

odip.bootstrap.logfile

Optional. The path and file name of the log file. The default is *ORACLE_HOME*`/ldap/odi/bootstrap.log`.

odip.bootstrap.logseverity

Optional. A number between 1 and 15 that corresponds to the level of events that should be logged. The levels are as follows.

- 1 – INFO

- 2 – WARNING
- 4 – DEBUG
- 8 – ERROR

To specify multiple levels, add the numbers together. For example, the default log severity is 9, INFO and ERROR (1+8=9).

odip.bootstrap.loadparallelism

Optional. The number of concurrent threads for loading data into Oracle Internet Directory. The default is 5.

odip.bootstrap.loadretry

Optional. If the loading of an entry fails, the number of times to retry to load the entry before the entry is marked as a bad entry. The default is 5.

odip.bootstrap.trcfile

Optional. The full path and file name of the trace logging file. The default location is *ORACLE_HOME*`/ldap/odi/log/bootstrap.trc`. If the file exists it will be overwritten.

odip.bootstrap.trclevel

Optional. The number that corresponds to the level of information to write to the trace logging file. To specify multiple levels, add the numbers together. The default trace level is 3 (1+2=3).

- 1 - Starting and stopping of threads
- 2 - Refreshing of profiles
- 4 - Initialization, execution, and end
- details of connectors
- 8 - Details during connector execution
- 16 - Change record of the connector
- 32 - Mapping details of the connector
- 64 - Execution time details of the connector

odip.bootstrap.srcencode

Optional. The native character set encoding of the LDIF file. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`. You should specify a character set if the LDIF file:

- Was generated by a third-party directory utility.
- Contains Globalization Support data.
- Was processed on a different platform.

Tasks and Examples for dipassistant bootstrap

Using the `bootstrap` operation you can perform the following tasks:

- Bootstrapping a Directory Using a Synchronization Profile
- Bootstrapping a Directory Using a Configuration File

Bootstrapping a Directory Using a Synchronization Profile The following example uses a synchronization profile named `iPlanetProfile` to perform bootstrapping.

Example:

```
dipassistant bootstrap -profile iPlanetProfile -h myhost -port 3060 -D cn=dipadmin
-w welcome1
```

Bootstrapping a Directory Using a Configuration File The following example uses a configuration file named `bootstrap.cfg` to perform bootstrapping. The configuration file contains the properties described in "Configuration File Properties for dipassistant bootstrap" on page 6-4.

Example:

```
dipassistant bootstrap -f bootstrap.cfg
```

The dipassistant bulkprov Operation

The `bulkprov (bp)` operation allows administrators to create user entries and provision them in bulk to various applications, or to delete user entries and de-provision them in bulk form various applications. You can also use this operation to modify the attributes of user entries. This operation takes an LDIF file as input. See Appendix A, "LDIF File Format" on page A-1 for more information about the proper formatting of the input LDIF file.

For example, here is a sample user entry in LDIF format:

```
dn: cn=John Smith,cn=users,dc=us,dc=mycompany,dc=com
changetype: add
cn: John Smith
cn: John
sn: Smith
mail: jsmith@mycompany.com
uid: jsmith_us
orclisenabled: True
```

The `bulkprov` operation invoked with this input file would add the user entry and provision it to the applications configured in the directory. If the configured applications all have a default provisioning policy of `PROVISIONING_REQUIRED`, then users will be created with this provisioning status by default for each of the applications.

The `bulkprov` operation also invokes any configured plug-ins for the application. These plug-ins can override the default provisioning policy by means of specifying plug-ins, which determine the provisioning policy, perform data validations, and assign defaults. If the application-specific attributes is maintained elsewhere, then you can provide a plug-in to manage that application's data.

You must ensure that the distinguished name (DN) for each user specified in the LDIF file is a valid DN within the realm. DN validation is not performed automatically. If the LDIF file specifies a DN outside of the realm and that does not fall in one of the user search bases, then the new users will not be visible when you search for users in the Oracle Internet Directory Provisioning Console or the Oracle Internet Directory Self-Service Console.

To delete user entries and de-provision them from applications, you would supply an LDIF file with user entries such as this:

```
dn: cn=John Smith,cn=users,dc=us,dc=mycompany,dc=com
changetype: delete
```

Syntax for dipassistant bulkprov

```
dipassistant bulkprov -f ldif_file [-h oid_hostname] [-p port] [-U ssl_mode] [-D
bindDN]
[-w password] [-realm realm_name] [-E character_set]
```

Arguments for dipassistant bulkprov

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-realm *realm_name*

The realm in which the users are to be provisioned. If not specified, then the default identity management realm specified in the Root Oracle Context will be used.

-E "*character_set*"

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `ISO-8859-1`, `JA16SJIS`, or `AL32UTF8`.

Tasks and Examples for dipassistant bulkprov

Using the `dipassistant bulkprov` operation you can perform the following tasks:

- Provisioning Users in Bulk

Provisioning Users in Bulk

Example:

```
dipassistant bulkprov -f users.ldif -h myhost.company.com -p 3040 -D
"cn=orcladmin" -w password -E ISO-8859-1
```

The dipassistant chgpasswd Operation

The `chgpasswd (cpw)` operation resets the password of the Oracle Directory Integration Platform administrator (`dipadmin`) account. The default password for the `dipadmin` account is same as `ias_admin` password chosen during installation. To reset the password, you must provide the security credentials of the Oracle Internet Directory administrator (`orcladmin`) account.

Syntax for dipassistant chgpasswd

```
dipassistant chgpasswd [-h oid_hostname] [-p port] [-U ssl_mode] [-D bindDn] [-w password]
```

Arguments for dipassistant chgpasswd

In addition to the arguments provided on the command line, the tool will prompt you for the new Oracle Directory Integration Platform administrator (`dipadmin`) account password.

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

Tasks and Examples for dipassistant chgpasswd

Using the `dipassistant chgpasswd` operation you can perform the following tasks:

- Changing the Password for the Oracle Directory Integration Platform Administrator

Changing the Password for the Oracle Directory Integration Platform Administrator

Example:

```
dipassistant chgpasswd -h myhost -p 3060 -D cn=orcladmin -w welcome1
```

The Directory Integration Platform Assistant then prompts for the new password as follows:

```
New Password:
Confirm Password:
```

The dipassistant createprofile Operation

The `createprofile (cp)` operation creates a new synchronization profile for Oracle Internet Directory and an external directory.

Syntax for dipassistant createprofile

```
dipassistant createprofile [-h oid_hostname] [-p port] [-U ssl_mode] [-D bindDN]
[-w password]
-f prop_file -configset configset_number
```

Arguments for dipassistant createprofile

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-f *prop_file*

Required. The full path and file name of the profile properties file containing the properties described in "Configuration File Properties for dipassistant createprofile" on page 6-11.

-configset *configset_number*

Required. An integer greater than 0 that represents the configuration set with which to associate the profile.

Configuration File Properties for dipassistant createprofile

odip.profile.agentexecommand

In the case of a NON-LDAP interface, the command to produce the information in LDIF format. This is stored in the orclODIPAgentExeCommand attribute of the profile entry.

odip.profile.condiraccount

DN or user name used to connect to the third party directory. This is stored in the orclODIPConDirAccessAccount attribute of the profile entry.

odip.profile.condirpassword

The password used to connect to the third party directory. This is stored in the orclODIPConDirAccessPassword attribute of the profile entry.

odip.profile.condirfilter

Filter that needs to be applied to the changes read from the connected directory before importing to Oracle Internet Directory. This is stored in the orclODIPConDirMatchingFilter attribute of the profile entry.

odip.profile.condirurl

The `hostname:port` of the third party directory. This is stored in the orclODIPConDirURL attribute of the profile entry.

odip.profile.configfile

Name of the file that contains the additional profile-specific information to be used for execution.

odip.profile.configinfo

Contains additional profile-specific information to be used for execution. This is stored in the orclODIPAgentConfigInfo attribute of the profile entry.

odip.profile.debuglevel

Specifies the debugging level. This is stored in the orclODIPProfileDebugLevel attribute of the profile entry.

odip.profile.interface

The format used for data exchange—LDAP, LDIF, DB or TAGGED. LDAP is the default. This is stored in the orclODIPProfileInterfaceType attribute of the profile entry.

odip.profile.lastchgnum

Last applied change number. In the case of an export profile this number refers to Oracle Internet Directory's last applied change number. However, in the case of the import profile, this number refers to the last applied change number in the connected directory. This is stored in the orclODIPConDirLastAppliedChgNum attribute of the profile entry. You can use the `ldapsearch` command to determine the last change number in Oracle Internet Directory. For example:

```
ldapsearch -D cn=orcladmin -w welcome1 -b "" -s base objectclass=*
lastchangenumber
```

odip.profile.mapfile

Name of the file that contains the mapping rules. This is stored in the orclODIPAttributeMappingRules attribute of the profile entry.

odip.profile.name

Name of the synchronization profile. This is stored in the orclODIPAgentName attribute of the profile entry.

odip.profile.oidfilter

Filter that needs to be applied to the changes that are read from the Oracle Internet Directory before exporting to the connected directory. This is stored in the orclODIPOIDMatchingFilter attribute of the profile entry.

odip.profile.password

The password to access this profile. This is stored in the orclODIPAgentPassword attribute of the profile entry.

odip.profile.retry

Maximum number of times the Oracle Directory Integration Platform server should attempt to execute an entry. This is stored in the orclODIPSyncRetryCount attribute of the profile entry. Default is 4.

odip.profile.schedinterval

Interval between successive executions of this profile by the integration server. If the previous execution has not completed then the next execution will not resume until it completes. This is stored in the orclODIPSchedulingInterval attribute of the profile entry. Default is 1 minute.

odip.profile.status

Whether to ENABLE or DISABLE this profile. This is stored in the orclODIPAgentControl attribute of the profile entry. The default is DISABLE.

odip.profile.syncmode

Direction of synchronization. When the changes are propagated from the third party to Oracle Internet Directory, the synchronization mode is IMPORT. When the changes are propagated to the third party directory, the synchronization mode is EXPORT. This is is stored in the orclODIPSchedulingInterval attribute of the profile entry. Default is IMPORT.

Tasks and Examples for dipassistant createprofile

Using the `createprofile` operation you can perform the following tasks:

- Creating a New Synchronization Profile

Creating a New Synchronization Profile The following example uses a configuration file named `import.profile` to create a new profile and associate the new profile with configuration set 1.

Example:

```
dipassistant createprofile -h myhost -p 3060 -D cn=dipadmin -w welcome1
-f import.profile -configset 1
```

The dipassistant createprofilelike Operation

The `createprofilelike (cpl)` operation creates a new synchronization profile by using an existing profile as a template.

Syntax for dipassistant createprofilelike

```
dipassistant createprofilelike [-h oid_hostname] [-p port] [-U ssl_mode] [-D
bindDN]
[-w password] -profile orig_profile_name -newprofile new_profile_name
```

Arguments for dipassistant createprofilelike

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-profile *orig_profile_name*

Required. The name of the existing profile to be used as a template.

-newprofile *new_profile_name*

Required. The name of the new profile to be created.

Tasks and Examples for dipassistant createprofilelike

Using the `createprofilelike` operation you can perform the following tasks:

- Creating a New Synchronization Profile Using an Existing Profile as a Template

Creating a New Synchronization Profile Using an Existing Profile as a Template The following example creates a new profile named `iPlImport` with values copied from a profile named `iPllmportTemplate`.

Example:

```
dipassistant createprofilelike -h myhost -p 3060 -D cn=dipadmin -w welcome1
```

```
-profile iPlImportTemplate -newProfile iPlImport
```

The dipassistant deleteprofile Operation

The `deleteprofile (dp)` operation deletes a synchronization profile from Oracle Internet Directory.

Syntax for dipassistant deleteprofile

```
dipassistant deleteprofile -profile profile_name [-h oid_hostame] [-p port] [-U
ssl_mode] [-D bindDN] [-w password] [-configset configset_number]
```

Arguments for dipassistant deleteprofile

-profile *profile_name*

Required. The name of the profile to be deleted.

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-configset *configset_number*

Optional. An integer greater than 0 that represents the configuration set associated with the profile. Default is 1.

Tasks and Examples for dipassistant deleteprofile

Using the `deleteprofile` operation you can perform the following tasks:

- Deleting a Synchronization Profile

Deleting a Synchronization Profile The following example deletes the `myprofile` profile.

Example:

```
dipassistant deleteprofile -profile myprofile -h myhost -p 3060 -D cn=dipadmin -w
welcome1 -configset 1
```

The dipassistant expressconfig Operation

The `expressconfig (ec)` operation performs an express configuration of the third-party directory connector. It performs all required configurations and also creates two profiles, an import profile and an export profile. For more information about configuring third-party directory connectors, see the *Oracle Identity Management Integration Guide*.

Syntax for dipassistant expressconfig

```
dipassistant expressconfig [-h oid_hostname] [-p port] [-U ssl_mode] [-3rdpartyds
third_party_ds ] [-configset configset_number]
```

Arguments for dipassistant expressconfig

In addition to the arguments supplied on the command-line, the tool will prompt you for the following information:

- Oracle Internet Directory credentials. You must specify the DN and password of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).
- Third-party directory connection details and credentials of a privileged user. You need to specify whether the connection uses SSL mode. You are also prompted for the DN of the subtree to be synchronized, except when the third-party directory is Microsoft Active Directory.

  If the third-party directory is Microsoft Active Directory, then the DN of the subtree to be synchronized is automatically set to "`cn=users,` *`default_naming_context`*". To synchronize deletions, you must have the necessary administrative privileges in Microsoft Active Directory, for example `administrator@mycompany.com` if the host on which Microsoft Active Directory is installed is `myhost@mycompany.com`.
- Name to identify the synchronization profiles to be created. For example, if you specify the name `abc`, then the tool creates two profiles: `abcImport` and `abcExport`.
- Appropriate ACLs on the cn=users container (Optional). You can choose to enable users and groups to be managed by Oracle components under the `cn=users` container. If you customize ACLs in this way, then the original ACLs are saved in *`ORACLE_HOME`*`/ldap/odi/archive/profile_name_prefix_useracl.ldif` .

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-3rdpartyds *third_party_ds*

Optional. The third-party directory service to which you are connecting. If not provided on the command-line, the tool will prompt you for this information. The following values are supported:

- `ActiveDirectory` or `AD`
- `SunJava` or `iPlanet`
- `eDirectory` or `edir`
- `OpenLDAP`

> **Note:** The preceding values are not case-sensitive

-configset *configset_number*

Optional. An integer greater than 0 that represents the configuration set associated with the profile. Default is 1.

Tasks and Examples for dipassistant expressconfig

Using the `dipassistant expressconfig` operation you can perform the following tasks:

- Performing an Express Configuration for Microsoft Active Directory

Performing an Express Configuration for Microsoft Active Directory

Example:

```
dipassistant expressconfig -h myoidhost.company.com -p 3040 -3rdpartyds
ActiveDirectory -configset 1
```

The dipassistant listprofiles Operation

The `listprofiles (lp)` operation prints a list of all the synchronization profiles in Oracle Internet Directory.

Syntax for dipassistant listprofiles

```
dipassistant listprofiles [-h oid_hostname] [-p port] [-U ssl_mode] [-D bindDN]
[-w password] [-configset configset_number]
```

Arguments for dipassistant listprofiles

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-configset *configset_number*

Optional. An integer greater than 0 that represents the configuration set associated with the profile. Default is 1.

Tasks and Examples for dipassistant listprofiles

Using the `listprofiles` operation you can perform the following tasks:

- Showing a List of All Synchronization Profiles in Oracle Internet Directory

Showing a List of All Synchronization Profiles in Oracle Internet Directory The following example prints a list of all the synchronization profiles in Oracle Internet Directory.

Example:

```
dipassistant listprofiles -h myhost -p 3060 -D cn=dipadmin -w welcome1
```

By default, the preceding command prints the following list of sample profiles created during installation. However, your deployment of Oracle Internet Directory may contain additional synchronization profiles.

```
IplanetExport
IplanetImport
ActiveImport
ActiveExport
LdifExport
LdifImport
TaggedExport
TaggedImport
OracleHRAgent
ActiveChgImp
```

The dipassistant loaddata Operation

The `loaddata` operation loads data from a CSV file into Oracle Internet Directory.

Syntax for dipassistant loaddata

```
dipassistant loaddata -f properties_file | [-h oid_hostname] [-p port] [-U
ssl_mode] [-D bindDn] [-w password] [-c control_file]  [-a application] [-g
groupDN]  -data data_file [-map map_file] [-log log_file] [-logseverity 1-15]
[-trace trace_file] [-tracelevel level]
```

Arguments for dipassistant loaddata

-f *properties_file*

Required for loading data with a properties file. The full path and file name of a properties file containing the properties described in "Configuration File Properties for dipassistant loaddata" on page 6-19.

See the following sample properties file, which demonstrates how to load data from a CSV file into Oracle Internet Directory:

`$ORACLE_HOME/ldap/odi/samples/csv2ldp.properties`

See the following sample properties file, which demonstrates how to load data from a CSV file into Oracle Internet Directory and make the data available to Oracle Instant Portal. In addition to creating new users in Oracle Internet Directory, the properties file also adds each user to the group required by Oracle Instant Portal. If you need the new users to be available in Oracle Instant Portal and you do not use the following properties file, then you must manually add each user to the required Oracle Instant Portal group.

`$ORACLE_HOME/ldap/odi/samples/load2oip.properties`

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

Optional. The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

Optional. The password used to bind to the directory.

-c *control_file*

Required for loading data from a data file. The full path and file name of a control file. See "odip.bootstrap.srcctl" on page 6-20for more information.

-a *application*

Optional. The name of an application that will use the loaded data. In Oracle Identity Management 10*g* (10.1.4.0.1), the only valid value for this argument is `portal`, for Oracle Instant Portal.

-g *groupDN*

Optional. The group DN of the application specified with the `-a` argument. In Oracle Identity Management 10*g* (10.1.4.0.1), the only valid value for this argument is the group DN for Oracle Instant Portal.

-data *data_file*

Required for loading data from a data file. The full path and file name of a CSV file containing the data to load. See "odip.bootstrap.srcurl" on page 6-20 for more information.

-map *map_file*

Required for loading data from a data file. The full path and file name of a mapping file. See "odip.bootstrap.mapfile" on page 6-20 for more information.

-log *log_file*

Optional. The full path and file name of a log file. The default is $*ORACLE_HOME*/ldap/odi/log/loaddata.trc.

-logseverity *1-15*

Optional. A number between 1 and 15 that corresponds to the level of events that should be logged. The levels are as follows.

- 1—INFO
- 2—WARNING
- 4—DEBUG
- 8—ERROR

To specify multiple levels, add the numbers together. For example, the default log severity is 9, INFO and ERROR (1+8=5).

-trace *trace_file*

Optional. The full path and file name of the trace logging file.

-tracelevel *level*

Optional. The number that corresponds to the level of information to write to the trace logging file. To specify multiple levels, add the numbers together. The default trace level is 3 (1+2=3).

Configuration File Properties for dipassistant loaddata

odip.bootstrap.srctype

Required. The source type of the data to be loaded. The only valid value for this property is CSV.

odip.bootstrap.dsttype

Required. The destination type of the data to be loaded. The only valid value for this property is LDAP.

odip.bootstrap.srcurl

Required. The absolute path of the CSV file that contains the data to load into Oracle Internet Directory. See the following sample data file:

`$ORACLE_HOME/ldap/odi/samples/csvsample.data`

odip.bootstrap.srcctl

Required. The absolute path of the file containing source control information about how the data is stored. See the following sample source control file:

`$ORACLE_HOME/ldap/odi/samples/csvsample.ctl`

odip.bootstrap.desturl

Required. The `LDAP host_name:port` of the directory server that is the destination for the data.

odip.bootstrap.destdn

Required. The DN used to bind to the destination directory. The default is the DN of the Oracle Directory Integration Platform administrator, for example `"cn=dipadmin"`.

odip.bootstrap.destpasswd

Required. The password used to bind to the destination directory. In the case of LDAP binding, this is used as a security credential. Oracle Corporation recommends that you remove the value assigned to this property from the properties file immediately after loading data.

odip.bootstrap.mapfile

Required. The absolute path of the map file that contains the attribute and domain mappings. See the following sample map file:

`$ORACLE_HOME/ldap/odi/samples/csvload.map.sample`

odip.bootstrap.logfile

Optional. The path and file name of the log file. The default is *ORACLE_HOME*`/ldap/odi/loaddata.log`.

odip.bootstrap.trcfile

Optional. The full path and file name of the trace logging file. The default location is `$`*ORACLE_HOME*`/ldap/odi/log/loaddata.trc`. If the file exists it will be overwritten.

Tasks and Examples for dipassistant loaddata

Using the `loaddata` operation you can perform the following task:

- Loading Data with a Properties File into Oracle Internet Directory
- Loading Data from a Data File into Oracle Internet Directory

Loading Data with a Properties File into Oracle Internet Directory The following example uses a properties file named `loadcsv.properties` to load a CSV file into Oracle Internet Directory.

Example:

```
dipassistant loaddata -f loadcsv.properties
```

Loading Data from a Data File into Oracle Internet Directory The following example uses a data file named `loadcsv.data` to load a CSV file into Oracle Internet Directory.

Example:

```
dipassistant loaddata -h myhost -p 3060 -D cd=dipadmin -w welcome1
-data loadcsv.data -c loadcsv.ctl -map loadcsv.map
```

The dipassistant modifyprofile Operation

The `modifyprofile (mp)` operation enables you to change certain properties of a synchronization profile. You can specify a profile property to change on the command-line, or you can supply a configuration file that lists the properties you want to change and their new values. See "Configuration File Properties for dipassistant createprofile" on page 6-11 for a description of the properties of a synchronization profile.

Syntax for dipassistant modifyprofile

```
dipassistant modifyprofile [-h oid_hostname] [-p port] [-U ssl_mode] [-D bindDN]
[-w password] {-f prop_file | -profile profile_name [-updlcn] [propName1=value]
[propName2=value]...}
```

Arguments for dipassistant modifyprofile

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-f *prop_file*

The full path and file name of the profile properties file containing the properties you want to change and their new values. The properties are described in "Configuration File Properties for dipassistant createprofile" on page 6-11.

-profile *profile_name*

The name of the synchronization profile you want to modify.

-updlcn

Optional. Used to update the last change number of the synchronization profile with the last change number of the source directory.

propName=value

The name of the property whose value you want to change and the new value for that property. The properties are described in "Configuration File Properties for dipassistant createprofile" on page 6-11.

Tasks and Examples for dipassistant modifyprofile

Using the `modifyprofile` operation you can perform the following tasks:

- Modifying a Synchronization Profile

Modifying a Synchronization Profile The following example uses a properties file named `changes.profile` to modify a profile named `myprofile`.

Example:

```
dipassistant modifyprofile -profile myprofile -h myhost -p 3060 -D cn=dipadmin -w
welcome1 -f changes.profile
```

The following example uses the -U option to connect to Oracle Internet Directory in SSL mode.

```
dipassistant modifyprofile -profile myprofile -h myhost -p 636 -U 2 -D cn=dipadmin
-w welcome1 -f changes.profile
```

The dipassistant reassociate Operation

The `reassociate (rs)` operation moves synchronization profiles to another node and reassociates the profiles with the new node. For example, if the middle-tier components are associated with a particular Oracle Identity Management infrastructure, then all the profiles existing in that infrastructure node can be moved to a new infrastructure node and the profiles will be reassociated accordingly.

If a profile does not exist on the new node, it is copied to the new Oracle Internet Directory node and disabled after copying. It must be enabled by the application. The `lastchangenumber` attribute in the integration profile is modified to the current last change number on the second Oracle Internet Directory node.

If a profile is moved to a node that already has a corresponding profile, both integration profiles are reconciled in the following manner:

- Any new attribute in the profile on node 1 is added to the profile on node 2.
- For existing same attributes, the values in profile on node 1 override the attributes in the profile on node 2.
- The profile is disabled after copying. It needs to be enabled by the application.

- The `lastchangenumber` attribute in the integration profile is modified to the current last change number on the second Oracle Internet Directory node.

Syntax for dipassistant reassociate

```
dipassistant reassociate [-src_ldap_host oid1_hostname] [-src_ldap_port port]
[-src_sslmode ssl_mode] [-src_ldap_dn bindDN] [-src_ldap_passwd password]
-dst_ldap_host oid2_hostname [-dst_ldap_port port] [-dst_sslmode
ssl_mode][-dst_ldap_dn bindDN] [-dst_ldap_passwd password] [-log logfile]
```

Arguments for dipassistant reassociate

-src_ldap_host *oid1_hostname*

Optional. The host name of the source Oracle Internet Directory server. If not provided then the name of the local host is used.

-src_ldap_port *port*

Optional. The LDAP listening port of the source Oracle Internet Directory server. The default is 389.

-src_sslmode *ssl_mode*

Optional. The SSL authentication mode of the source Oracle Internet Directory server. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-src_ldap_dn *bindDN*

The DN of the super user on the source Oracle Internet Directory server (`cn=orcladmin`).

-src_ldap_passwd *password*

The password used to bind to the source directory.

-dst_ldap_host *oid2_hostname*

Required. The host name of the destination Oracle Internet Directory server.

-dst_ldap_port *port*

Optional. The LDAP listening port of the destination Oracle Internet Directory server. The default is 389.

-dst_sslmode *ssl_mode*

Optional. The SSL authentication mode of the destination Oracle Internet Directory server. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-dst_ldap_dn *bindDN*

The DN of the super user on the destination Oracle Internet Directory server (`cn=orcladmin`).

-dst_ldap_passwd *password*

The password used to bind to the destination directory.

-log *logfile*

The file name of the log for the operation.

Tasks and Examples for dipassistant reassociate

Using the `reassociate` operation you can perform the following tasks:

- Moving an Integration Profile to a Different Identity Management Node

Moving an Integration Profile to a Different Identity Management Node

Example:

```
dipassistant reassociate -src_ldap_host oid1.mycorp.com -dst_ldap_host
oid2.mycorp.com -src_ldap_passwd srcpassword -dst_ldap_passwd dstpassword
```

The dipassistant showprofile Operation

The `showprofile (sp)` operation prints the details of a specific synchronization profile.

Syntax for dipassistant showprofile

```
dipassistant showprofile -profile profile_name [-h oid_hostname] [-p port] [-U
ssl_mode] [-D bindDN] [-w password]
```

Arguments for dipassistant showprofile

-p *profile_name*

Required. The name of the synchronization profile you want to view.

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-U *ssl_mode*

Optional. A number between 1 and 3 that represents the SSL mode of Oracle Internet Directory. The SSL modes are as follows:

- 1 – SSL mode with no authentication
- 2 – SSL mode with server-only authentication
- 3 – SSL mode with both client and server authentication

-D "*bindDN*"

The DN of the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration Platform Administrators group (`cn=dipadmingrp,cn=odi,cn=oracle internet directory`).

-w *password*

The password used to bind to the directory.

-configset *configset_number*

Optional. An integer greater than 0 that represents the configuration set associated with the profile. Default is 1.

Tasks and Examples for dipassistant showprofile

Using the `showprofile` operation you can perform the following tasks:

- Viewing the Details of a Specific Synchronization Profile

Viewing the Details of a Specific Synchronization Profile The following example command prints the details for the `ActiveImport` sample profile that is created during installation.

Example:

```
dipassistant showprofile -profile ActiveImport -h myhost -p 3060 -D cn=dipadmin -w
welcome1
```

The preceding command prints the following details of the `ActiveImport` sample profile:

```
odip.profile.version = 2.0
odip.profile.lastchgnum = 0
odip.profile.interface = LDAP
odip.profile.oidfilter = orclObjectGUID
odip.profile.schedinterval = 60
odip.profile.name = ActiveImport
odip.profile.syncmode = IMPORT
odip.profile.condirfilter =
searchfilter=(|(objectclass=group)(objectclass=organizationalunit)
(&(objectclass=user)(!(objectclass=computer))))
odip.profile.retry = 5
odip.profile.debuglevel = 0
odip.profile.status = DISABLE
```

The dipassistant wpasswd Operation

The `wpasswd (wp)` operation sets the wallet password that the Oracle Directory Integration Platform server uses to connect to Oracle Internet Directory.

Syntax for dipassistant wpasswd

```
dipassistant wpasswd
```

Arguments for dipassistant wpasswd

The Directory Integration Platform Assistant prompts you to enter, and then confirm, the password.

Tasks and Examples for dipassistant wpasswd

Using the `wpasswd` operation you can perform the following tasks:

- Setting the Wallet Password for the Oracle Directory Integration Platform Server

Setting the Wallet Password for the Oracle Directory Integration Platform Server

Example:

```
dipassistant wp
```

The dipassistant extauth Operation

The `extauth (ea)` operation configures external authentication plug-in for the connected directory.

Syntax for dipassistant extauth

```
dipassistant exauth [-h hostName] [-p port] -D bindDN -w bindPassword -t
extDirType
```

Arguments for dipassistant extauth

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *oid_port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-D *bindDN*

The DN of the super user (`cn=orcladmin`), or any other user that is a member of the Directory Integration Platform Administrators goup (`cn=dipadmingrp, cn=odi, cn=oracle internet directory`).

-w *bindPassword*

The password used to bind to the directory.

-t *extDirType*

The external directory type. The values allowed are:

- AD (Active Directory)
- iPlanet
- eDirectory
- OpenLDAP

Tasks and Examples for dipassistant extauth

Using the `extauth` operation, you can perform the following tasks:

- Configuring External Authentication plug-in for the Connected Directory

Configuring External Authentication plug-in for the Connected Directory The following example configures an external authentication plug-in for Microsoft Active Directory.

Example:

```
dipassistant ea -h localhost -p 389 -D cn=orcladmin -w welcome -t AD
```

Running dipassistant in SSL Mode

`dipassistant` can connect to Oracle Internet Directory or a third-party directory in SSL mode. The following topics discuss the tasks you need to perform to connect to the directory using SSL mode:

- Connecting to Oracle Internet Directory
- Connecting to a Third-Party Directory

Connecting to Oracle Internet Directory

You need to perform the following tasks before running `dipassistant` in SSL mode:

1. Specify the wallet location in the `odi.properties` file. This file can be found under the `$ORACLE_HOME/ldap/odi/conf` directory.
2. Set the wallet password using the `dipassistant wpasswd` command. See "The dipassistant wpasswd Operation" on page 6-25 for more information.

> **Note:** The preceding steps are required only when connecting to Oracle Internet Directory using the `-U 2` (server-only authentication) or `-U 3` (server and client authentication) option.These steps are not required when connecting to Oracle Internet Directory using the `-U 1` (SSL mode with no authentication) option.

Connecting to a Third-Party Directory

`dipassistant` can connect to a third-party directory in the following scenarios:

- `dipassistant bootstrap` is used to perform an initial migration of data between the third-party directory and Oracle Internet Directory.
- `dipassistant modifyprofile -updlcn` is used to get the last change number from the third-party (connected) directory for an import profile.

Perform the following tasks before using `dipassistant` to connect to a third-party directory in SSL mode:

1. Specify the wallet location in the `odi.properties` file. This file can be found under the `$ORACLE_HOME/ldap/odi/conf` directory.
2. Set the wallet password using the `dipassistant wpasswd` command. See "The dipassistant wpasswd Operation" on page 6-25 for more information.
3. Generate a certificate from the connected directory. An external certificate authority is not required for this.
4. Export the certificate to `Base64` encoded format.
5. Import the certificate as a trust point into the Oracle wallet using Oracle Wallet Manager.

Related Command-Line Tools for dipassistant

- See "oidprovtool" on page 6-29

odisrvreg

The `odisrvreg` command-line tool registers an Oracle Directory Integration Platform server with Oracle Internet Directory. This tool creates an entry in the directory and sets the password for the Directory Integration Platform server. If the registration entry already exists, then you can use the tool to reset the existing password. The `odisrvreg` tool also creates a local file called `odisrvwallet_`*`hostname`* in *`ORACLE_HOME`*`/ldap/odi/conf`. This file acts as a private wallet for the Directory Integration Platform server, which uses it on startup to bind to the directory.

Syntax for odisrvreg

```
odisrvreg -h oid_hostname -p port -D bindDN -w password
[-U SSL_auth_mode -W wallet_location -P wallet_password]
```

Arguments for odisrvreg

-h *oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

-p *port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

-D "*bindDN*"

The DN of the directory super user (`cn=orcladmin`).

-w *password*

The password used to bind to the directory.

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

- `1` for no authentication required.
- `2` for one way authentication required. You must also supply a wallet location and wallet password.
- `3` for two way authentication required. You must also supply a wallet location and wallet password.

-W *wallet_location*

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

-P *wallet_password*

Required if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument.

Tasks and Examples for odisrvreg

Using the `odisrvreg` command-line tool, you can perform the following tasks:

- Registering the Oracle Directory Integration Platform Server With Oracle Internet Directory

Registering the Oracle Directory Integration Platform Server With Oracle Internet Directory

The following example shows how to register the Oracle Directory Integration Platform server with Oracle Internet Directory using SSL for secure communications.

Example:

```
odisrvreg -h myhost.company.com -p 3040 -D "cn=orcladmin" -w welcome1 -U 2
-W "file:/home/my_dir/my_wallet" -P walpasswd123
```

Related Command-Line Tools for odisrvreg

- See "schemasync" on page 6-35

oidprovtool

Provisioning enables you to ensure that an application is notified of directory changes, such as changes to user or group information. Such changes can affect whether the application allows a user access to its processes and resources.

When you install an application that you want to provision, you must create a provisioning integration profile for it by using the Provisioning Registration Tool (`oidprovtool`). Use this tool to:

- Create a new provisioning profile. A new provisioning profile is created and set to the enabled state so that Oracle Directory Integration Platform can process it.
- Disable an existing provisioning profile.
- Enable a disabled provisioning profile.
- Modify an existing provisioning profile.
- Delete an existing provisioning profile.
- Get the current status of a given provisioning profile.
- Clear all of the errors in an existing provisioning profile.

The Provisioning Registration Tool shields the location and schema details of the provisioning profile entries from the callers of the tool. From the callers' perspective, the combination of an application and a realm uniquely identify a provisioning profile. The constraint in the system is that there can be only one provisioning profile for each application for each realm.

Once a profile is created, its mode—that is, INBOUND, OUTBOUND, or BOTH—cannot be changed by using the `modify` operation. To change the mode, you must delete, then re-create, the profile.

The Oracle directory integration platform server automatically monitors provisioning profile configuration changes in Oracle Internet Directory, including the creation, modification, and deletion of provisioning profiles. For this reason, you do not need to manually enable or disable a provisioning profile.

Syntax for oidprovtool

```
oidprovtool operation=[create|modify] ldap_host=oid_hostname ldap_port=port \
ldap_user_dn="bindDN" ldap_user_password=password \
[profile_mode=INBOUND|OUTBOUND|BOTH]
application_dn="DN" application_type=type [application_name=name] \
[application_display_name=display name] organization_dn=DN \
[application_isdasvisible=TRUE|FALSE] [manage_application_defaults=TRUE|FALSE] \
[enable_bootstrap=TRUE|FALSE]  [user_data_location=DN] \
[default_provisioning_policy=PROVISIONING_REQUIRED|PROVISIONING_NOT_REQUIRED] \
interface_name=SCHEMA.PACKAGE [interface_type=PLSQL|JAVA] \
interface_version=1.1|2.0|3.0] interface_connect_info=connection_string \
schedule=number_seconds lastchangenumber=number   \
max_prov_failure_limit=number  \
max_events_per_schedule=number max_events_per_invocation=number \
event_mapping_rules="OBJECT_TYPE:FILTER:DOMAIN" \
event_permitted_operations="OBJECT:DOMAIN:OPERATION(attributes,...)" \
event_subscription="USER|GROUP:DOMAIN:OPERATION(attributes,...)" \
max_events_per_schedule=number max_retries=number profile_group=number \
profile_status=ENABLED | DISABLED profile_debug=debug_level

oidprovtool {operation=enable|disable|delete|status|reset}
application_dn=DN [organization_dn=DN] [ldap_host=oid_hostname] [ldap_port=port]
[ldap_user_dn=bindDN] [ldap_user_password=password] [profile_debug=debug_level]
```

Arguments for oidprovtool

operation=create | modify | enable | disable | delete | status | reset

Required. The operation to perform using `oidprovtool`. You can only perform one operation at a time. The operations are:

- create - Creates a new provisioning profile.
- modify - Modifies the given properties of an existing provisioning profile.
- enable - Enables a provisioning profile.
- disable - Disables a provisioning profile.
- delete - Deletes a provisioning profile.
- status - Shows the current status of a given provisioning profile.
- reset - Clears all errors for a provisioning profile.

ldap_host=*oid_hostname*

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

ldap_port=*port*

Optional. The LDAP listening port of Oracle Internet Directory. The default is 389.

ldap_user_dn=*bindDN*

The DN of the super user or a user that has sufficient permissions to perform provisioning subscription operations. The default is `cn=orcladmin`.

ldap_user_password=*password*

The user password used to bind to the directory.

profile_mode=OUTBOUND | INBOUND | BOTH

Optional for the `create` operation only. The direction of the provisioning events. The default is OUTBOUND (data is provisioned from Oracle Internet Directory to the application).

application_dn=*DN*

Required. The distinguished name of the application to which the provisioning subscription belongs. The combination of the application DN and organization DN uniquely identifies a provisioning profile. For example, here is the application DN for Portal:

```
"orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext"
```

application_type=*type*

Required. The type of application being provisioned.

application_name=*name*

Optional. The name of the application being provisioned. If not provided, defaults to the distinguished name assigned to `application_dn`.

application_display_name=*name*

Optional. The display name of the application being provisioned. If not provided, defaults to the value assigned to `application_name`.

organization_dn=*DN*

Optional. If not provided, defaults to the default identity management realm. The distinguished name of the organization to which the provisioning subscription belongs, for example "`dc=company,dc=com`". The combination of the application DN and organization DN uniquely identifies a provisioning profile.

application_isdasvisible=TRUE | FALSE

Optional. Determines whether the application is visible as a provisioning-integrated application in the Oracle Internet Directory Provisioning Console. The default value is TRUE.

manage_application_default=TRUE | FALSE

Optional. Determines whether the Oracle Internet Directory Provisioning Console manages the application's default values. The default value is TRUE.

enable_bootstrap=TRUE | FALSE

Optional. Indicates whether the application should receive provisioning events for users that existed in Oracle Internet Directory before creating the application's provisioning integration profile. The default value is FALSE.

user_data_location=*DN*

Optional. Identifies the DN of the container in which to store application-specific user information.

default_provisioning_policy=PROVISIONING_REQUIRED | PROVISIONING_NOT_REQUIRED

Optional. Specifies the application's default provisioning policy. The default value is PROVISIONING_REQUIRED.

interface_name=SCHEMA.PACKAGE

Required for `create` or `modify` operations. The database schema name for the PLSQL package. The format of the value is `schema.package_name`, for example here is the schema and PLSQL package information for Portal:

```
interface_name=PORTAL.WWSEC_OID_SYNC
```

interface_version=1.1 | 2.0 | 3.0

The version of the interface protocol. Allowed values are 1.1, 2.0, or 3.0. The default value is 2.0.

interface_type=PLSQL | JAVA

Optional. The type of interface to which events will be propagated. The default is PLSQL.

interface_connect_info=*connection_string*

Required for `create` or `modify` operations. To connect to an Oracle database and propagate events, use one of the following formats for the connection string:

- DBURL=ldap://*ldaphost*:*ldapport*/*service*:*username*:*password* (recommended)
- *host*:*port*:*sid*:*username*:*password*
- DBSVC=*service*:*username*:*password*

schedule=*number_seconds*

Optional for `create` and `modify` operations only. The number of seconds between executions of this profile. The default is 3600, which means the profile is scheduled to be executed every hour.

lastchangenumber=*number*

Optional for `create` and `modify` operations on `OUTBOUND` events only. The last change number in Oracle Internet Directory after which all qualifying events should be provisioned to the application. Defaults to the latest current change number.

max_prov_failure_limit=*number*

Optional. Determines the number of times the Oracle Provisioning System attempts to provision a user. The default is 1.

max_events_per_schedule=*number*

Optional for `create` and `modify` operations only. The maximum number of events that the Oracle directory integration platform server sends to an application during one execution of a provisioning profile. The default is 100.

max_events_per_invocation=*number*

Optional for `create` and `modify` operations only. The maximum number of events that can be packaged and sent to a target in one invocation of the interface.

event_mapping_rules="*OBJECT_TYPE*:*FILTER*:*DOMAIN*"

Required for `create` and `modify` operations on `INBOUND` events only. This rule maps the object type received from the application (using an optional filter condition) to a domain in Oracle Internet Directory A provisioning profile can have multiple mapping rules defined.

The following example shows two mapping rules. The first rule shows that an employee object (EMP) whose locality attribute equals America (l=AMERICA) should be mapped to the domain l=AMER,cn=users,dc=company,dc=com. The second rule shows that an employee object (EMP) should be mapped to the domain cn=users,dc=company,dc=com (no filter conditions).

```
event_mapping_rules="EMP:l=AMERICA:l=AMER,cn=users,dc=company,dc=com"
event_mapping_rules="EMP::cn=users,dc=company,dc=com"
```

event_permitted_operations="*OBJECT*:*DOMAIN*:*OPERATION*(*attributes*,...)

Required for create and modify operations on INBOUND events only. This property is used to define the types of events that the application is allowed to send to the Oracle Directory Integration Platform service. A provisioning profile can have multiple permitted operations defined.

For example, if you wanted to permit the application to send events whenever a user object was added or deleted, or when certain attributes were modified, you would have three permitted operations such as this:

```
event_permitted_operations="USER:dc=mycompany,dc=com:ADD(*)"
event_permitted_operations="USER:dc=mycompany,dc=com:MODIFY(cn,sn,mail,password)"
event_permitted_operations="USER:dc=mycompany,dc=com:DELETE(*)"
```

event_subscription="USER | GROUP:*DOMAIN*:*OPERATION*(*attributes*,...)"

Required for create and modify operations on OUTBOUND events only. This property is used to define the types of events that the Oracle Directory Integration Platform service should send to the application. A provisioning profile can have multiple event subscriptions defined.

For example, if you wanted the directory integration server to send events to the application whenever a user or group object was added or deleted, you would have four event subscriptions such as this:

```
event_subscription="GROUP:dc=mycompany,dc=com:ADD(*)"
event_subscription="GROUP:dc=mycompany,dc=com:DELETE(*)"
event_subscription="USER:dc=mycompany,dc=com:ADD(*)"
event_subscription="USER:dc=mycompany,dc=com:DELETE(*)"
```

max_events_per_schedule=*number*

Optional for create and modify operations only. The maximum number of events to be provisioned in one schedule. The default is 100.

max_retries=*number*

Optional for create and modify operations only. The number of times a failed event should be retried. The default is 5.

profile_group=*number*

Required for create and modify operations only. The group number of the profile. Default is "DEFAULT". This is required to address scalability issues when different Oracle Directory Integration Platform server instances will be used to execute different selected groups.

profile_status=ENABLED | DISABLED

Required for the create operation only. Determines whether the profile is enabled or disabled. The default is ENABLED.

profile_debug=*debug_level*

Required. The debug level for the profile.

Tasks and Examples for oidprovtool

Using the Provisioning Registration Tool (`oidprovtool`) you can perform the following tasks:

- Creating a Provisioning Profile
- Modifying a Provisioning Profile
- Deleting a Provisioning Profile
- Disabling a Provisioning Profile

Creating a Provisioning Profile

The following example creates a new provisioning profile that makes Portal aware of updates to the user and group information that is maintained in Oracle Internet Directory.

Example:

```
oidprovtool operation=create ldap_host=myhost.mycompany.com ldap_port=389 \
ldap_user_dn="cn=orcladmin" ldap_user_password=welcome1
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com" interface_name=PORTAL.WWSEC_OID_SYNC \
interface_type=PLSQL interface_connect_info=myhost:1521:iasdb:PORTAL:password \
schedule=360 event_subscription="USER:dc=us,dc=mycompany,dc=com:DELETE" \
event_subscription="GROUP:dc=us,dc=mycompany,dc=com:DELETE" \
event_subscription="USER:dc=us,dc=mycompany,dc=com:MODIFY(orclDefaultProfileGroup,
userpassword)" \
event_subscription="GROUP:dc=us,dc=mycompany,dc=com:MODIFY(uniqueMember)" \
profile_mode=OUTBOUND
```

Modifying a Provisioning Profile

The following example modifies an existing provisioning profile for the Portal application. It changes the event subscription for the attributes that are provisioned when a user entry is modified.

Example:

```
oidprovtool operation=modify ldap_host=myhost.mycompany.com ldap_port=389 \
ldap_user_dn="cn=orcladmin" ldap_user_password=welcome1
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com" \
subscription="USER:dc=us,dc=mycompany,dc=com:MODIFY(orclDefaultProfileGroup,userpa
ssword,mail,cn,sn)"
```

Deleting a Provisioning Profile

The following example disables a provisioning profile for the Portal application.

Example:

```
oidprovtool operation=delete ldap_host=myhost.mycompany.com ldap_port=389 \
ldap_user_dn="cn=orcladmin" ldap_user_password=welcome1
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
```

```
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com"
```

Disabling a Provisioning Profile

The following example disables a provisioning profile for the Portal application.

Example:

```
oidprovtool operation=disable ldap_host=myhost.mycompany.com ldap_port=389 \
ldap_user_dn="cn=orcladmin" ldap_user_password=welcome1
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com"
```

Related Command-Line Tools for oidprovtool

- See "dipassistant" on page 6-1

schemasync

The `schemasync` command-line tool enables you to synchronize schema elements—namely attributes and object classes—between an Oracle Internet Directory server and a third-party LDAP directory.

The errors that occur during schema synchronization are logged in the following files:

- $*ORACLE_HOME*/ldap/odi/log/attributetypes.log
- $*ORACLE_HOME*/ldap/odi/log/objectclasses.log

Syntax for schemasync

```
schemasync -srchost hostname -srcport port -srcdn bindDN -srcpwd password
-dsthost hostname -dstport port -dstdn bindDN -dstpwd password [-ldap]
```

Arguments for schemasync

-srchost *hostname*

The host name of the source directory server.

-srcport *port*

The LDAP listening port of the source directory server, for example 389.

-srcdn *bindDN*

The DN of the user used to bind to the source directory. This user must have permissions to modify the directory schema, for example the super user (`cn=orcladmin`).

-srcpwd *password*

The user password used to bind to the source directory.

-dsthost *hostname*

The host name of the destination directory server.

-dstport *port*

The LDAP listening port of the destination directory server, for example 389.

-dstdn *bindDN*

The DN of the user used to bind to the destination directory. This user must have permissions to modify the directory schema, for example the super user.

-dstpwd *password*

The user password used to bind to the destination directory.

-ldap

Optional. If specified, then the schema changes are applied directly from the source LDAP directory to the destination LDAP directory. If it is not specified, then the schema changes are placed in the following LDIF files:

- $*ORACLE_HOME*/ldap/odi/data/attributetypes.ldif: This file has the new attribute definitions.
- $*ORACLE_HOME*/ldap/odi/data/objectclasses.ldif: This file has the new object class definitions.

If you do not specify `-ldap`, then you must use "ldapmodify" on page 4-27 to upload the definitions from these two files, first attribute types and then object classes.

Tasks and Examples for schemasync

Using the `schemasync` command-line tool, you can perform the following tasks:

- Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory

Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory

The following example shows how to synchronize the schema between Oracle Internet Directory and a third-party directory server.

Example:

```
schemasync -srchost myhost1.mycompany.com -srcport 389 -srcdn "cn=orcladmin"
-srcpwd welcome1 -dsthost myhost2.mycompany.com -dstport 389 -dstdn
"uid=superuser,ou=people,dc=mycompany,dc=com" -dstpwd admin123 -ldap
```

Related Command-Line Tools for schemasync

- See "ldapmodify" on page 4-27

Part II

LDAP Schema Reference

Part II of the *Oracle Identity Management User Reference* contains information about the LDAP schema elements for Oracle Identity Management.

Part II contains the following chapters:

7

LDAP Schema Overview

This chapter provides an overview of some of the basic concepts of the LDAP directory schema, and provides categorized lists of the schema elements for Oracle Identity Management. This chapter contains the following topics:

Overview of Directory Schema

A directory schema specifies, among other rules, the types of objects that a directory may have and the mandatory and optional attributes of each object type. The Lightweight Directory Access Protocol (LDAP) version 3 defines a schema based on the X.500 standard for common objects found in a network, such as countries, localities, organizations, people, groups, and devices. In the LDAP v3, the schema is available from the directory. That is, it is represented as entries in the directory and its information as attributes of those entries.

Object Classes

An object class is an LDAP directory term that denotes the type of object being represented by a directory entry or record. There are also object classes that define an object's relationship to other objects, such as object class `top` denotes that the object may have subordinate objects under it in a hierarchical tree structure. Some LDAP object classes may be combined to create an entry in the directory. For example, and entry for a user uses the `top`, `person`, `organizationalPerson`, `inetOrgPerson`, and `orclUserV2` object classes.

Required and Allowed Attributes

The definition of an object class includes a list of required attributes (MUST) and allowed attributes (MAY). Required attributes include the attributes that must be present in entries using the object class. Allowed attributes include the attributes that may be present in entries using the object class.

Object Class Types

The X.500 1993 specification requires that object classes be assigned to one of four categories:

- Structural: Object classes that can have instances in the directory. Structural classes are used to create directory objects or entries.
- Abstract: Template object classes that are used only to derive new structural classes. Abstract classes cannot be instantiated in the directory.

- Auxiliary: A list of attributes that can be appended to the definition of a Structural or Abstract class. An Auxiliary class cannot be instantiated in the directory.
- 88 Classes: Assigning object classes to categories was not required in the X.500 1988 specification. Classes that were defined prior to the X.500 1993 standards, default to the 88 class. Do not define new 88 classes.

Object Class Inheritance

Inheritance, which is also referred to as derivation, is the ability to build new object classes from existing object classes. The new object is defined as a subclass of the parent object. A subclass is a class that inherits from some other class; for example, a subclass inherits structure and content rules from the parent. The parent object becomes a superclass of the new object. A superclass is a class from which one or more other classes inherit information.

Attributes

Directory data is represented as attribute-value pairs. Any piece of information in the directory is associated with a descriptive attribute. For example, the `cn` (`commonName`) attribute is used to store a nickname. A person named William (Bill) Smith can be represented in the directory as:

```
cn: Bill Smith
```

Attribute Name Limitations

The length of an attribute name must not exceed 127 characters. For more information about attribute management, refer to the *Oracle Internet Directory Administrator's Guide*.

Oracle Internet Directory imposes no limitations on the characters that can be used in attribute names. Other components of Oracle Identity Management, however, do limit the characters that can be used for certain attributes.

Oracle Delegated Administration Services and Oracle Directory Integration Platform prohibit the use of spaces and of any of the following characters in `UserID`: & ' % ? \ / + = ( ) * ^ , ; | ' ~

Oracle Application Server Single Sign-On requires that a password should not contain the following characters: & { } < > " ' ( )

Attribute Syntax

An attribute syntax is the basic building block of an attribute. Every attribute is assigned a syntax that defines the attribute value's data format. For example, attribute syntaxes determine whether an attribute stores an integer, string, or binary data. The syntax also defines the matching rules that control the type of comparison operations you can perform on the attribute value.

Oracle Internet Directory recognizes attribute syntax as specified in RFC 2252, that is, it enables you to associate the attribute syntax described in that document with an attribute. Oracle Internet Directory enforces attribute syntax for the following types:

- DN
- OID (object identifier)
- Telephone Number

The following table describes the attribute syntax most commonly used in Oracle Internet Directory:

Table 7–1 Attribute Syntax Commonly Used in Oracle Internet Directory

Syntax and Object ID	Description
ACI Item 1.3.6.1.4.1.1466.115.121.1.1	Values for this attribute are access control identifier items.
Binary 1.3.6.1.4.1.1466.115.121.1.5	Values for this attribute are binary.
Boolean 1.3.6.1.4.1.1466.115.121.1.7	The attribute can contain only one of two values: true (1) or false (0).
Directory String 1.3.6.1.4.1.1466.115.121.1.15	Values for this attribute are strings which are not case-sensitive.
DN 1.3.6.1.4.1.1466.115.121.1.12	Values for this attribute are DNs (distinguished names).
Generalized Time 1.3.6.1.4.1.1466.115.121.1.24	Values for this attribute are encoded as printable strings. A time zone must be specified (such as GMT).
IA5String 1.3.6.1.4.1.1466.115.121.1.26	International Reference Alphabet Reference Alphabet No. 5 string. Values for this attribute are case-sensitive.
Integer 1.3.6.1.4.1.1466.115.121.1.27	Valid values for this attribute are numbers.
JPEG 1.3.6.1.4.1.1466.115.121.1.28	Valid values for this attribute are JPEG files.
Name 1.3.6.1.4.1.1466.115.121.1.34	Valid values for this attribute are names or optional UIDs.
OID 1.3.6.1.4.1.1466.115.121.1.38	A unique object identifier.
Printable String 1.3.6.1.4.1.1466.115.121.1.44	A string that does NOT allow extended characters. Values for this attribute are not case-sensitive.
Telephone Number 1.3.6.1.4.1.1466.115.121.1.50	Values for this attribute are in the form of telephone numbers.

Attribute Aliases

As of 10*g* (10.1.4.0.1), you can create aliases for attribute names. For example. you could create the user-friendly alias `surname` for the attribute `sn`. Once you create an alias for an attribute name, a user can specify the alias instead of the attribute name in an LDAP operation.

You define an alias for an attribute in the LDAP schema definition of the attribute. The directory schema operational attribute `attributeTypes` has been enhanced to allow you to include aliases in the attribute name list. In previous releases, the format for an attribute name list was:

```
attributeTypes=( ObjectIdentifier NAME 'AttributeName'  ... )

attributeTypes=( ObjectIdentifier NAME ( 'AttributeName' 'Alias1' 'Alias2' ...)
... )
```

As of 10*g* (10.1.4.0.1), you may optionally specify:

This is consistent with the LDAP protocol as specified by RFC 2251 and RFC 2252. In the attribute name list, the first item is recognized as the name of the attribute and rest of the items in the list are recognized as attribute aliases. For example, to specify the alias `surname` for the attribute `sn`, you would change the schema definition for `sn` from:

```
attributeTypes=( 2.5.4.4 NAME 'sn' SUP name )
```

to:

```
attributeTypes=( 2.5.4.4 NAME ( 'sn' 'surname' ) SUP name )
```

> **See Also:** For more information regarding attribute alias rules, managing attribute aliases using command-line tools, and using attribute aliases refer to the "Attribute Aliases In the Directory" section in *Oracle Internet Directory Administrator's Guide*

Matching Rules

Matching rules are the rules for matching two attribute values that comply with the same attribute syntax. Oracle Internet Directory recognizes the following matching rule definitions in the schema.

- `accessDirectiveMatch`
- `IntegerMatch`
- `bitStringMatch`
- `numericStringMatch`
- `caseExactMatch`
- `objectIdentifierFirstComponentMatch`
- `caseExactIA5Match`
- `ObjectIdentifierMatch`
- `caseIgnoreIA5Match`
- `OctetStringMatch`
- `caseIgnoreListMatch`
- `presentationAddressMatch`
- `caseIgnoreMatch`
- `protocolInformationMatch`
- `caseIgnoreOrderingMatch`
- `telephoneNumberMatch`
- `distinguishedNameMatch`
- `uniqueMemberMatch`
- `generalizedTimeMatch`
- `generalizedTimeOrderingMatch`
- `orclpkimatchingrule`

Of the matching rules in the previous list, Oracle Internet Directory actually enforces the following when it compares attribute values:

- distinguishedNameMatch
- caseExactMatch
- caseIgnoreMatch
- numericStringMatch
- IntegerMatch
- telephoneNumberMatch
- orclpkimatchingrule

Sizing of Attribute Values

Attribute syntax does not put any specific size constraint on attribute values. You can, however, specify the size of the attribute value when defining the attribute. Some attributes in Oracle Internet Directory may have size constraints defined, however length characteristics of an attribute are not enforced.

For example, to limit an attribute `foo` to a size of 64, you would define the attribute as follows:

```
(object_identifier_of_attribute NAME 'foo' EQUALITY caseIgnoreMatch SYNTAX
'object_identifier_of_syntax{64}')
```

Single-Valued and Multi-Valued Attributes

By default, most attributes are multi-valued. This means that an entry can contain the same attribute with multiple values. For single-valued attributes, only one instance of the attribute can be specified in an entry. For example, the attribute `orclObjectGUID` attribute can only have one possible value.

Attribute Usage

Attribute Usage defines how the attribute is used in the directory. The attribute usage types are:

- userApplications - User applications attribute. This is the default attribute usage if not explicitly defined for the attribute.
- directoryOperation - Directory operational attribute.
- dSAOperation - DSA operational attribute.

Not User Modifiable

Attributes that are designated as "not user modifiable" can only be modified by the directory server. They cannot be modified by any other user or process.

LDAP Controls

As an LDAP Version 3 directory, Oracle Internet Directory extends the standard LDAP operations by using controls. These are extra pieces of information carried along with existing operations, altering the behavior of the operation. When a client application passes a control along with the standard LDAP command, the behavior of the commanded operation is altered accordingly.

Table 7–2 Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113730.3.4.2	GSL_MANAGE_ DSA_CONTROL	Used to manage referrals, dynamic groups, and alias objects in Oracle Internet Directory. For more information, please see RFC 3296 at http://www.ietf.org
2.16.840.1.113894.1.8.1	OID_RESET_ PROXYCONTROL _IDENTITY	Used to perform a proxy switch of an identity on an established LDAP connection. For example, suppose that Application A connects to the directory server and then wishes to switch to Application B. It can simply do a rebind by supplying the credentials of Application B. However, there are times when the proxy mechanism for the application to switch identities could be used even when the credentials are not available. With this control, Application A can switch to Application B provided Application A has the privilege in Oracle Internet Directory to proxy as Application B.
2.16.840.1.113894.1.8.2	OID_ APPLYUSEPASSW ORD_POLICY	Sent by applications that require Oracle Internet Directory to check for account lockout before sending the verifiers of the user to the application. If Oracle Internet Directory detects this control in the verifier search request and the user account is locked, then Oracle Internet Directory will not send the verifiers to the application. It will send an appropriate password policy error.

Table 7–2 (Cont.) Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113894.1.8.3	CONNECT_BY	Behavior determined based on the values passed with the control. Two values can be passed with the control: an integer and a string, in any order. The *string* value is required for queries where the hierarchy-establishing attribute cannot be determined from the search signature, that is, the base, scope, and filter. For searching all *containers in which an entry is contained*, the query filter (manger=cn=john doe,o=foo) contains the hierarchy -establishing attribute name (manager), so it does not need to be passed in the control value. The filter also contains the root of the hierarchy (cn=john doe, o=foo). For searching all *containers contained within an entry*, the query filter would typically be `objectclass=*` and the base would be the root of the hierarchy, and there is no information about the hierarchy-establishing attribute in the search signature. Thus, it must be passed in the control value. The *integer* value indicates the number of levels of the hierarchy to traverse. It can be present when querying in either direction, but is not required. If the value is zero or absent,then all levels are traversed. **Note:** For more information and examples of the CONNECT_BY control refer to the section "Performing Hierarchical Searches" in *Oracle Identity Management Application Developer's Guide*
2.16.840.1.113894.1.8.4	OID_CLIENT_IP_ ADDRESS	Intended for a client to send the end user IP address if IP lockout is to be enforced by Oracle Internet Directory.
2.16.840.1.113894.1.8.5	GSL_REQDATTR_ CONTROL	Used with dynamic groups. Directs the directory server to read the specific attributes of the members rather than the membership lists.
2.16.840.1.113894.1.8.6	OID_ PASSWORD_ REQUEST_ CONTROL	Password policy control. Request control that the client sends to get a response from the server.
2.16.840.1.113894.1.8.7	OID_ PASSWORD_ EXPWARNING_ CONTROL	Password policy control. Response control that the server sends when the `pwdExpireWarning` attribute is enabled and the client sends the request control. The response control value contains the time in seconds to password expiration.
2.16.840.1.113894.1.8.8	OID_ PASSWORD_ GRACELOGIN_ CONTROL	Password policy control. The response control that the server sends when grace logins are configured and the client sends a request control. The response control value contains the remaining number of grace logins.

Table 7–2 (Cont.) Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113894.1.8.9	OID_ PASSWORD_ MUSTCHANGE_ CONTROL	Password policy control. The response control that the server sends when forced password reset is enabled and the client sends the request control. The client must force the user to change the password upon receipt of this control.
2.16.840.1.113894.1.8.14	OID_DYNAMIC_ VERIFIER_ REQUEST_ CONTROL	The request control that the client sends when it wants the server to create a dynamic password verifier. The server uses the parameters in the request control to construct the verifier.
2.16.840.1.113894.1.8.15	OID_DYNAMIC_ VERIFIER_ RESPONSE_ CONTROL	The response control that the server sends to the client when an error occurs. The response control contains the error code.
2.16.840.1.113894.1.8.16	OID_ APPLYALLPWDP OLICIES_ CONTROL	Password policy for verifier control in the search request. If the control exists, then all state policies are applied to the verifier control that are applicable to the user.
2.16.840.1.113894.1.8.23	GSL_ CERTIFICATE_ CONTROL	Certificate search control. The request control that the client sends to specify how to search for a user certificate.
1.2.840.113556.1.4.473	OID_SEARCH_ SORTING_ REQUEST_ CONTROL	Obtains sorted results from an LDAP search, as described by IETF RFC 2891. You request sorted results by passing this control to the search function. The server returns a response control of type 1.2.840.113556.1.4.474. Error processing and other details are described in RFC 2891. **Note:** For the Oracle Internet Directory implementation of RFC 2891 refer to *Oracle Identity Management Application Developer's Guide*..
1.2.840.113556.1.4.319	OID_SEARCH_ PAGING_ CONTROL	Obtain paged results from an LDAP search, as described by IETF RFC 2696. You request sorted results by passing a control of type 1.2.840.113556.1.4.319 to the search function. Details are described in RFC 2696 **Note:** Sorting and paging may be used together. Also, refer to IETF RFC 2696, "LDAP Control Extension for Simple Paged Results Manipulation," at `http://www.ietf.org/rfc/rfc2696.txt`

Overview of Oracle Identity Management Schema Elements

This section lists the Oracle Identity Management schema elements by category. Each category contains a list of applicable LDAP object classes and attributes that link to the detailed information for the specified attribute or object class. The schema elements are grouped into the following categories:

- System Operational Schema Elements
- Oracle Internet Directory Configuration Schema Elements
- Audit and Error Logging Schema Elements

- Server Manageability Schema Elements
- Oracle Directory Replication Schema Elements
- Oracle Directory Integration Platform Schema Elements
- Oracle Delegated Administration Services Schema Elements
- Oracle Application Server Certificate Authority and PKI Schema Elements
- Application Schema Elements
- Resource Schema Elements
- Plug-in Schema Elements
- Directory User Agents Schema Elements
- User, Group, and Subscriber Schema Elements
- Password Policy Schema Elements
- Password Verifier Schema Elements

System Operational Schema Elements

System operational schema elements are those used by the directory server. System operational object classes are used by the directory server to create entries that pertain to directory server operations. Certain system operational attributes may be available for use on every entry in the directory, regardless of whether they are defined for the object class of the entry. This section contains the following topics:

- Directory Schema
- Access Control
- Change Logs
- Password Policy

Directory Schema

This section lists the operational attributes and object classes for the directory schema.

Attributes

attributeTypes, contentRules, ldapSyntaxes, matchingRules, objectClasses

Object Classes

subschema

Access Control

This section lists the operational attributes for access control.

Attributes

orclACI, orclEntryLevelACI

Change Logs

This section lists the operational attributes for change logs.

Attributes

createTimestamp, creatorsName, modifiersName, modifyTimestamp

Password Policy

This section lists the operational attributes for password policy.

Attributes

orclPwdAccountUnlock, orclPwdIPAccountLockedTime, orclPwdIPFailureTime, orclRevPwd, orclUnsyncRevPwd, pwdAccountLockedTime, pwdChangedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdHistory, pwdReset

Oracle Internet Directory Configuration Schema Elements

This section lists the schema elements that pertain to the configuration of Oracle Internet Directory. It contains the following topics:

- Oracle Internet Directory Server
- Oracle Context
- Oracle Network Services
- Garbage Collection
- Attribute Uniqueness

Oracle Internet Directory Server

This section lists the attributes and object classes that pertain to the configuration of Oracle Internet Directory server.

Attributes

namingContexts, orclAnonymousBindsFlag, orclAuditLevel, orclCatalogEntryDN, orclConfigSetNumber, orclCryptoScheme, orclDBType, orclDebugFlag, orclDebugForceFlush, orclDebugOp, orclDIPRepository, orclDirectoryVersion, orclDITRoot, orclEcacheEnabled, orclEcacheMaxEntries, orclEcacheMaxEntSize, orclEcacheMaxSize, orclEnableGroupCache, orclEventLevel, orclGUName, orclGUPassword, orclHostname, orclIndexedAttribute, orclIndexHints, orclIpAddress, orclLDAPConnTimeout, orclMatchDnEnabled, orclMaxCC, orclMaxEntInBER, orclMaxTcpIdleConnTime, orclNonSSLPort, orclNormDN, orclNwrwTimeout, orclPKIMatchingRule, orclPrName, orclPrPassword, orclReplAgreements, orclReplicaID, orclSASLAuthenticationMode, orclSASLCipherChoice, orclSASLMechanism, orclsDumpFlag, orclServerMode, orclServerProcs, orclSizeLimit, orclSkewedAttribute, orclSkipRefInSQL, orclSSLAuthentication, orclSSLCipherSuite, orclSSLEnable, orclSSLPort, orclSSLVersion, orclSSLWalletURL, orclStatsDN, orclStatsFlag, orclStatsLevel, orclStatsOp, orclStatsPeriodicity, orclSUAccountLocked, orclSuffix, orclSULoginFailureCount, orclSUName, orclSUPassword, orclTimeLimit, orclTLimitMode, orclUpgradeInProgress

Object Classes

orclDSAConfig, orclIndexOC, orclLDAPInstance, orclLDAPSubConfig, subentry, subregistry

Oracle Context

This section lists the attributes and object classes that pertain to the configuration of the Oracle Context.

Attributes

orclCommonAutoRegEnabled, orclCommonContextMap, orclCommonDefaultUserCreateBase, orclCommonGroupCreateBase, orclCommonNamingAttribute, orclCommonNicknameAttribute, orclCommonSASLRealm, orclCommonUserSearchBase, orclDefaultSubscriber, orclProductVersion, orclSubscriberNickNameAttribute, orclSubscriberSearchBase, orclUserObjectClasses, orclVersion

Object Classes

orclCommonAttributes, orclCommonAttributesV2, orclRootContext, orclSchemaVersion

Oracle Network Services

This section lists the attributes and object classes that pertain to the configuration of Oracle Network Services.

Attributes

labeledURI, orclActiveEndDate, orclActiveStartdate, orclAssocDB, orclAssocIasInstance, orclEnabled, orclFlexAttribute1, orclIsEnabled, orclMasterNode, orclNetDescName, orclNetDescString, orclOracleHome, orclServiceInstanceLocation, orclServiceMember, orclServiceSubscriptionLocation, orclServiceSubType, orclServiceType, orclSID, orclSuiteType, orclSystemName, orclVersion

Object Classes

orclService, orclServiceInstance, orclServiceInstanceReference, orclServiceRecipient, orclServiceSuite, orclServiceSubscriptionDetail

Garbage Collection

This section lists the attributes and object classes that pertain to the configuration of garbage collection.

Attributes

orclPurgeBase, orclPurgeDebug, orclPurgeEnable, orclPurgeFileLoc, orclPurgeFileName, orclPurgeFilter, orclPurgeInterval, orclPurgeNow, orclPurgePackage, orclPurgeStart, orclPurgeTargetAge, orclPurgeTranSize

Object Classes

orclPurgeConfig, tombstone

Attribute Uniqueness

This section lists the attributes and object classes that pertain to the configuration of attribute uniqueness.

Attributes

orclUniqueAttrName, orclUniqueEnable, orclUniqueObjectClass, orclUniqueScope, orclUniqueSubtree

Object Classes

orclUniqueConfig

Audit and Error Logging Schema Elements

This section lists the attributes and object classes that pertain to audit logs and error logs.

Attributes

orclAuditAttribute, orclAuditMessage, orclDBConnCreationFailed, orclDNSUnavailable, orclEventTime, orclEventType, orclFDIncreaseError, orclMaxFDLimitReached, orclMaxProcessLimitReached, orclMemAllocError, orclNWCongested, orclNwUnavailable, orclOpResult, orclORA28error, orclORA3113error, orclORA3114error, orclSequence, orclThreadSpawnFailed, orclUserDN

Object Classes

orclAuditOC, orclEventLog, orclEvents, orclSysResourceEvents

Server Manageability Schema Elements

This section lists the schema elements for Oracle Internet Directory server manageability statistics.

Attributes

orclACLResultsLatency, orclActiveConn, orclActiveThreads, orclAttrACLEvalLatency, orclAuditMessage, orclBERgenLatency, orclDBLatency, orclDIMEonlyLatency, orclEcacheHitRatio, orclEcacheNumEntries, orclEcacheSize, orclEntryACLEvalLatency, orclEventTime, orclEventType, orclFilterACLEvalLatency, orclFrontLatency, orclGenObjLatency, orclGetNearACLLatency, orclHostname, orclIdleConn, orclIdleThreads, orclInitialServerMemSize, orclIpAddress, orclLDAPInstanceID, orclLDAPProcessID, orclOpAbandoned, orclOpCompleted, orclOpenConn, orclOpFailed, orclOpInitiated, orclOpLatency, orclOpPending, orclOpResult, orclOpSucceeded, orclOpTimedOut, orclQueueDepth, orclQueueLatency, orclReadWaitThreads, orclSequence, orclServerAvgMemGrowth, orclSMSpec, orclSQLexeFetchLatency, orclSQLGenReusedParsed, orclTcpConnToClose, orclTcpConnToShutDown, orclTotFreePhyMem, orclTraceDimesionLevel, orclTraceFileLocation, orclTraceFileSize, orclTraceLevel, orclTraceMode, orclUserDN, orclWriteWaitThreads

Object Classes

orclGeneralStats, orclHealthStats, orclPerfStats, orclSecRefreshEvents, orclSM, orclTraceConfig, orclUserStats

Oracle Directory Replication Schema Elements

This section lists the schema elements for directory replication.

Attributes

orclAgreementId, orclChangeLogLife, orclChangeRetryCount, orclConfigSetNumber, orclDirReplGroupAgreement, orclDirReplGroupDSAs, orclExcludedAttributes, orclExcludedNamingContexts, orclHIQSchedule, orclHostname, orclIncludedNamingContexts, orclLastAppliedChangeNumber, orclLDAPConnKeepALive, orclPilotMode, orclPurgeSchedule, orclReplicaDN, orclReplicaID, orclReplicaSecondaryURI, orclReplicaState, orclReplicationProtocol, orclReplicaType, orclReplicaURI, orclReplicaVersion, orclThreadsPerSupplier, orclUpdateSchedule, pilotStartTime

Object Classes

orclReplAgreementEntry, orclReplInstance, orclReplicaSubentry, orclReplNameCtxConfig, orclReplSubConfig

Oracle Directory Integration Platform Schema Elements

This section lists the schema elements for Oracle Directory Integration Platform. It contains the following topics:

- Applications
- Change Logs
- Events and Objects
- Plug-ins and Interfaces
- Server Configuration
- Profiles
- Schema
- Active Directory Users

Applications

This section lists the attributes and object classes for Oracle Directory Integration Platform applications.

Attributes

orclApplicationType, orclInterval, orclODIPAgent, orclODIPApplicationName, orclODIPCommand, orclODIPDbConnectInfo, orclODIPEventSubscriptions, orclOwnerGUID, orclStatus, orclVersion

Object Classes

orclODIPApplicationCommonConfig, orclODIPAppSubscription

Change Logs

This section lists the attributes and object classes for Oracle Directory Integration Platform change logs.

Attributes

orclLastAppliedChangeNumber, orclSubscriberDisable, serverName, userPassword

Object Classes

orclChangeSubscriber

Events and Objects

This section lists the attributes and object classes for Oracle Directory Integration Platform events and objects.

Attributes

orclODIPAttributeMappingRules, orclODIPEventFilter, orclODIPFilterAttrCriteria, orclODIPMustAttrCriteria, orclODIPObjectCriteria, orclODIPObjectEvents, orclODIPObjectName, orclODIPObjectSyncBase, orclODIPOperationMode, orclODIPOptAttrCriteria, orclODIPProvEventCriteria,

orclODIPProvEventLDAPChangeType, orclODIPProvEventObjectType, orclODIPProvEventRule, orclODIPProvEventRuleDTD, orclStatus

Object Classes

orclODIPEventContainer, orclODIPObject, orclODIPProvEventDefn, orclODIPProvEventTypeConfig

Plug-ins and Interfaces

This section lists the attributes and object classes for Oracle Directory Integration Platform plug-ins and interfaces.

Attributes

orclODIPPluginAddInfo, orclODIPPluginConfigInfo, orclODIPPluginEvents, orclODIPPluginExecData, orclODIPPluginExecName, orclODIPProfileProvSubscriptionMode, orclODIPProfileStatusUpdate, orclODIPProvInterfaceFilter, orclODIPProfileInterfaceType, orclODIPProvInterfaceProcessor, orclStatus

Object Classes

orclODIPProvInterfaceDetails, orclODIPPlugin, orclODIPPluginContainer

Server Configuration

This section lists the attributes and object classes for configuring the Oracle Directory Integration Platform server.

Attributes

cn, orclConfigSetNumber, orclHostname, orclODIPConfigDNs, orclODIPConfigRefreshFlag, orclODIPInstanceStatus, orclODIPProfileExecGroupID, orclODIPSearchCountLimit, orclODIPSearchTimeLimit, orclODIPServerCommitSize, orclODIPServerDebugLevel, orclODIPServerRefreshIntvl, orclODIPServerSSLMode, orclODIPServerWalletLoc, orclSSLEnable, orclVersion, seeAlso, userPassword

Object Classes

orclODIPServerConfig, orclODISConfig, orclODIServer, orclODISInstance

Profiles

This section the attributes and object classes for Oracle Directory Integration Platform synchronization and provisioning profiles.

Attributes

cn, orclODIPAgentConfigInfo, orclODIPAgentControl, orclODIPAgentExeCommand, orclODIPAgentHostName, orclODIPAgentName, orclODIPAgentPassword, orclODIPAttributeMappingRules, orclODIPBootStrapStatus, orclODIPConDirAccessAccount, orclODIPConDirAccessPassword, orclODIPConDirLastAppliedChgNum, orclODIPConDirMatchingFilter, orclODIPConDirURL, orclODIPEncryptedAttrKey, orclODIPInterfaceType, orclODIPLastExecutionTime, orclODIPLastSuccessfulExecutionTime, orclODIPOIDMatchingFilter, orclODIPProfileDebugLevel, orclODIPProfileExecGroupID, orclODIPProfileInterfaceAdditionalInformation, orclODIPProfileInterfaceConnectInformation, orclODIPProfileInterfaceName, orclODIPProfileInterfaceType, orclODIPProfileInterfaceVersion, orclODIPProfileLastAppliedAppEventID, orclODIPProfileLastProcessingTime,

orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileMaxErrors, orclODIPProfileMaxEventsPerInvocation, orclODIPProfileMaxEventsPerSchedule, orclODIPProfileMaxRetries, orclODIPProfileName, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclODIPProfileSchedule, orclODIPProvisioningAppGUID, orclODIPProvisioningAppName, orclODIPProvisioningEventMappingRules, orclODIPProvisioningEventPermittedOperations, orclODIPProvisioningEventSubscription, orclODIPProvisioningOrgGUID, orclODIPProvisioningOrgName, orclODIPSchedulingInterval, orclODIPSynchronizationErrors, orclODIPSynchronizationMode, orclODIPSynchronizationStatus, orclODIPSyncRetryCount, orclPasswordAttribute, orclStatus, orclVersion, userPassword

Object Classes

orclODIPIntegrationProfile, orclODIProfile, orclODIPProvisioningIntegrationProfile, orclODIPProvisioningIntegrationProfileV2, orclODIPProvisioningIntegrationOutBoundProfile, orclODIPProvisioningIntegrationOutBoundProfileV2

Schema

This section lists the attributes and object classes for Oracle Directory Integration Platform schema information.

Attributes

orclODIPApplicationsLocation, orclODIPInstancesLocation, orclODIPObjectDefnLocation, orclODIPProvProfileLocation, orclODIPRootLocation, orclODIPSchemaVersion, orclODIPServerConfigLocation, orclODIPSyncProfileLocation

Object Classes

orclODIPSchemaDetails

Active Directory Users

The following attributes and object classes are used for users that are imported into Oracle Internet Directory from Microsoft Active Directory using Oracle Directory Integration Platform.

Attributes

orclObjectGUID, orclObjectSID, orclSAMAccountName, orclUserPrincipalName

Object Classes

orclADGroup, orclADUser, orclNTUser

Oracle Delegated Administration Services Schema Elements

This section lists the attributes and object classes for Oracle Delegated Administration Services.

Attributes

orclDASAdminModifiable, orclDASAttrDispOrder, orclDASAttrName, orclDASEnableProductLogo, orclDASEnableSubscriberLogo, orclDASIsEnabled, orclDASIsMandatory, orclDASIsPersonal, orclDASLOV, orclDASPublicGroupDNs,

orclDASSearchable, orclDASSearchColIndex, orclDASSearchFilter, orclDASSearchSizeLimit, orclDASSelfModifiable, orclDASUIType, orclDASURL, orclDASURLBase, orclDASValidatePwdReset, orclDASViewable

Object Classes

orclDASAppContainer, orclDASAttrCategory, orclDASConfigAttr, orclDASConfigPublicGroup, orclDASLOVVal, orclDASOperationURL, orclDASSubscriberContainer

Oracle Application Server Certificate Authority and PKI Schema Elements

This section lists the attributes and object classes that pertain to public key infrastructure (PKI), certificates, and Oracle Application Server Certificate Authority.

Attributes

orclCertExtensionAttribute, orclCertExtensionOID, orclCertificateHash, orclCertificateMatch, orclCertMappingAttribute, orclPKINextUpdate, orclPKIValMecAttr, x509issuer

Object Classes

orclCertIdMapping, orclPKICRL, orclPKIValMecCl

Application Schema Elements

This section lists the attributes and object classes that pertain to applications.

Attributes

authPassword, description, labeledURI, orclAppFullName, orclApplicationCommonName, orclCategory, orclDBSchemaIdentifier, orclOwnerGUID, orclPasswordVerifier, orclResourceIdentifier, orclTrustedApplicationGroup, orclVersion, protocolInformation, seeAlso, userCertificate;binary, userPassword, userPKCS12

Object Classes

orclApplicationEntity, orclAppSpecificUserInfo, orclAppUserEntry

Resource Schema Elements

This section lists the attributes and object classes that pertain to resources.

Attributes

description, displayName, javaClassName, orclConnectionFormat, orclFlexAttribute1, orclFlexAttribute2, orclFlexAttribute3, orclOwnerGUID, orclPasswordAttribute, orclResourceName, orclResourceTypeName, orclResourceViewers, orclUserIDAttribute, orclUserModifiable

Object Classes

orclResourceDescriptor, orclResourceType

Plug-in Schema Elements

This section lists the attributes and object classes for configuring Plug-ins for Oracle Internet Directory.

Attributes

orclPluginAttributeList, orclPluginCheckEntryExist, orclPluginEnable, orclPluginEntryProperties, orclPluginIsReplace, orclPluginKind, orclPluginLDAPOperation, orclPluginName, orclPluginPort, orclPluginRequestGroup, orclPluginRequestNegGroup, orclPluginResultCode, orclPluginSASLCallBack, orclPluginSearchNotFound, orclPluginShareLibLocation, orclPluginSubscriberDNList, orclPluginTiming, orclPluginType, orclPluginVersion, userPassword

Object Classes

orclPluginConfig, orclPluginContainer, orclPluginUser

Directory User Agents Schema Elements

This section lists the attributes and object classes for configuring directory user agents (DUAs).

Attributes

attributeMap, authenticationMethod, bindTimeLimit, cn, credentialLevel, defaultSearchBase, defaultSearchScope, defaultServerList, followReferrals, objectClass, objectClassMap, preferredServerList, profileTTL, searchTimeLimit, serviceAuthenticationMethod, serviceCredentialLevel, serviceSearchDescriptor

Object Classes

duaConfigProfile

User, Group, and Subscriber Schema Elements

This section lists the attributes and object classes used for users, groups, and subscribers. It contains the following topics:

- Groups
- Dynamic Groups
- Users

Groups

Oracle Internet Directory uses the standard object classes `groupOfNames` and `groupOfUniqueNames` as defined in RFC 2256. In addition to the standard attributes and object classes, the following are also used for groups.

Attributes

displayName, mail, orclGlobalID, orclIsVisible

Object Classes

orclGroup

Dynamic Groups

This section lists the attributes and object classes for dynamic groups.

Attributes

labeledURI, mail, orclConnectByAttribute, orclConnectBySearchBase, orclConnectByStartingValue

Object Classes

orclDynamicGroup

Users

Oracle Internet Directory uses the standard object classes `person` and `inetOrgPerson` as defined in RFC 2256. In addition to the standard attributes and object classes, the following are also used for users.

Attributes

authPassword, c, jpegPhoto, krbPrincipalName, middleName, orclActiveEndDate, orclActiveStartdate, orclContact, orclDateOfBirth, orclDefaultProfileGroup, orclDisplayPersonalInfo, orclGender, orclHireDate, orclHostedCreditCardExpireDate, orclHostedCreditCardNumber, orclHostedCreditCardType, orclHostedDunsNumber, orclHostedPaymentTerm, orclIsEnabled, orclIsVisible, orclMaidenName, orclPassword, orclPasswordHint, orclPasswordHintAnswer, orclPasswordVerifier, orclPKCS12Hint, orclSAMAccountName, orclSearchFilter, orclSubscriberFullName, orclSubscriberType, orclTimeZone, orclUIAccessibilityMode, orclVersion, orclWirelessAccountNumber, orclWorkflowNotificationPref, userPKCS12

Object Classes

orclSubscriber, orclUserV2

Password Policy Schema Elements

This section lists the attributes and object classes that pertain to password policy configuration.

Attributes

cn, displayName, orclPwdAllowHashCompare, orclPwdAlphaNumeric, orclPwdEncryptionEnable, orclPwdIllegalValues, orclPwdIPLockout, orclPwdIPLockoutDuration, orclPwdIPMaxFailure, orclPwdPolicyEnable, pwdAllowUserChange, pwdCheckSyntax, pwdExpireWarning, pwdFailureCountInterval, pwdGraceLoginLimit, pwdInHistory, pwdLockout, pwdLockoutDuration, pwdMaxAge, pwdMaxFailure, pwdMinAge, pwdMinLength, pwdMustChange, pwdSafeModify

Object Classes

pwdpolicy

Password Verifier Schema Elements

This section lists the attributes and object classes that pertain to password verifiers.

Attributes

cn, displayName, orclAppId, orclPwdVerifierParams, owner

Object Classes

orclPwdVerifierProfile

8

Object Class Reference

This chapter contains reference information about the object classes used for Oracle Identity Management. It contains the following topics:

- Standard LDAP Object Classes
- Oracle Identity Management Object Class Reference

For a list of object classes grouped by functional categories, see "Overview of Oracle Identity Management Schema Elements" on page 7-8.

Standard LDAP Object Classes

Oracle Internet Directory supports the following standard LDAP object classes as defined in the Internet Engineering Task Force (IETF) Requests for Comments (RFC) specifications.

Details of RFC specifications can be found on the IETF Web site at: `http://www.ietf.org`.

Table 8–1 Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
accessControlSubentry	RFC 1274
account	RFC 1274
alias	RFC 2256
applicationEntity	RFC 2256
applicationProcess	RFC 2256
bootableDevice	RFC 2307
certificationAuthority	RFC 2256
certificationAuthority-V2	RFC 2256
collectiveAttributeSubentry	RFC 3671
country	RFC 2256
crlDistributionPoint	RFC 2256
device	RFC 2256
dmd	RFC 2256
dnsDomain	RFC 1274
documentSeries	RFC 1274

Table 8–1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
domain	RFC 1274
domainRelatedObject	RFC 1274
dsa	RFC 1274
extensibleObject	RFC 2252
friendlyCountry	RFC 1274
groupOfNames	RFC 2256
groupOfUniqueNames	RFC 2256
ieee802Device	RFC 2307
inetOrgPerson	RFC 2798
ipHost	RFC 2307
ipNetwork	RFC 2307
ipProtocol	RFC 2307
ipService	RFC 2307
javaContainer	RFC 2713
javaMarshalledObject	RFC 2713
javaNamingReference	RFC 2713
javaObject	RFC 2713
javaSerializedObject	RFC 2713
labeledURIObject	RFC 2079
locality	RFC 2256
mailRecipient	RFC 2256
newPilotPerson	RFC 2377
nisDomainObject	RFC 2307
nisKeyObject	RFC 2307
nisMap	RFC 2307
nisNetgroup	RFC 2307
nisObject	RFC 2307
oldQualityLabelledData	RFC 2307
oncRpc	RFC 2307
organization	RFC 2256
organizationalPerson	RFC 2256
organizationalRole	RFC 2256
organizationalUnit	RFC 2256
person	RFC 2256
pilotDSA	RFC 2256
pilotObject	RFC 2256
pilotOrganization	RFC 2256

Table 8–1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
posixAccount	RFC 2307
posixGroup	RFC 2307
referral	RFC 3296
residentialPerson	RFC 2256
room	RFC 1274
shadowAccount	RFC 2307
simpleSecurityObject	RFC 1274
strongAuthenticationUser	RFC 2256

Oracle Identity Management Object Class Reference

This section contains an alphabetical listing of the Oracle Identity Management object classes. These are the object classes used to create entries pertaining to Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, OracleAS Single Sign-On, and Oracle Application Server Certificate Authority. For more information about an attribute or the superior of an object class, click the link of the attribute name or superior object class name.

duaConfigProfile

Description

Configuration profile for a directory user agent (DUA). A DUA is software that accesses the LDAP directory service on behalf of the directory user. The directory user may be a person or another software element.

Object ID

1.3.6.1.4.1.11.1.3.1.2.4

Superior Object Class

top

Object Class Type

88

Required Attributes

cn, objectClass

Allowed Attributes

attributeMap, authenticationMethod, bindTimeLimit, credentialLevel, defaultSearchBase, defaultSearchScope, defaultServerList, followReferrals, objectClassMap, preferredServerList, profileTTL, searchTimeLimit , serviceAuthenticationMethod, serviceCredentialLevel, serviceSearchDescriptor

orclADGroup

Description
Contains Microsoft Active Directory group attributes, which are used to synchronize Active Directory group objects with Oracle Internet Directory group objects in an Oracle Directory Integration Platform environment.

Object ID
2.16.840.1.113894.8.2.899

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclSAMAccountName

Allowed Attributes
displayName, orclObjectGUID, orclObjectSID

orclADUser

Description
Contains Microsoft Active Directory user attributes, which are used to synchronize Active Directory user objects with Oracle Internet Directory user objects in an Oracle Directory Integration Platform environment.

Object ID
2.16.840.1.113894.8.2.900

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclSAMAccountName

Allowed Attributes
displayName, orclObjectGUID, orclObjectSID, orclUserPrincipalName

orclApplicationEntity

Description
Defines an application entity.

Object ID
2.16.840.1.113894.1.2.55

Superior Object Class
top

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
authPassword, description, labeledURI, orclAppFullName, orclApplicationCommonName, orclCategory, orclDBSchemaIdentifier, orclPasswordVerifier, orclResourceIdentifier, orclTrustedApplicationGroup, orclVersion, protocolInformation, seeAlso, userCertificate;binary, userPassword, userPKCS12

orclAppSpecificUserInfo

Description
An auxiliary object class for an application entity that defines user information.

Object ID
2.16.840.1.13894.8.2.420

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
orclOwnerGUID

Allowed Attributes
N/A

orclAppUserEntry

Description
The user associated with an application entity.

Object ID
2.16.840.1.13894.8.2.423

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclOwnerGUID

Allowed Attributes
N/A

orclAuditOC

Description
Generic audit log attributes that can be used in a server audit log entry.

Object ID
2.16.840.1.113894.1.2.18

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclAuditMessage, orclEventTime, orclEventType, orclSequence

Allowed Attributes
orclAuditAttribute, orclOpResult, orclUserDN

orclCertIdMapping

Description
Oracle Internet Directory public key infrastructure (PKI) structural object class for mapping attributes in a client certificate to entries in Oracle Internet Directory.

Object ID
2.16.840.1.113894.1.2.130

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes

description, orclCertExtensionAttribute, orclCertExtensionOID, orclCertMappingAttribute

orclChangeSubscriber

Description

Status information for an Oracle Directory Integration Platform change subscriber event.

Object ID

2.16.840.1.113894.1.2.21

Superior Object Class

top

Object Class Type

Structural

Required Attributes

orclLastAppliedChangeNumber, orclSubscriberDisable

Allowed Attributes

cn, serverName, userPassword

orclCommonAttributes

Description

Oracle Context configuration attributes.

Object ID

2.16.840.1.113894.7.2.1004

Superior Object Class

orclContainer

Object Class Type

Structural

Required Attributes

N/A

Allowed Attributes

orclCommonAutoRegEnabled, orclCommonContextMap, orclCommonDefaultUserCreateBase, orclCommonGroupCreateBase, orclCommonNamingAttribute, orclCommonNicknameAttribute, orclCommonSASLRealm, orclCommonUserSearchBase, orclVersion

orclCommonAttributesV2

Description
Oracle Context configuration attributes.

Object ID
2.16.840.1.113894.1.2.51

Superior Object Class
top

Object Class Type
88

Required Attributes
N/A

Allowed Attributes
orclDefaultSubscriber, orclSubscriberNickNameAttribute, orclSubscriberSearchBase, orclUserObjectClasses

orclConfigSet

Description
Configuration set entry for a server instance.

Object ID
2.16.840.1.113894.1.2.2

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
description, seeAlso

orclContainer

Description
Container object for an Oracle Context.

Object ID
2.16.840.1.113894.7.2.2

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclVersion, orclServiceType

orclDASAppContainer

Description
Container object for a Oracle Delegated Administration Services application.

Object ID
2.16.840.1.113894.1.2.61

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclDASURLBase

orclDASAttrCategory

Description
Oracle Delegated Administration Services attribute categories.

Object ID
2.16.840.1.113894.1.2.59

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
cn, displayName, orclDASAttrDispOrder, orclDASAttrName

orclDASConfigAttr

Description
Oracle Delegated Administration Services configuration attributes.

Object ID
2.16.840.1.113894.1.2.56

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
displayName, orclDASAdminModifiable, orclDASIsMandatory, orclDASIsPersonal, orclDASLOV, orclDASSearchable , orclDASSearchColIndex, orclDASSearchFilter, orclDASSelfModifiable, orclDASUIType, orclDASValidatePwdReset, orclDASViewable

orclDASConfigPublicGroup

Description
Oracle Delegated Administration Services public group configuration attributes.

Object ID
2.16.840.1.113894.1.2.60

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
cn

Allowed Attributes
orclDASIsEnabled, orclDASPublicGroupDNs

orclDASLOVVal

Description
Oracle Delegated Administration Services list of values.

Object ID
2.16.840.1.113894.1.1.919

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, displayName

Allowed Attributes
N/A

orclDASOperationURL

Description
Oracle Delegated Administration Services URL.

Object ID
2.16.840.1.113894.1.2.54

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
cn, description, orclDASURL

orclDASSubscriberContainer

Description
Oracle Delegated Administration Services subscriber container object.

Object ID
2.16.840.1.113894.1.2.66

Superior Object Class
N/A

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
orclDASEnableProductLogo, orclDASEnableSubscriberLogo, orclDASSearchSizeLimit

orclIDMapping

Description
Auxilliary object class defining the attributes that hold information about directory operations to be performed for mapping.

Object ID
2.16.840.1.113894.1.2.131

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclMappedDN, orclSearchBaseDN, orclSearchFilter, orclSearchScope

orclDSAConfig

Description
Configuration attributes for Oracle Internet Directory server.

Object ID
2.16.840.1.113894.1.2.70

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclAnonymousBindsFlag, orclAuditLevel, orclCatalogEntryDN, orclCryptoScheme, orclDebugFlag, orclDebugForceFlush, orclDebugOp, orclDIPRepository, orclEcacheEnabled, orclEcacheMaxEntries, orclEcacheMaxEntSize, orclEcacheMaxSize, orclEnableGroupCache, orclGUName, orclGUPassword, orclIndexHints,

orclIpAddress, orclLDAPConnTimeout, orclMatchDnEnabled, orclMaxEntInBER , orclMaxConnInCache, orclNwrwTimeout, orclPKIMatchingRule, orclPrName, orclPrPassword, orclReplAgreements, orclReplicaID, orclsDumpFlag, orclServerMode, orclSizeLimit, orclSkewedAttribute, orclSkipRefInSQL, orclStatsDN, orclStatsFlag, orclStatsLevel, orclStatsOp, orclStatsPeriodicity, orclSUAccountLocked, orclSULoginFailureCount, orclSUName, orclSUPassword, orclTimeLimit, orclTLimitMode, orclUpgradeInProgress

orclDynamicGroup

Description

Attributes that are used to create dynamic groups. A dynamic group is one whose membership, rather than being maintained in a list, is computed on the fly, based on rules and assertions you specify.

Object ID

2.16.840.1.113894.1.2.190

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

labeledURI, mail, orclConnectByAttribute , orclConnectBySearchBase, orclConnectByStartingValue

orclEventLog

Description

Object class used for audit logging of server events.

Object ID

2.16.840.1.113894.1.2.17

Superior Object Class

top

Object Class Type

Structural

Required Attributes

cn

Allowed Attributes

orclEvents

Description
Object class used for audit logging of events.

Object ID
2.16.840.1.113894.1.2.19

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclEventType

orclGeneralStats

Description
Statistical information for Oracle Internet Directory server operations.

Object ID
2.16.840.1.113894.1.2.30

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclOpAbandoned, orclOpCompleted, orclOpInitiated, orclOpPending, orclOpTimedOut, orclQueueDepth

orclGroup

Description
Additional optional attributes for a group.

Object ID
2.16.840.1.113894.1.2.53

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
displayName, mail, orclGlobalID, orclIsVisible

orclHealthStats

Description
Statistical information for Oracle Internet Directory server performance.

Object ID
2.16.840.1.113894.1.2.27

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclActiveThreads, orclEcacheHitRatio, orclEcacheNumEntries, orclEcacheSize, orclIdleConn, orclIdleThreads, orclInitialServerMemSize, orclOpenConn, orclQueueDepth, orclQueueLatency , orclReadWaitThreads, orclServerAvgMemGrowth, orclTcpConnToClose, orclTcpConnToShutDown, orclTotFreePhyMem, orclWriteWaitThreads

orclIndexOC

Description
Configuration of the indexed attributes for the Oracle Internet Directory server.

Object ID
2.16.840.1.113894.1.2.15

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclIndexedAttribute

orclLDAPInstance

Description
Configuration attributes for an Oracle Internet Directory server instance.

Object ID
2.16.840.1.113894.1.2.13

Superior Object Class
top, orclLDAPSubConfig

Object Class Type
Structural

Required Attributes
cn, orclConfigSetNumber, orclHostname

Allowed Attributes
description, seeAlso

orclLDAPSubConfig

Description
Configuration attributes for Oracle Internet Directory server.

Object ID
2.16.840.1.113894.1.2.3

Superior Object Class
top, orclConfigSet

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclMaxCC, orclNonSSLPort, orclSASLAuthenticationMode, orclSASLCipherChoice, orclSASLMechanism, orclServerProcs, orclSSLAuthentication, orclSSLCipherSuite, orclSSLEnable, orclSSLPort , orclSSLVersion, orclSSLWalletURL

orclNTUser

Description
Contains Microsoft NT user attributes, which are used to synchronize NT user objects with Oracle Internet Directory user objects in an Oracle Directory Integration Platform environment.

Object ID
2.16.840.1.113894.8.2.898

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclSAMAccountName

Allowed Attributes
displayName, orclObjectGUID, orclObjectSID

orclODIPApplicationCommonConfig

Description
Oracle Directory Integration Platform configuration attributes.

Object ID
2.16.840.1.13894.8.2.421

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclApplicationType

orclODIPAppSubscription

Description
Application subscription attributes for Oracle Directory Integration Platform.

Object ID
2.16.840.1.113894.9.2.1

Superior Object Class
top

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
orclInterval, orclODIPAgent, orclODIPApplicationName, orclODIPCommand, orclODIPDbConnectInfo, orclODIPEventSubscriptions, orclOwnerGUID, orclStatus, orclVersion

orclODIPEventContainer

Description
Container object for an Oracle Directory Integration Platform event.

Object ID
2.16.840.1.113894.8.2.414

Superior Object Class
N/A

Object Class Type
88

Required Attributes
cn

Allowed Attributes
orclODIPAttributeMappingRules, orclODIPEventFilter, orclODIPOperationMode, orclODIPProvEventRule, orclStatus

orclODIPIntegrationProfile

Description
Oracle Directory Integration Platform integration profiles for integrating with third-party directories.

Object ID
2.16.840.1.113894.8.2.200

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclODIPProfileName, orclVersion

Allowed Attributes
orclODIPEncryptedAttrKey, orclODIPProfileDebugLevel, orclODIPProfileExecGroupID, orclODIPProfileInterfaceAdditionalInformation, orclODIPProfileInterfaceConnectInformation, orclODIPProfileInterfaceName, orclODIPProfileInterfaceType, orclODIPProfileInterfaceVersion, orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileMaxErrors, orclODIPProfileMaxEventsPerInvocation, orclODIPProfileMaxEventsPerSchedule, orclODIPProfileMaxRetries, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclODIPProfileSchedule, orclPasswordAttribute, orclStatus, userPassword

orclODIPObject

Description
Attributes to identify Oracle Directory Integration Platform objects.

Object ID
2.16.840.1.113894.8.2.431

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
orclODIPObjectCriteria, orclODIPObjectName

Allowed Attributes
orclODIPFilterAttrCriteria, orclODIPMustAttrCriteria, orclODIPOptAttrCriteria

orclODIPPlugin

Description
Configuration attributes for Oracle Directory Integration Platform plug-ins.

Object ID
2.16.840.1.113894.8.2.412

Superior Object Class
N/A

Object Class Type
Structural

Required Attributes
cn, orclODIPPluginEvents, orclODIPPluginExecName

Allowed Attributes
description, orclODIPPluginAddInfo, orclStatus

orclODIPPluginContainer

Description
Configuration attributes for Oracle Directory Integration Platform plug-ins.

Object ID
2.16.840.1.113894.8.2.411

Superior Object Class
N/A

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
description, orclODIPPluginConfigInfo, orclODIPPluginExecData

orclODIPProvEventDefn

Description
Defines a provisioning event.

Object ID
2.16.840.1.113894.8.2.413

Superior Object Class
N/A

Object Class Type
88

Required Attributes
N/A

Allowed Attributes
cn, orclODIPEventFilter, orclODIPObjectEvents, orclODIPObjectName, orclODIPObjectSyncBase, orclODIPProvEventRule, orclStatus

orclODIPProvEventTypeConfig

Description
Configuration attributes for a provisioning event type.

Object ID
2.16.840.1.113894.8.2.500

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclODIPProvEventObjectType

Allowed Attributes
orclODIPProvEventCriteria, orclODIPProvEventLDAPChangeType

orclODIPProvInterfaceDetails

Description
Provisioning interface details.

Object ID
2.16.840.1.113894.8.2.16

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
orclODIPProfileInterfaceType, orclODIPProfileProvSubscriptionMode

Allowed Attributes
orclODIPProfileStatusUpdate, orclODIPProvInterfaceFilter, orclODIPProvInterfaceProcessor

orclODIPProvisioningIntegrationInBoundProfileV2

Description
Configuration for an Oracle Directory Integration Platform profile for imports from third-party directories.

Object ID
2.16.840.1.113894.8.2.402

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclODIPProfileLastAppliedAppEventID, orclODIPProvisioningAppGUID, orclODIPProvisioningEventMappingRules, orclODIPProvisioningEventPermittedOperations

Allowed Attributes
orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclStatus

orclODIPProvisioningIntegrationOutBoundProfile

Description
Configuration for an Oracle Directory Integration Platform profile for exports to third-party directories. This object class is used for profiles created prior to release 10*g*.

Object ID
2.16.840.1.113894.8.2.404

Superior Object Class
top, orclChangeSubscriber

Object Class Type
Structural

Required Attributes
cn, orclODIPProvisioningAppGUID, orclODIPProvisioningEventSubscription

Allowed Attributes
orclODIPProfileProvSubscriptionMode, orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclStatus, orclVersion

orclODIPProvisioningIntegrationOutBoundProfileV2

Description
Configuration for an Oracle Directory Integration Platform profile for exports to third-party directories.

Object ID
2.16.840.1.113894.8.2.403

Superior Object Class
top, orclChangeSubscriber

Object Class Type
Structural

Required Attributes

cn, orclODIPProvisioningAppGUID, orclODIPProvisioningEventSubscription

Allowed Attributes

orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclStatus

orclODIPProvisioningIntegrationProfile

Description

Configuration for an Oracle Directory Integration Platform profile for integration with third-party directories. This object class is used for profiles created in releases prior to 10*g*.

Object ID

2.16.840.1.113894.8.2.400

Superior Object Class

top, orclODIPIntegrationProfile, orclChangeSubscriber

Object Class Type

Structural

Required Attributes

orclODIPProvisioningAppName, orclODIPProvisioningAppGUID, orclODIPProvisioningOrgName, orclODIPProvisioningOrgGUID, orclODIPProvisioningEventSubscription

Allowed Attributes

N/A

orclODIPProvisioningIntegrationProfileV2

Description

Configuration for an Oracle Directory Integration Platform profile for integration with third-party directories.

Object ID

2.16.840.1.113894.8.2.401

Superior Object Class

top, orclODIPIntegrationProfile

Object Class Type

Structural

Required Attributes

orclODIPProvisioningAppGUID, orclODIPProvisioningAppName, orclODIPProvisioningOrgGUID, orclODIPProvisioningOrgName

Allowed Attributes
N/A

orclODIProfile

Description
Profile for Oracle Directory Integration Platform server

Object ID
2.16.840.1.113894.8.2.1

Superior Object Class
top

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
orclODIPAgentConfigInfo, orclODIPAgentControl, orclODIPAgentExeCommand, orclODIPAgentHostName, orclODIPAgentName, orclODIPAgentPassword, orclODIPAttributeMappingRules, orclODIPBootStrapStatus, orclODIPConDirAccessAccount, orclODIPConDirAccessPassword, orclODIPConDirLastAppliedChgNum, orclODIPConDirMatchingFilter, orclODIPConDirURL, orclODIPInterfaceType, orclODIPLastExecutionTime, orclODIPLastSuccessfulExecutionTime, orclODIPOIDMatchingFilter, orclODIPProfileDebugLevel, orclODIPSchedulingInterval, orclODIPSynchronizationErrors, orclODIPSynchronizationMode, orclODIPSynchronizationStatus, orclODIPSyncRetryCount, orclVersion, userPassword

orclODIPSchemaDetails

Description
Oracle Directory Integration Platform DIT configuration.

Object ID
2.16.840.1.113894.8.2.11

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes

cn, orclODIPApplicationsLocation, orclODIPInstancesLocation, orclODIPObjectDefnLocation , orclODIPProfileDataLocation , orclODIPProvProfileLocation, orclODIPRootLocation, orclODIPSchemaVersion, orclODIPServerConfigLocation, orclODIPSyncProfileLocation

orclODIPServerConfig

Description

Configuration attributes for the Oracle Directory Integration Platform server.

Object ID

2.16.840.1.113894.8.2.501

Superior Object Class

top

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

cn, orclODIPSearchCountLimit, orclODIPSearchTimeLimit, orclODIPServerCommitSize, orclODIPServerDebugLevel, orclODIPServerRefreshIntvl, orclODIPServerSSLMode, orclODIPServerWalletLoc

orclODISConfig

Description

Configuration attributes for the Oracle Directory Integration Platform server.

Object ID

2.16.840.1.113894.8.2.3

Superior Object Class

top

Object Class Type

Structural

Required Attributes

cn

Allowed Attributes

orclODIPConfigDNs, orclODIPConfigRefreshFlag

orclODIServer

Description
Configuration attributes for the Oracle Directory Integration Platform server.

Object ID
2.16.840.1.113894.8.2.2

Superior Object Class
top

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
cn, orclHostname, orclVersion, userPassword

orclODISInstance

Description
Configuration attributes for the Oracle Directory Integration Platform server instance.

Object ID
2.16.840.1.113894.8.2.4

Superior Object Class
top, orclODISConfig

Object Class Type
Structural

Required Attributes
cn, orclconfigsetnumber, orclhostname

Allowed Attributes
description, orclODIPInstanceStatus, orclODIPProfileExecGroupID, orclSSLEnable, seeAlso

orclPerfStats

Description
Oracle Internet Directory Server Manageability performance statistics.

Object ID
2.16.840.1.113894.1.2.26

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclACLResultsLatency, orclAttrACLEvalLatency, orclBERgenLatency, orclDBLatency, orclDIMEonlyLatency, orclEntryACLEvalLatency, orclFilterACLEvalLatency, orclFrontLatency, orclGenObjLatency, orclGetNearACLLatency, orclOpLatency, orclSQLexeFetchLatency, orclSQLGenReusedParsed

orclPKICRL

Description
Oracle Application Server Certificate Authority certificate revocation list (CRL).

Object ID
2.16.840.1.113894.2.2.300.1

Superior Object Class
crlDistributionPoint (RFC 2256)

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclPKINextUpdate, x509issuer

orclPKIValMecCl

Description
Used by Oracle Application Server Certificate Authority.

Object ID
2.16.840.1.113894.2.2.300.2

Superior Object Class
orclContainer

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclPKIValMecAttr

orclPluginConfig

Description
Configuration attributes for Oracle Internet Directory plug-ins.

Object ID
2.16.840.1.113894.1.2.90

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclPluginLDAPOperation, orclPluginName, orclPluginType

Allowed Attributes
orclPluginAttributeList, orclPluginCheckEntryExist, orclPluginEnable, orclPluginEntryProperties, orclPluginIsReplace, orclPluginKind, orclPluginRequestGroup, orclPluginRequestNegGroup, orclPluginResultCode, orclPluginSASLCallBack, orclPluginSearchNotFound, orclPluginShareLibLocation, orclPluginSubscriberDNList, orclPluginTiming, orclPluginVersion

orclPluginContainer

Description
Container object for Oracle Internet Directory plug-ins.

Object ID
2.16.840.1.113894.1.2.92

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclPluginPort

orclPluginUser

Description
Configuration attributes for Oracle Internet Directory plug-ins.

Object ID
2.16.840.1.113894.1.2.91

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, userPassword

Allowed Attributes
description

orclPurgeConfig

Description
Configuration attributes for Oracle Internet Directory garbage collectors. Oracle Internet Directory provides several predefined garbage collectors that, together, clean up all unwanted data in the directory server.

Object ID
2.16.840.1.113894.1.2.150

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclPurgeBase

Allowed Attributes
orclPurgeDebug, orclPurgeEnable, orclPurgeFileLoc, orclPurgeFileName, orclPurgeFilter, orclPurgeInterval, orclPurgeNow, orclPurgePackage, orclPurgeStart , orclPurgeTargetAge, orclPurgeTranSize

orclPwdVerifierPolicy

Description
A password verifier policy entry associates a password policy with an application.

Object ID
2.16.840.1.113894.1.2.42

Superior Object Class
pwdpolicy

Object Class Type
Auxilliary

Required Attributes
orclAppId

Allowed Attributes
N/A

orclPwdVerifierProfile

Description
Oracle Internet Directory and other Oracle components both store the user password in the user entry, but use different attributes. A password verifier profile entry associates the correct user password attribute with a component or application.

Object ID
2.16.840.1.113894.1.2.41

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclAppId

Allowed Attributes
displayName, orclPwdVerifierParams, owner

orclReplAgreementEntry

Description
Configuration attributes for replication.

Object ID
2.16.840.1.113894.1.2.8

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclAgreementId, orclReplicationProtocol, orclUpdateSchedule

Allowed Attributes
orclDirReplGroupDSAs, orclExcludedAttributes, orclExcludedNamingContexts, orclHIQSchedule, orclIncludedNamingContexts, orclLastAppliedChangeNumber, orclLDAPConnKeepALive, orclReplicaDN

orclReplicaSubentry

Description
Configuration attributes for replication.

Object ID
2.16.840.1.113894.1.2.151

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclReplicaID

Allowed Attributes
orclPilotMode, orclReplicaSecondaryURI, orclReplicaState, orclReplicaType, orclReplicaURI, orclReplicaVersion, pilotStartTime, seeAlso

orclReplInstance

Description
Configuration attributes for an Oracle Directory Replication server instance.

Object ID
2.16.840.1.113894.1.2.14

Superior Object Class
top, orclReplSubConfig

Object Class Type
Structural

Required Attributes
cn, orclConfigSetNumber, orclHostname

Allowed Attributes
description, seeAlso

orclReplNameCtxConfig

Description
Configuration attributes for replication naming contexts.

Object ID
2.16.840.1.113894.1.2.104

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclIncludedNamingContexts

Allowed Attributes
orclExcludedAttributes, orclExcludedNamingContexts

orclReplSubConfig

Description
Directory Replication server configuration attributes.

Object ID
2.16.840.1.113894.1.2.4

Superior Object Class
top, orclConfigSet

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
orclChangeLogLife, orclChangeRetryCount, orclDirReplGroupAgreement, orclPurgeSchedule, orclThreadsPerSupplier

orclResourceDescriptor

Description
Configuration attributes for a resource.

Object ID
2.16.840.1.113894.1.2.65

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclResourceName

Allowed Attributes
description, displayName, orclFlexAttribute1, orclFlexAttribute2, orclFlexAttribute3, orclOwnerGUID, orclPasswordAttribute, orclResourceTypeName, orclResourceViewers, orclUserIDAttribute, orclUserModifiable

orclResourceType

Description
Configuration attributes for resource types.

Object ID
2.16.840.1.113894.1.2.63

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclResourceTypeName

Allowed Attributes
description, javaClassName, orclConnectionFormat, orclFlexAttribute1, orclFlexAttribute2, orclFlexAttribute3, orclPasswordAttribute, orclUserIDAttribute

orclRootContext

Description
Configuration of the Oracle Context.

Object ID
2.16.840.1.113894.7.2.1006

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
description

orclSchemaVersion

Description
Configuration of the Oracle Context.

Object ID
2.16.840.1.113894.7.2.6

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclProductVersion

Allowed Attributes
N/A

orclSecRefreshEvents

Description
Oracle Internet Directory Server Manageability attributes for security refresh events.

Object ID
2.16.840.1.113894.1.2.28

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclAuditMessage, orclEventType, orclOpResult, orclUserDN

orclService

Description
Configuration attributes for a service.

Object ID
2.16.840.1.113894.7.2.1001

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
description, orclNetDescName, orclNetDescString, orclOracleHome, orclServiceType, orclSID, orclSystemName, orclVersion

orclServiceInstance

Description
Configuration attributes for a service instance.

Object ID
2.16.840.1.113894.1.2.191

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclServiceType

Allowed Attributes
description, displayName, labeledURI, orclAssocDB, orclAssocIasInstance, orclEnabled, orclFlexAttribute1, orclMasterNode, orclNetDescName, orclNetDescString, orclOracleHome, orclServiceSubType, orclSID, orclSystemName, orclVersion

orclServiceInstanceReference

Description
Reference for a service instance.

Object ID
2.16.840.1.113894.1.2.200

Superior Object Class
N/A

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
cn, description, orclServiceInstanceLocation, orclServiceSubscriptionLocation, seeAlso

orclServiceRecipient

Description
Additional attributes for a service recipient.

Object ID
2.16.840.1.113894.1.2.68

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclActiveEndDate, orclActiveStartdate, orclIsEnabled

orclServiceSubscriptionDetail

Description
Service subscription detail.

Object ID
2.16.840.1.113894.1.2.201

Superior Object Class
orclReferenceObject

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
orclActiveEndDate, orclActiveStartdate, orclIsEnabled

orclServiceSuite

Description
Configuration for a suite of services.

Object ID
2.16.840.1.113894.1.2.193

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn, orclSuiteType

Allowed Attributes
description, displayName, orclEnabled, orclFlexAttribute1, orclServiceMember, orclVersion

orclSM

Description
Oracle Internet Directory Server Manageability statistics.

Object ID
2.16.840.1.113894.1.2.25

Superior Object Class
top

Object Class Type
Structural

Required Attributes
orclSequence

Allowed Attributes
orclEventTime, orclHostname, orclLDAPInstanceID, orclLDAPProcessID, orclSMSpec

orclSubscriber

Description
Subscriber info for a user entry.

Object ID
2.16.840.1.113894.1.2.58

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
c, jpegPhoto, orclContact, orclHostedCreditCardExpireDate, orclHostedCreditCardNumber, orclHostedCreditCardType, orclHostedDunsNumber, orclHostedPaymentTerm, orclSubscriberFullName, orclSubscriberType, orclVersion

orclSysResourceEvents

Description
Error log entry for Oracle Internet Directory server.

Object ID
2.16.840.1.113894.1.2.29

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclDBConnCreationFailed, orclDNSUnavailable, orclEventType, orclFDIncreaseError, orclMaxFDLimitReached, orclMaxProcessLimitReached, orclMemAllocError, orclNWCongested, orclNwUnavailable, orclORA28error, orclORA3113error, orclORA3114error, orclThreadSpawnFailed

orclTraceConfig

Description
Configuration for Oracle Internet Directory Server Manageability.

Object ID
2.16.840.1.113894.1.2.31

Superior Object Class
top

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
orclTraceDimesionLevel, orclTraceFileLocation, orclTraceFileSize, orclTraceLevel, orclTraceMode

orclUniqueConfig

Description
Configuration for attributes that must have unique values for each entry that meets the specified requirements.

Object ID
2.16.840.1.113894.1.2.103

Superior Object Class
orclCommonAttributes

Object Class Type
Structural

Required Attributes
orclUniqueAttrName

Allowed Attributes
orclUniqueEnable, orclUniqueObjectClass, orclUniqueScope, orclUniqueSubtree

orclUserStats

Description
Oracle Internet Directory Server Manageability statistics for users.

Object ID
2.16.840.1.113894.1.2.32

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
N/A

Allowed Attributes
orclACLResultsLatency, orclAttrACLEvalLatency, orclBERgenLatency, orclDBLatency, orclDIMEonlyLatency, orclEntryACLEvalLatency, orclFilterACLEvalLatency, orclFrontLatency, orclGenObjLatency, orclGetNearACLLatency, orclIpAddress, orclOpAbandoned, orclOpCompleted, orclOpenConn, orclOpFailed, orclOpInitiated, orclOpLatency, orclOpPending, orclOpSucceeded, orclOpTimedOut, orclSQLexeFetchLatency, orclSQLGenReusedParsed, orclUserDN

orclUserV2

Description
Optional attributes for user entries.

Object ID
2.16.840.1.113894.1.2.52

Superior Object Class
top

Object Class Type
88

Required Attributes
N/A

Allowed Attributes
authPassword, c, krbPrincipalName, middleName, orclActiveEndDate, orclActiveStartdate, orclDateOfBirth, orclDefaultProfileGroup, orclDisplayPersonalInfo, orclGender, orclHireDate, orclIsEnabled, orclIsVisible, orclMaidenName, orclPassword, orclPasswordHint, orclPasswordHintAnswer, orclPasswordVerifier, orclPKCS12Hint, orclSAMAccountName, orclSearchFilter , orclTimeZone, orclUIAccessibilityMode, orclWirelessAccountNumber, orclWorkflowNotificationPref, userPKCS12

pwdpolicy

Description
Defines password policy information for a set of users in a given DIT. It contains attributes that define the password policy information for the entire directory.

Object ID
1.3.6.1.4.1.42.2.27.8.2.1

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
displayName, orclPwdAllowHashCompare, orclPwdAlphaNumeric, orclPwdEncryptionEnable, orclPwdIllegalValues, orclPwdIPLockout , orclPwdIPLockoutDuration, orclPwdIPMaxFailure, orclPwdPolicyEnable, pwdAllowUserChange , pwdCheckSyntax, pwdExpireWarning, pwdFailureCountInterval, pwdGraceLoginLimit, pwdInHistory, pwdLockout, pwdLockoutDuration, pwdMaxAge, pwdMaxFailure, pwdMinAge, pwdMinLength, pwdMustChange, pwdSafeModify

subentry

Description
Oracle Internet Directory DIT configuration for subentries.

Object ID
2.5.17.0

Superior Object Class
top

Object Class Type
Structural

Required Attributes
cn

Allowed Attributes
N/A

subregistry

Description
Oracle Internet Directory DIT configuration.

Object ID
2.16.840.1.113894.1.2.12

Superior Object Class
top

Object Class Type
Auxilliary

Required Attributes
cn

Allowed Attributes
N/A

subschema

Description
Oracle Internet Directory schema elements.

Object ID
2.5.20.1

Superior Object Class
N/A

Object Class Type
Auxilliary

Required Attributes
attributetypes, objectclasses

Allowed Attributes
contentRules, ldapSyntaxes, matchingRules

tombstone

Description
Garbage collector to clean up entries marked as deleted.

Object ID
2.16.840.1.113894.1.2.24

Superior Object Class
top

Object Class Type
Structural

Required Attributes
N/A

Allowed Attributes
ref

top

Description

Contains common and operational attributes used by various objects in Oracle Internet Directory.

Object ID

2.5.6.0

Superior Object Class

N/A

Object Class Type

Abstract

Required Attributes

objectClass

Allowed Attributes

authPassword, createTimestamp, creatorsName, modifiersName, modifyTimestamp, orclACI, orclEntryLevelACI, orclGUID, orclNormDN, orclObjectGUID, orclPwdAccountUnlock, orclPwdIPAccountLockedTime, orclPwdIPFailureTime, orclRevPwd, orclUnsyncRevPwd, pwdAccountLockedTime, pwdChangedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdHistory

9

Attribute Reference

This chapter contains reference information about the LDAP attributes used for Oracle Identity Management. It contains the following topics:

- Standard LDAP Attributes
- Oracle Identity Management Attribute Reference

For a list of attributes grouped by functional categories, see "Overview of Oracle Identity Management Schema Elements" on page 7-8.

Standard LDAP Attributes

Oracle Internet Directory supports the following standard LDAP attributes as defined in the Internet Engineering Task Force (IETF) Requests for Comments (RFC) specifications.

Details of RFC specifications can be found on the IETF Web site at: `http://www.ietf.org`.

Table 9–1 Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
aliasedObjectName	RFC 2256
applicationEntity	RFC 2256
associatedDomain	RFC 1274
associatedName	RFC 1274
audio	RFC 1274
authorityRevocationList	RFC 2256
authPassword	RFC 3112
bootFile	RFC 2307
bootParameter	RFC 2307
businessCategory	RFC 2256
c	RFC 2256
caCertificate	RFC 2256
carLicense	RFC 2798
certificateRevocationList	RFC 2256
cn	RFC 2256

Table 9–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
co	RFC 1274
crossCertificatePair	RFC 2256
dc	RFC 2247
deltaRevocationList	RFC 2256
departmentNumber	RFC 2798
description	RFC 2256
destinationIndicator	RFC 2256
displayName	RFC 2798
dITRedirect	RFC 1274
dmdName	RFC 2256
dNSRecord	RFC 1274
drink	RFC 1274
dSAQuality	RFC 1274
employeeNumber	RFC 2798
employeeType	RFC 2798
facsimileTelephoneNumber	RFC 2256
gecos	RFC 2307
gidNumber	RFC 2307
givenName	RFC 2798
homeDirectory	RFC 2307
homePhone	RFC 1274
homePostalAddress	RFC 1274
host	RFC 1274
initials	RFC 2256
internationalISDNNumber	RFC 2256
ipHostNumber	RFC 2307
ipNetmaskNumber	RFC 2307
ipNetworkNumber	RFC 2307
ipProtocolNumber	RFC 2307
ipServicePort	RFC 2307
ipServiceProtocol	RFC 2307
javaClassName	RFC 2713
javaClassNames	RFC 2307
javaCodebase	RFC 2307
javaDoc	RFC 2307
javaFactory	RFC 2307
javaReferenceAddress	RFC 2713

Table 9–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
javaSerializedData	RFC 2713
janetMailbox	RFC 1274
jpegPhoto	RFC 1488
knowledgeInformation	RFC 2256
l	RFC 2256
labeledURI	RFC 2079
lastModifiedBy	RFC 1274
lastModifiedTime	RFC 1274
loginShell	RFC 2307
macAddress	RFC 2307
mail	RFC 2798
mailAlternateAddress	RFC 2256
mailHost	RFC 2256
mailPreferenceOption	RFC 1274
mailRoutingAddress	RFC 2256
manager	RFC 1274
member	RFC 2256
memberNisNetgroup	RFC 2307
memberUid	RFC 2307
mobile	RFC 1274
nisDomain	RFC 2307
nisMapEntry	RFC 2307
nisMapName	RFC 2307
nisNetgroupTriple	RFC 2307
nisPublicKey	RFC 2307
nisSecretKey	RFC 2307
o	RFC 2256
oncRpcNumber	RFC 2307
organizationalStatus	RFC 1274
otherMailbox	RFC 1274
ou	RFC 2256
owner	RFC 2256
pager	RFC 1274
personalSignature	RFC 1274
personalTitle	RFC 1274
photo	RFC 1274
physicalDeliveryOfficeName	RFC 2256

Table 9–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
postalAddress	RFC 2256
postalCode	RFC 2256
postOfficeBox	RFC 2256
preferredDeliveryMethod	RFC 2256
preferredDeliveryMethod	RFC 2377
preferredLanguage	RFC 2798
presentationAddress	RFC 2256
protocolInformation	RFC 2256
ref	RFC 3296
registeredAddress	RFC 2256
roleOccupant	RFC 2256
roomNumber	RFC 1274
searchGuide	RFC 2256
secretary	RFC 1274
seeAlso	RFC 2256
serialNumber	RFC 2256
shadowExpire	RFC 2307
shadowFlag	RFC 2307
shadowInactive	RFC 2307
shadowLastChange	RFC 2307
shadowMax	RFC 2307
shadowMin	RFC 2307
shadowWarning	RFC 2307
sn	RFC 2256
st	RFC 2256
street	RFC 2256
subtreeMaximumQuality	RFC 1274
subtreeMinimumQuality	RFC 1274
supportedApplicationContext	RFC 2256
telephoneNumber	RFC 2256
teletexTerminalIdentifier	RFC 2256
telexNumber	RFC 2256
textEncodedORaddress	RFC 2377
title	RFC 2256
uid	RFC 2253
uidNumber	RFC 2307
uniqueIdentifier	RFC 1274

Table 9–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
uniqueMember	RFC 2256
userCertificate;binary	RFC 2256
userClass	RFC 1274
userPassword	RFC 2256
userPKCS12	RFC 2798
userSMIMECertificate	RFC 2798
x121Address	RFC 2256
x500UniqueIdentifier	RFC 2256

Oracle Identity Management Attribute Reference

This section contains an alphabetical listing of the Oracle Identity Management attributes. These are the attributes used in entries pertaining to Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, OracleAS Single Sign-On, and Oracle Application Server Certificate Authority.

attributeMap

Description

Attribute mappings used by the **POSIX** naming directory user agent (DUA).

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.9

attributeTypes

Description

Attribute types supported by the directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.3 (Attribute Type Description)

Matching Rule

objectIdentifierFirstComponentMatch

Object ID

2.5.21.5

Other
Directory operational attribute.

authenticationMethod

Description
Identifies the type of authentication method used to contact the directory server agent (DSA).

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseIgnoreIA5Match

Object ID
1.3.6.1.4.1.11.1.3.1.1.6

Other
Single-valued attribute.

authPassword

Description
Attribute for storing a password to an Oracle component when that password is the same as that used to authenticate the user to the directory, namely, userPassword. The value in this attribute is synchronized with that in the userPassword attribute.

Several different applications can require the user to enter the same clear text password used for the directory, but each application may hash it with a different algorithm. In this case, the same clear text password can become the source of several different password verifiers.

This attribute is multivalued and can contain all the other verifiers that different applications use for this user's clear text password. If the `userpassword` attribute is modified, then the `authpassword` values for all applications are regenerated.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
1.3.6.1.4.1.4203.1.3.4

bindTimeLimit

Description
Maximum time in seconds a **POSIX** directory user agent (DUA) should allow for a search to complete.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.11.1.3.1.1.4

Other
Single-valued attribute.

c

Description
Specifies the country associated with a user's address.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.5.4.6

Other
Single-valued attribute.

cn

Description
The common name (nickname) attribute which contains the name of an object. If the object corresponds to a user, it is typically the user's full name. A cn (common name) isn't unique, whereas a dn (distinguished name) is unique.

For example, if ABC corp employs two people with the name John Smith, one in HR and one in Finanace then they both would have a cn=John Smith, but they would have unique DNs because the DN would take the form:

```
cn=John Smith, ou=HR, o=ABC or
cn=John Smith, ou=Finance, 0=ABC

Where ou= organizational unit, and o=organization
```

Syntax
1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule
caseIgnoreMatch

Object ID
2.5.4.3

contentRules

Description
Specifies the permissible content of entries of a particular structural object class through the identification of an optional set of auxiliary object classes, mandatory, optional, and precluded attributes.

Syntax
1.3.6.1.4.1.1466.115.121.1.16 (DIT Content Rule Description)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1004

createTimestamp

Description
The time that the entry was created.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rules
generalizedTimeMatch

Object ID
2.5.18.1

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

creatorsName

Description
The DN of the entity (such as a user or an application) that created the entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.5.18.3

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

credentialLevel

Description
Identifies the type of credentials a **POSIX** directory user agent (DUA) should use when binding to the directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseIgnoreIA5Match

Object ID
1.3.6.1.4.1.11.1.3.1.1.10

Other
Single-valued attribute.

defaultSearchBase

Description
The default base DN used by a **POSIX** directory user agent (DUA).

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
1.3.6.1.4.1.11.1.3.1.1.1

defaultSearchScope

Description
User defined search scope used by a **POSIX** directory user agent (DUA).

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
N/A

Object ID
1.3.6.1.4.1.11.1.3.1.1.12

Other
Single-valued attribute.

defaultServerList

Description
The IP addresses of the default servers that a directory user agent (DUA) should use in a space separated list. After the servers in preferredServerList are tried, those default servers on the client's subnet are tried, followed by the remaining default servers, until a connection is made. At least one server must be specified in either `preferredServerList` or `defaultServerList`. This attribute has no default value.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseIgnoreIA5Match

Object ID
1.3.6.1.4.1.11.1.3.1.1.0

Other
Single-valued attribute.

description

Description
An optional description for the entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{1024} (Directory String, 1024 character maximum)

Matching Rule
caseIgnoreMatch

Object ID
2.5.4.13

displayName

Description
The preferred name used when displaying the entry in the GUI tools.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113730.3.1.241

Other
Single-valued attribute.

followReferrals

Description
Tells a **POSIX** directory user agent (DUA) if it should follow referrals returned by a directory server agent (DSA) search result.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseIgnoreIA5Match

Object ID
1.3.6.1.4.1.11.1.3.1.1.5

Other
Single-valued attribute.

javaClassName

Description
Fully qualified name of a distinguished Java class or interface.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseExactMatch

Object ID
1.3.6.1.4.1.42.2.27.4.1.6

Other
Single-valued attribute.

jpegPhoto

Description
A photograph file in JPEG format.

Syntax
1.3.6.1.4.1.1466.115.121.1.28 (Binary)

Matching Rule
octetStringMatch

Object ID
0.9.2342.19200300.100.1.60

krbPrincipalName

Description
Contains the Kerberos principal name.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
1.3.18.0.2.4.1091

Other
Single-valued attribute.

labeledURI

Description
Uniform Resource Locator (URL).

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseExactIA5Match

Object ID
1.3.6.1.4.1.250.1.57

ldapSyntaxes

Description
Identifies the LDAP syntaxes implemented in the directory schema.

Syntax
1.3.6.1.4.1.1466.115.121.1.54 (LDAP Syntax Description)

Matching Rule
objectIdentifierFirstComponentMatch

Object ID
1.3.6.1.4.1.1466.101.120.16

Other
Directory operational attribute.

mail

Description
This attribute is defined in RFC 1274. Identifies a user's primary e-mail address (the e-mail address retrieved and displayed by "white-pages" lookup applications).

For example: `mail: user.name@oracle.com`

Syntax
1.3.6.1.4.1.1466.115.121.1.26{256} (IA5 String, 256 character maximum)

Matching Rule
caseIgnoreIA5Match

Object ID
0.9.2342.19200300.100.1.3

Other
Directory operational attribute.

matchingRules

Description
Identifies the matching rules implemented in the directory schema.

Syntax
1.3.6.1.4.1.1466.115.121.1.30 (Matching Rule Description)

Matching Rule
objectIdentifierFirstComponentMatch

Object ID
2.5.21.4

middleName

Description
A user's middle name.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
1.3.6.1.4.1.1466.101.120.34

modifiersName

Description
The DN of the entity (such as a user or application) that last updated the entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.5.18.4

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

modifyTimestamp

Description
The time the entry was last modified.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.5.18.2

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

namingContexts

Description
Top-level DNs for the naming contexts contained in this server. You must have super user privileges to publish a DN as a naming context. There is no default value.

This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
N/A

Object ID
1.3.6.1.4.1.1466.101.120.5

Other
DSA operational attribute.

objectClass

Description
The list of object classes from which this object class is derived.

Syntax
1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

Matching Rule
objectIdentifierMatch

Object ID
2.5.4.0

objectClasses

Description
Defines the object classes which are in force within a subschema.

Syntax
1.3.6.1.4.1.1466.115.121.1.37 (Object Class Description)

Matching Rule
objectIdentifierFirstComponentMatch

Object ID
2.5.21.6

Other
Directory operational attribute.

objectClassMap

Description
A mapping from an object class defined by a directory user agent (DUA) to an object class in an alternative schema used in the directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
N/A

Object ID
1.3.6.1.4.1.11.1.3.1.1.11

orclACI

Description
Access control instructions are stored in the directory as attributes of entries. The `orclACI` attribute is an operational attribute; it is available for use on every entry in the directory, regardless of whether it is defined for the object class of the entry. It is used by the directory server to evaluate what rights are granted or denied when it receives an LDAP request from a client.

Syntax
1.3.6.1.4.1.1466.115.121.1.1 (Access Control Item)

Matching Rule
accessDirectiveMatch

Object ID
2.16.840.1.113894.1.1.42

orclACLResultsLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.129

Other
Single-valued attribute.

orclActiveConn

Description
Specifies the number of active connections to the Oracle Internet Directory server, including client LDAP connections and database connections.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.150

Other
Single-valued attribute.

orclActiveEndDate

Description
Specifies the date and time beyond which a user account is no longer active and beyond which the user is not allowed to authenticate.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.339

Other
Single-valued attribute.

orclActiveStartdate

Description
Specifies the date and time that a user account is active and the user is allowed to authenticate. If not specified, then the user is considered active immediately.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.330

Other
Single-valued attribute.

orclActiveThreads

Description
Specifies the number of active threads on the Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.140

orclAgreementId

Description
Naming attribute for the replication agreement entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.26

Other
Single-valued attribute.

orclAnonymousBindsFlag

Description
Specifies whether anonymous binds to the directory are allowed or not. If set to 1, then anonymous binds are allowed. If set to 0 (zero), then they are not allowed. The default is 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.299

Other
Single-valued attribute.

orclAppFullName

Description
The full name of an application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.320

orclAppId

Description
The unique identifier of an application entry associated with a password verifier.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 characters maximum)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.207

Other
Single-valued attribute.

orclApplicationCommonName

Description
The common name (cn) of the application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.319

orclApplicationType

Description
Identifies the application type, such as OracleAS Portal.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.280

Other
Single-valued attribute.

orclAssocDB

Description
Identifies the associated Oracle Database instance with the application or service.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1007

orclAssoclasInstance

Description
Identifies the associated Oracle Application Server instance with the application or service.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1006

orclAttrACLEvalLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.138

Other
Single-valued attribute.

orclAuditAttribute

Description
Identifies the audit attribute.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.58

orclAuditLevel

Description
Specifies the audit level.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.63

Other
Single-valued attribute.

orclAuditMessage

Description
Stores an audit message.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.59

orclBERgenLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.139

Other
Single-valued attribute.

orclCatalogEntryDN

Description
Contains the DN of the catalog entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.50

Other
Single-valued attribute.

orclCategory

Description
Identifies the business category of a service or an application entity

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.317

orclCertExtensionAttribute

Description
Holds the `OID` of a field within an extension field of the client certificate.

Syntax
1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

Matching Rule
objectIdentifierMatch

Object ID
2.16.840.1.113894.1.1.711

Other
Single-valued attribute.

orclCertExtensionOID

Description
Holds the extension field `OID` of the client certificate.

Syntax
1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

Matching Rule
objectIdentifierMatch

Object ID
2.16.840.1.113894.1.1.709

Other
Single-valued attribute.

orclCertificateHash

Description
This is a special catalog attribute used for certificate matching. The value of this attribute is computed by calculating a hash of the user certificate when it is added to Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
2.16.840.1.113894.1.1.184

Other
Single-valued attribute.

Not user modifiable.

orclCertificateMatch

Description
This is a special catalog attribute used for certificate matching. The value of this attribute contains the correct matching value to use for a user certificate based on the orclPKIMatchingRule setting.

Syntax
1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule
octetStringMatch

Object ID
2.16.840.1.113894.1.1.183

Other
Single-valued attribute.

Not user modifiable.

orclCertMappingAttribute

Description
Holds the standard field `OID` of the client certificate.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.708

Other
Single-valued attribute.

orclChangeLogLife

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.806

Other
Single-valued attribute.

DSA operational attribute.

orclChangeRetryCount

Description
The number of processing retry attempts for a replication change-entry before being moved to the human intervention queue. The value for this parameter must be equal to or greater than 1 (one).

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.23

Other
Single-valued attribute.

DSA operational attribute.

orclCommonAutoRegEnabled

Description
Specifies if auto-registration is enabled or disabled. Allowed values are 0 (disabled) or 1 (enabled).

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.567

Other
Single-valued attribute.

orclCommonContextMap

Description
Stores the common context map.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.904

Other
Single-valued attribute.

orclCommonDefaultUserCreateBase

Description
Identifies the default user creation base where users are created.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.908

Other
Single-valued attribute.

orclCommonGroupCreateBase

Description
Identifies the group creation base under which Oracle Delegated Administration Services creates groups

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.903

orclCommonNamingAttribute

Description
Specifies the name of the attribute that is used as an RDN component when creating a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.900

orclCommonNicknameAttribute

Description
Specifies the name of the attribute that uniquely identifies users.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.7

Other
Single-valued attribute.

orclCommonSASLRealm

Description
Identifies the common SASL realm. This attribute contains a string value specifying a subset of related entries under a subscriber realm.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.20

Other
Single-valued attribute.

orclCommonUserSearchBase

Description
Identifies the branch that contains user entries.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.7.1.10

orclCommonVerifierEnable

Description
If this attribute is enabled then the common verifier will be used for all related applications. If this attribute is disabled then each application must setup their own verifier profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.214

Other
Single-valued attribute.

orclConfigSetNumber

Description
The configuration parameters for each Oracle Internet Directory server instance are stored in an entry called a configuration set entry (configset). This attribute specifies a number of a configset entry, which can be referenced when starting an Oracle Internet Directory server instance. The number of the default configset entry is 0 (zero).

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.40

Other
Single-valued attribute.

orclConnectByAttribute

Description
The attribute type name that you want to use as the filter for a dynamic group query—for example, `manager`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1001

Other
Single-valued attribute.

orclConnectBySearchBase

Description
A naming context in the DIT that you want to use as the base for a dynamic group query—for example, `l=us,dc=mycompany,dc=com`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1003

Other
Single-valued attribute.

orclConnectByStartingValue

Description
For a dynamic group query, this specifies the DN of the attribute you specified in the orclConnectByAttribute attribute—for example, `Anne Smith`.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.1002

Other
Single-valued attribute.

orclConnectionFormat

Description
Specifies the format used to construct the connect string associated with a resource.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.354

Other
Single-valued attribute.

orclContact

Description
Identifies a contact person for an organization or an application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.332

Other
Single-valued attribute.

orclCryptoScheme

Description
The hash algorithm used to encrypt passwords that are stored in the directory. Options are: MD4, MD5, No encryption, SHA, SSHA, or UNIX Crypt. The default is MD4.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 characters maximum)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.68

Other
Single-valued attribute.

orclDASAdminModifiable

Description
Specifies whether or not administration of this entry is available through Oracle Delegated Administration Services.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.324

Other
Single-valued attribute.

orclDASAttrDispOrder

Description
Specifies the display order of an attribute in Oracle Delegated Administration Services.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.341

orclDASAttrName

Description
Specifies the name of an attribute to show in Oracle Delegated Administration Services.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.340

orclDASEnableProductLogo

Description
Specifies whether or not to display a product logo on the Identity Management Realm Configuration window of Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.362

Other
Single-valued attribute.

orclDASEnableSubscriberLogo

Description
Specifies whether or not to display a realm logo on the Identity Management Realm Configuration window of Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.361

Other
Single-valued attribute.

orclDASIsEnabled

Description
Specifies whether or not an attribute is enabled for Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.344

Other
Single-valued attribute.

orclDASIsMandatory

Description
Specifies whether or not an attribute is mandatory for Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.321

Other
Single-valued attribute.

orclDASIsPersonal

Description
Specifies whether or not an attribute is personal information to be supplied by a user in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.326

Other
Single-valued attribute.

orclDASLOV

Description
The list of values to display to users in the UI when the orclDASUIType=Predefined List.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.328

orclDASPublicGroupDNs

Description
Specifies the DNs of groups available for Oracle Delegated Administration Services.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.343

orclDASSearchable

Description
Specifies whether of not this attribute is searchable in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.906

Other
Single-valued attribute.

orclDASSearchColIndex

Description
Indicates the position in the DAS search result table column, if present.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.902

Other
Single-valued attribute.

orclDASSearchFilter

Description
Specifies whether the attribute is searchable through Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.325

Other
Single-valued attribute.

orclDASSearchSizeLimit

Description
The maximum number of entries to return in a Oracle Delegated Administration Services search.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.363

Other
Single-valued attribute.

orclDASSelfModifiable

Description
Specifies whether or not an attribute is modifiable by the user in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.322

Other
Single-valued attribute.

orclDASUIType

Description
Specifies the UI field type for an attribute when displayed in Oracle Delegated Administration Services. Options are:

- Single Line Text
- Multi Line Text
- Predefined List
- Date
- Browse and Select
- Number

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.327

Other
Single-valued attribute.

orclDASURL

Description
The corresponding URL of an Oracle Delegated Administration Services unit.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.310

orclDASURLBase

Description
This holds the URL base in install area for Oracle Delegated Administration Services.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.345

orclDASValidatePwdReset

Description
Specifies whether or not this attribute can be used for password reset validation purposes in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.905

Other
Single-valued attribute.

orclDASViewable

Description
Specifies whether or not this attribute is viewable through Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.323

Other
Single-valued attribute.

orclDateOfBirth

Description
Specifies the date on which a user was born.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.307

Other
Single-valued attribute.

orclDBConnCreationFailed

Description
Indicates a connection failure to the database in an error log entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.155

Other
Single-valued attribute.

orclDBLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.130

Other
Single-valued attribute.

orclDBSchemaIdentifier

Description
DN of the DB registration entry in OID that an application entity uses.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.347

orclDBType

Description
The type of database used. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.5

Other
Single-valued attribute.

orclDebugFlag

Description
The debug level associated with a server instance. The default for is 0 (zero). The valid range is 0 to 67108863.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.97

Other
Single-valued attribute.

orclDebugForceFlush

Description
Specifies whether debug messages are to be written to the log file when a message is logged by the directory server. To enable it, set its value to 1. To disable it set it to 0, which is its default value.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.193

Other
Single-valued attribute.

orclDebugOp

Description
To make logging more focused, limits logged information to particular directory server operations by specifying the debug dimension to those operations. Values for operations are:

- 1 - ldapbind
- 2 - ldapunbind
- 4 - ldapadd
- 8 - ldapdelete

- 16 - ldapmodify
- 32 - ldapmodrdn
- 64 - ldapcompare
- 128 - ldapsearch
- 264 - ldapabandon
- 511 - all operations

To log more than one operation, add the values of their dimensions. For example, if you want to trace ldapbind (1), ldapadd (4) and ldapmodify (16) operations, then the value would be 21 (1 + 4 + 16 = 21).

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.601

Other
Single-valued attribute.

orclDefaultProfileGroup

Description
Holds the DN of the group to designate the default group for a user, such that a default profile can be built for the user based on this attribute value.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.309

Other
Single-valued attribute.

orclDefaultSubscriber

Description
Identifies the default realm.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.312

orclDIMEonlyLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.131

Other
Single-valued attribute.

orclDIPRepository

Description
Used to determine if the directory is used as the Oracle Directory Integration Platform repository.

Syntax
1.3.6.1.4.1.1466.115.121.1.15

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.124

Other
Single-valued attribute.

orclDirectoryVersion

Description
The version of Oracle Internet Directory. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax
1.3.6.1.4.1.1466.115.121.1.15

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.67

Other
Single-valued attribute.

orclDirReplGroupAgreement

Description
Contains the directory replication group agreement DN.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.25

Other
DSA operational attribute.

orclDirReplGroupDSAs

Description
For Advanced Replication-based directory replication groups (DRGs), the orclReplicaID values of all the nodes in the DRG. This list must be identical on all nodes in the group. This attribute is not applicable for LDAP-based replication agreements.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.48

Other
DSA operational attribute.

orclDisplayPersonalInfo

Description
Specifies if the user's personal information should be displayed in white pages queries. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.304

Other
Single-valued attribute.

orclDITRoot

Description
The root of the directory information tree (DIT). This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.7

Other
Single-valued attribute.

orclDNSUnavailable

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.161

Other
Single-valued attribute.

orclEcacheEnabled

Description
Specifies whether or not entry caching is enabled. The value for enabled is 1; the value for disabled is 0. The default is 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.400

Other
Single-valued attribute.

orclEcacheHitRatio

Description
Stores the cache hit ratio.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.170

Other
Single-valued attribute.

orclEcacheMaxEntries

Description
Maximum number of entries that can be present in the entry cache. The default is 25,000.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.402

Other
Single-valued attribute.

orclEcacheMaxEntSize

Description
Stores the maximum size of a cache entry in bytes.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.602

Other
Single-valued attribute.

orclEcacheMaxSize

Description
Maximum number of bytes of RAM that the entry cache can use. The default is 100 MB.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.401

Other
Single-valued attribute.

orclEcacheNumEntries

Description
The number of entries currently in the entry cache.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.171

Other
Single-valued attribute.

orclEcacheSize

Description
The current size of the entry cache.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.172

Other
Single-valued attribute.

orclEnabled

Description
Determines whether an application is enabled or disabled for use.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.1008

Other
Single-valued attribute.

orclEnableGroupCache

Description

Whether or not to cache privilege groups and ACL groups. Using this cache improves the performance of access control evaluation for users.

Use the group cache when a privilege group membership does not change frequently. If a privilege group membership does change frequently, then it is best to turn off the group cache. This is because, in such a case, computing a group cache increases overhead. The default is 1 (enabled). Change to 0 (zero) to disable.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.403

Other

Single-valued attribute.

orclEntryACLEvalLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.136

Other

Single-valued attribute.

orclEntryLevelACI

Description

Specifies the ACI that holds object level ACL.

Syntax

1.3.6.1.4.1.1466.115.121.1.1 (Access Control Item)

Matching Rule

accessDirectiveMatch

Object ID
2.16.840.1.113894.1.1.43

orclEventLevel

Description
Specifies critical events related to security and system resources to be recorded for server manageability statistics. The default value is 0. Allowed values are:

- 0 — No events
- 1— Super user login
- 2 — Proxy user login
- 4 — Replication login
- 8 — Add access
- 16 — Delete access
- 32 — Write access
- 64 — ORA-3113 error
- 128 — ORA-3114 error
- 255 — All critical events

This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

For events other than super user, proxy user, and replication login, set the value of the orclStatsFlag attribute to 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.195

Other
Single-valued attribute.

orclEventTime

Description
The time that a logged directory event occurred.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.60

orclEventType

Description
The type of logged directory event.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.57

orclExcludedAttributes

Description
Specifies an attribute (within the specified naming context) to be excluded from replication. Applies to partial replication only.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.506

Other
DSA operational attribute.

orclExcludedNamingContexts

Description
For Advanced Replication-based agreements, this attribute specifies one or more subtrees to be excluded from replication.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.47

Other
DSA operational attribute.

orclFDIncreaseError

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.163

Other
Single-valued attribute.

orclFilterACLEvalLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.137

Other
Single-valued attribute.

orclFlexAttribute1

Description
An additional attribute for storing more information about a resource, service, or component.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.355

orclFlexAttribute2

Description
An additional attribute for storing more information about a resource, service, or component.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.356

orclFlexAttribute3

Description
An additional attribute for storing more information about a resource, service, or component.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.357

orclFrontLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.128

Other
Single-valued attribute.

orclGender

Description
The gender of a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.346

Other
Single-valued attribute.

orclGenObjLatency

Description
Stores the general object latency.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.133

Other
Single-valued attribute.

orclGetNearACLLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.135

Other
Single-valued attribute.

orclGlobalID

Description
Specifies the attribute that is used to identify the global ID of a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.8

Other
Single-valued attribute.

orclGUID

Description
This is the global unique identifier for an entry within Oracle Internet Directory. The value for this attribute is automatically generated when an entry is created and remains constant, even if an entry is moved.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.37

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

orclGUName

Description
The DN of the guest user account for Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.11

Other
Single-valued attribute.

orclGUPassword

Description
Password for the guest user account in Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.1.1.12

Other
Single-valued attribute.

orclHIQSchedule

Description
The interval, in minutes, at which the directory replication server repeats the change application process.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.98

Other
Single-valued attribute.

DSA operational attribute.

orclHireDate

Description
Specifies the date on which a user was hired by the organization.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.308

Other
Single-valued attribute.

orclHostedCreditCardExpireDate

Description
The credit card expiration date for a subscriber.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.338

Other
Single-valued attribute.

orclHostedCreditCardNumber

Description
The credit card number for a subscriber.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.337

Other
Single-valued attribute.

orclHostedCreditCardType

Description
The credit card type for a subscriber.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.336

Other
Single-valued attribute.

orclHostedDunsNumber

Description
The DUNS number of a business subscriber. DUNS (Data Universal Numbering System) is a unique nine character company identification number issued by Dun and Bradstreet Corporation used to identify a US corporate entity.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.334

Other
Single-valued attribute.

orclHostedPaymentTerm

Description
Payment terms for a subscriber account.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.335

Other
Single-valued attribute.

orclHostname

Description
The host name of the Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.41

Other
Single-valued attribute.

orclIdleConn

Description
The number of open connections that are currently inactive. Oracle Internet Directory tracks the idle connections for server manageability statistics.

Syntax
1.3.6.1.4.1.1466.115.121.1.27

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.151

Other
Single-valued attribute.

orclIdleThreads

Description
The number of application process threads that are currently inactive. Oracle Internet Directory tracks the idle threads for server manageability statistics.

Syntax
1.3.6.1.4.1.1466.115.121.1.27

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.141

Other
Single-valued attribute.

orclIncludedNamingContexts

Description
The naming context included in a partial replica. For each naming context object, you can specify only one unique subtree.

In partial replication, except for subtrees listed in the orclExcludedNamingContexts attribute, all subtrees in the specified included naming context are replicated.

Only LDAP-based replication agreements respect this attribute to define one or more partial replicas. If this attribute contains any values in an Advanced Replication-based replication agreement, then it is ignored.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.819

Other
Single-valued attribute.

DSA operational attribute.

orclIndexedAttribute

Description
Attributes that are indexed in the Oracle Internet Directory catalog.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.49

orclIndexHints

Description
Whether or not index hints are used. Index hints are used to specify which index or indexes you want used when a query runs.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.409

Other
Single-valued attribute.

orclInitialServerMemSize

Description
The memory size of the Oracle Internet Directory server at start up.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.147

Other
Single-valued attribute.

orclInterval

Description
Time interval in seconds between executions of Oracle Directory Integration Platform profiles.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.9.1.8

orclIpAddress

Description
The IP address of the Oracle Internet Directory server host.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.186

orclIsEnabled

Description
Whether or not a user or service subscriber is enabled in Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.316

Other
Single-valued attribute.

orclIsVisible

Description
This attribute is used to determine if users or groups will be visible to applications managed by Oracle Delegated Administration Services, such as OracleAS Portal. OracleAS Single Sign-On does not use this attribute. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.303

Other
Single-valued attribute.

orclLastAppliedChangeNumber

Description
For Oracle Directory Integration Platform export operations, the last change from Oracle Internet Directory that was applied to the connected directory. The default value is 0. If you have used the Oracle Directory Integration Platform Assistant to bootstrap the connected directory, then this value is set automatically at the end of the bootstrapping process. This is valid only in the export profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.69

Other
Single-valued attribute.

orclLDAPConnKeepALive

Description
For replication, whether or not to keep the LDAP connection to the connected directory alive due to activity. If not set Oracle Internet Directory will drop inactive connections after a period of time. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.822

Other
Single-valued attribute.

orclLDAPConnTimeout

Description
The number of minutes before Oracle Internet Directory times out and drops an inactive connection.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.194

Other
Single-valued attribute.

orclLDAPInstanceID

Description
The instance number of a particular Oracle Internet Directory server instance.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.125

Other
Single-valued attribute.

orclLDAPProcessID

Description
The process ID of a particular Oracle Internet Directory server instance.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.126

Other
Single-valued attribute.

orclMaidenName

Description
The maiden name of a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.306

orclMappedDN

Description
Holds the required information for generating the mapped identity.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.704

Other
Single-valued attribute.

orclMasterNode

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.1010

Other
Single-valued attribute.

orclMatchDnEnabled

Description

If the base DN of a search request is not found, then the directory server returns the nearest DN that matches the specified base DN. Whether the directory server tries to find the nearest match DN is controlled by this attribute. If set to 1, then match DN processing is enabled. If set to 0, then match DN processing is disabled. The default is 1.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.404

Other

Single-valued attribute.

orclMaxCC

Description

Maximum number of concurrent database connections. The default is 10.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.4

Other

Single-valued attribute.

orclMaxConnInCache

Description

The number of connection DNs whose privileged groups can be cached is controlled by orclMaxConnInCache in the DSA configuration entry. The default value is 25000 identities (connection DNs). Increase the value of orclMaxConnInCache if your installation has more than 25000 users.

> **See Also:** section "Caching of Connection DNs" of Oracle Internet Directory Administrator's Guide for more information.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.605

Other
Single-valued attribute.

orclMaxEntInBER

Description
Stores the maximum allowed BER entry. When searching a subtree, the server does not write to the client until a configured number of entries have been processed. This number is controlled by orclMaxEntInBER in the DSA configuration entry. By default this value is 5. If the entries are larger than 8000 bytes, then reduce this value to 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.604

Other
Single-valued attribute.

orclMaxFDLimitReached

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.156

Other
Single-valued attribute.

orclMaxProcessLimitReached

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.164

Other
Single-valued attribute.

orclMaxTcpIdleConnTime

Description
Maximum TCP connection time in minutes for an idle connection to be recorded as idle. The default value is 120 minutes (2 hours). The value of this attribute should be less than that of the DSA configuration set attribute orclLDAPConnTimeout.

This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.196

Other
Single-valued attribute.

orclMemAllocError

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.162

Other
Single-valued attribute.

orclNetDescName

Description
The DN of an Oracle Net Service description entry. Oracle Net directory naming allows net service names to be stored in and retrieved from Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.3.1.12

Other
Single-valued attribute.

orclNetDescString

Description
The description string for an Oracle Net Service. For example:

(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = hostname)(PORT =1521))) (CONNECT_DATA = (SID = ORCL)))

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.3.1.13

Other
Single-valued attribute.

orclNonSSLPort

Description
The non-SSL LDAP listening port for Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.102

Other
Single-valued attribute.

orclNormDN

Description
Identifies the normalized DN of an entry.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.1000

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

orclNWCongested

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.160

Other
Single-valued attribute.

orclNwrwTimeout

Description
Stores the network read/write time out. When an LDAP client initiates an operation, then does not respond to the server for a configured number of seconds, the server closes the connection. The number of seconds is controled by the attribute orclnwrwtimeout in the DSA configuration entry. The default is 300 seconds.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.603

Other
Single-valued attribute.

orclNwUnavailable

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.159

Other
Single-valued attribute.

orclObjectGUID

Description
Stores Microsoft Active Directory's `OBJECTGUID` attribute value for users and groups migrated to Oracle Internet Directory from Active Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.901

Other
Single-valued attribute.

orclObjectSID

Description
Stores Microsoft Active Directory's `OBJECTSID` attribute value for users and groups migrated to Oracle Internet Directory from Active Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.902

Other
Single-valued attribute.

orclODIPAgent

Description
The DN of a provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.9.1.6

orclODIPAgentConfigInfo

Description
Any configuration information that you want the connector to store in Oracle Internet Directory. It is passed by the Directory Integration Platform server to the connector at time of connector invocation. The information is stored as an attribute and the Directory Integration Platform server does not have any knowledge of its content. When the connector is scheduled for execution, the value of the attribute is stored in the file, *`ORACLE_HOME`*`/ldap/odi/conf/profile_name.cfg` that can be processed by the connector.

Upload the file by using either the Directory Integration Platform Assistant. See "dipassistant" on page 6-1 for more information. Do this for both import and export agents.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.24

orclODIPAgentControl

Description
Whether a synchronization profile is enabled or disabled. Valid values are ENABLE or DISABLE. The default is DISABLE.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.3

Other
Single-valued attribute.

orclODIPAgentExeCommand

Description
The executable name and argument list used by the Directory Integration Platform server to invoke a connector. It can be passed as a command-line argument when the connector is invoked. For example, here is a command to invoke the Oracle HR connector:

```
odihragent OracleHRAgent connect=hrdb login=%orclodipConDirAccessAccount
pass=%orclodipConDirAccessPassword date=%orclODIPLastSuccessfulExecutionTime
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.21

Other
Single-valued attribute.

orclODIPAgentHostName

Description
The host name of the Oracle Directory Integration Platform server where the synchronization profile is run.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.5

Other
Single-valued attribute.

orclODIPAgentName

Description
The name of a third-party synchronization profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.1

Other
Single-valued attribute.

orclODIPAgentPassword

Description
Password that the synchronization profile uses to bind to the directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.4

Other
Single-valued attribute.

orclODIPApplicationName

Description
The name of an application to which a provisioning subscription belongs.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.9.1.7

orclODIPApplicationsLocation

Description
The DN of the application to which a provisioning subscription belongs.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.918

Other
Single-valued attribute.

orclODIPAttributeMappingRules

Description
Attribute for storing the mapping rules used by a synchronization profile. Store the mapping rules in a file by using the Directory Integration Platform Assistant. See "dipassistant" on page 6-1 and the *Oracle Identity Management Integration Guide* for more information about mapping rules.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.41

orclODIPBootStrapStatus

Description
The bootstrap status of a synchronization profile (the initial migration of data between a connected directory and Oracle Internet Directory).

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.101

Other
Single-valued attribute.

orclODIPCommand

Description
The command to invoke a provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.9.1.5

orclODIPConDirAccessAccount

Description
Valid user account in the connected directory to be used by the connector for synchronization. The value is specific to the connected directory with which you are integrating. For instance, for the SunONE synchronization connector, it is the valid bind DN in the SunONE Directory Server. For the Human Resources Connector, it is a valid user identifier in the Oracle Human Resources database. For other connectors, it can be passed as a command-line argument when the connector is invoked.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.22

Other
Single-valued attribute.

orclODIPConDirAccessPassword

Description
Password to be used by the user specified in the orclODIPConDirAccessAccount attribute to connect to the connected directory. The value is specific to the third-party directory with which you are integrating. For instance, for the SunONE synchronization connector, it is the valid bind password in the SunONE Directory Server. For the Human Resources Agent, it is the Oracle Human Resources database password.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.23

orclODIPConDirLastAppliedChgNum

Description
For Oracle Directory Integration Platform import operations, the last change from the connected directory that was applied to Oracle Internet Directory. The default value is 0. If you have used the Directory Integration Platform Assistant to bootstrap the connected directory, then this value is set automatically. See "dipassistant" on page 6-1 for more information about the bootstrap operation. This is valid only in the import profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.65

Other
Single-valued attribute.

orclODIPConDirMatchingFilter

Description
This attribute specifies the filter to apply to the third-party directory change log. It is used in the Oracle Directory Integration Platform import profile. The filter must be set in the import profile when both the import and export integration profiles are enabled, as follows:

```
Modifiersname != connected_directory_account
```

This prevents the same change from being exchanged between the two directories indefinitely. To avoid confusion, make this account specific to synchronization.

See Also: Oracle MetaLink Note 280474.1, "Setting Up Filtering in a DIP Synchronization Profile" available at Oracle MetaLink at http://metalink.oracle.com/.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.42

orclODIPConDirURL

Description
Connection string required to connect to the third-party connected directory. This value refers to the host name and port number as *host:port:*[*sslmode*].

To connect by using SSL, enter *host:port:*1.

Make sure the certificate to connect to the directory is stored in the wallet, the location of which is specified in the file `odi.properties`.

Note: To connect to SunONE Directory Server by using SSL, the server certificate needs to be loaded into the wallet.

See Also: The chapter on Oracle Wallet Manager in *Oracle Advanced Security Administrator's Guide*.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.25

Other
Single-valued attribute.

orclODIPConfigDNs

Description
Stores the DNs of integration profiles for a particular configuration set in Oracle Directory Integration Platform.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.72

orclODIPConfigRefreshFlag

Description
Stores a flag which indicates whether any integration profiles have been added, deleted, or modified. Used in association with a configuration set.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.71

Other
Single-valued attribute.

orclODIPDbConnectInfo

Description
The connection string for the database of a provisioning profile subscriber. The format of the string is `host:port:sid:username:password`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.9.1.2

orclODIPEncryptedAttrKey

Description
Stores a key which is used to encrypt and decrypt sensitive data that is transmitted by the Oracle directory integration platform server to other applications.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.215

Other
Single-valued attribute.

orclODIPEventFilter

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.433

orclODIPEventSubscriptions

Description
Store configuration information for events to which a provisioned-integrated application subscribes.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID
2.16.840.1.113894.9.1.1

orclODIPFilterAttrCriteria

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.605

Other
Single-valued attribute.

orclODIPInstancesLocation

Description
Identifies the location in the directory that stores information about instances of the Oracle directory integration platform server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.913

Other
Single-valued attribute.

orclODIPInstanceStatus

Description
Stores a flag that indicates whether an instance of the Oracle directory integration platform server should continue running or shut down. This flag provides a means of communication between the OID Monitor, OID Control, and the Oracle directory integration platform server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.76

Other
Single-valued attribute.

orclODIPInterfaceType

Description
The data format or protocol used in synchronization with a third-party directory. Supported values are:

- LDIF—Import or export from a LDIF File.
- Tagged—Import or export from a tagged file—a proprietary format supported by the Oracle Directory Integration Platform server, similar to LDIF format.
- LDAP—Import from or export to an LDAP-compliant directory.
- DB —Import from or export to an Oracle Database directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.28

Other
Single-valued attribute.

orclODIPLastExecutionTime

Description
Status attribute set to the last time the integration profile was executed by the Oracle Directory Integration Platform server. Its format is `dd-mon-yyyy hh:mm:ss`, where `hh` is the time of day in 24-hour format. This attribute is initialized during profile creation.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.61

Other
Single-valued attribute.

orclODIPLastSuccessfulExecutionTime

Description
Status attribute set to the last time the integration profile was executed successfully by the Oracle Directory Integration Platform server. Its format is `dd-mon-yyyy hh:mm:ss`, where `hh` is the time of day in 24-hour format. This attribute is initialized during profile creation.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.62

Other
Single-valued attribute.

orclODIPMustAttrCriteria

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.603

Other
Single-valued attribute.

orclODIPObjectCriteria

Description
Used in an object definition to identify and classify a particular type of object.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.602

orclODIPObjectDefnLocation

Description
Identifies the location of the various object definitions used by the Oracle directory integration platform server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.917

Other
Single-valued attribute.

orclODIPObjectEvents

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.432

orclODIPObjectName

Description
Used in an object definition to store the name of an object.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.601

Other
Single-valued attribute.

orclODIPObjectSyncBase

Description
The search base in the directory for an object associated with an Oracle Directory Integration Platform synchronization profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.431

orclODIPOIDMatchingFilter

Description
In export profiles, this attribute specifies the filter to apply to the Oracle Internet Directory change log container. It is used in the export profile. It must be set in the export profile when both the import and export integration profiles are enabled, as in the following example:

```
Modifiersname !=orclodipagentname=iPlanetImport,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
```

This prevents the same change from being exchanged between the two directories indefinitely.

In import profiles, this attribute specifies a key for mapping entries between Oracle Internet Directory and the connected directory. This is useful when the DN cannot be used as the key.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.43

orclODIPOperationMode

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.430

orclODIPOptAttrCriteria

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.604

Other
Single-valued attribute.

orclODIPPluginAddInfo

Description
Additional information that may be needed by an Oracle Directory Integration Platform connector plug-in.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.264

Other
Single-valued attribute.

orclODIPPluginConfigInfo

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.261

Other
Single-valued attribute.

orclODIPPluginEvents

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.265

orclODIPPluginExecData

Description
The Oracle Directory Integration Platform connector plug-in executable data, which is typically a JAR file.

Syntax
1.3.6.1.4.1.1466.115.121.1.5 (Binary Data)

Matching Rule
N/A

Object ID
2.16.840.1.113894.8.1.262

orclODIPPluginExecName

Description
The fully qualified name of the Oracle Directory Integration Platform connector plug-in executable, which is typically a Java class.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.263

Other
Single-valued attribute.

orclODIPProfileDataLocation

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.914

Other
Single-valued attribute.

orclODIPProfileDebugLevel

Description
The debugging level for an Oracle Directory Integration Platform synchronization profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.251

Other
Single-valued attribute.

orclODIPProfileExecGroupID

Description
Associates a group number with a particular provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.250

Other
Single-valued attribute.

orclODIPProfileInterfaceAdditionalInformation

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.223

orclODIPProfileInterfaceConnectInformation

Description
Contains information that is used by the Oracle directory integration platform server on how to connect to a provisioning-integrated application for event propagation.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.222

Other
Single-valued attribute.

orclODIPProfileInterfaceName

Description

Contains a provisioning-integrated application's interface name, which is used by the Oracle directory integration platform server for event propagation. The value assigned to this attribute depends on the interface type.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.220

Other

Single-valued attribute.

orclODIPProfileInterfaceType

Description

Specifies the type of interface to which events will be propagated by the Oracle directory integration platform server. Valid values for this attribute are PLSQL or JAVA.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.221

Other

Single-valued attribute.

orclODIPProfileInterfaceVersion

Description

Specifies the provisioning profile version to which events will be propagated by the Oracle directory integration platform server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.224

Other
Single-valued attribute.

orclODIPProfileLastAppliedAppEventID

Description
Contains the number of the last event that was generated by a provisioning-integration application and updated in Oracle Internet Directory by the Oracle directory integration platform server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.234

Other
Single-valued attribute.

orclODIPProfileLastProcessingTime

Description
The last time the Oracle Directory Integration Platform synchronization profile was executed.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.232

Other
Single-valued attribute.

orclODIPProfileLastSuccessfulProcessingTime

Description
The last time the Oracle Directory Integration Platform synchronization profile was successfully executed.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.233

Other
Single-valued attribute.

orclODIPProfileMaxErrors

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.214

Other
Single-valued attribute.

orclODIPProfileMaxEventsPerInvocation

Description
Specifies the maximum number of events that the Oracle directory integration platform server packages and sends to an application during one invocation of a provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.212

Other
Single-valued attribute.

orclODIPProfileMaxEventsPerSchedule

Description
Specifies the maximum number of events that the Oracle directory integration platform server sends to an application during one execution of a provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.213

Other
Single-valued attribute.

orclODIPProfileMaxRetries

Description
The maximum number of times an Oracle Directory Integration Platform profile is retried in the event of an error.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.211

Other
Single-valued attribute.

orclODIPProfileName

Description
The name of the Oracle Directory Integration Platform profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.201

Other
Single-valued attribute.

orclODIPProfileProcessingErrors

Description
Contains errors raised during event propagation by the Oracle directory integration platform server for a particular provisioning-integrated application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.231

orclODIPProfileProcessingStatus

Description
Contains the Oracle directory integration platform server's event propagation status for a particular provisioning-integrated application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.230

Other
Single-valued attribute.

orclODIPProfileProvSubscriptionMode

Description
The subscription mode for a provisioning profile: INBOUND, OUTBOUND, or BOTH.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.408

orclODIPProfileSchedule

Description
The number of seconds between executions of an Oracle Directory Integration Platform profile. The default is 3600, which means the profile is scheduled to run every hour.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.210

Other
Single-valued attribute.

orclODIPProfileStatusUpdate

Description
Indicates whether the Oracle directory integration platform server should perform a provisioning profile status update while propagating events to a provisioning-integrated application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.610

Other
Single-valued attribute.

orclODIPProvEventCriteria

Description
Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to identify a particular type of event.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.503

orclODIPProvEventLDAPChangeType

Description
Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to indicate what type of operation in LDAP (add, modify, delete) can cause some type of event.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.502

orclODIPProvEventObjectType

Description
Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to indicate the type of object (i.e whether it is a USER or a GROUP and so forth) based on other qualifying criteria.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.501

Other
Single-valued attribute.

orclODIPProvEventRule

Description
Stores the XML-based rule definitions used by the Oracle directory integration platform server to convert changes in Oracle Internet Directory into events before propagating them to a provisioning-integrated application.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.607

Other
Single-valued attribute.

orclODIPProvEventRuleDTD

Description
Stores the XML DTD for event rule definitions used by the Oracle directory integration platform server to understand and parse event rule definitions.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.606

Other
Single-valued attribute.

orclODIPProvInterfaceFilter

Description
Used with version 3.0 provisioning profiles to identify and classify an object based on the entry's object class. This attribute is used in the object definitions stored in Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.609

orclODIPProvInterfaceProcessor

Description
Used by the Oracle directory integration platform server to identify the Java classes to use for reading and writing events from and to provisioning-integration applications and for processing event propagation results. The default configurations in this attribute should not be changed.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.608

Other
Single-valued attribute.

orclODIPProvisioningAppGUID

Description
The global unique identifier for the application entry associated with a provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.402

Other
Single-valued attribute.

orclODIPProvisioningAppName

Description
The distinguished name (DN) of the application to which the provisioning subscription belongs. The combination of the application name and organization name uniquely identifies a provisioning profile, for example, Email.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.401

Other
Single-valued attribute.

orclODIPProvisioningEventMappingRules

Description
The event mapping rule maps the object type received from the application (using an optional filter condition) to a domain in Oracle Internet Directory. An inbound provisioning profile can have multiple mapping rules defined.

The following example shows a sample mapping rule value. The rule shows that a user object (`USER`) whose locality attribute equals US (`l=US`) should be mapped to the domain `l=US,cn=users,dc=company,dc=com`.

```
USER:l=US:l=US,cn=users,dc=company,dc=com
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.406

orclODIPProvisioningEventPermittedOperations

Description
Defines the types of events that the application is allowed to send to the Oracle Directory Integration Platform service. An inbound provisioning profile can have multiple permitted operations defined.

For example, if you wanted to permit the application to send events whenever a user object was added or deleted, or when certain attributes were modified, you would have three permitted operation values such as this:

```
USER:dc=mycompany,dc=com:ADD(*)
USER:dc=mycompany,dc=com:MODIFY(cn,sn,mail,password)
USER:dc=mycompany,dc=com:DELETE(*)
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.407

orclODIPProvisioningEventSubscription

Description
Defines the types of events that the Oracle Directory Integration Platform service should send to the application. An outbound provisioning profile can have multiple event subscriptions defined.

For example, if you wanted the directory integration server to send events to the application whenever a user or group object was added or deleted, you would have four event subscription values such as this:

```
GROUP:dc=mycompany,dc=com:ADD(*)
GROUP:dc=mycompany,dc=com:DELETE(*)
USER:dc=mycompany,dc=com:ADD(*)
USER:dc=mycompany,dc=com:DELETE(*)
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.405

orclODIPProvisioningOrgGUID

Description
The global unique identifier for the organization entry associated with a provisioning profile.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.404

Other
Single-valued attribute.

orclODIPProvisioningOrgName

Description
The distinguished name (DN) of the organization to which the provisioning subscription belongs, for example `dc=company,dc=com`. The combination of the

application DN and organization DN uniquely identifies a provisioning profile. Defaults value is the DN of the default identity management realm.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.403

Other
Single-valued attribute.

orclODIPProvProfileLocation

Description
Contains the DN of the directory container that stores provisioning profiles.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.916

Other
Single-valued attribute.

orclODIPRootLocation

Description
Refers to the root location in the directory tree where the Oracle Directory Integration Platform configuration is stored.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.912

Other
Single-valued attribute.

orclODIPSchedulingInterval

Description
Time interval in seconds after which a connected directory is synchronized with Oracle Internet Directory. The default is 600.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.6

Other
Single-valued attribute.

orclODIPSchemaVersion

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.911

Other
Single-valued attribute.

orclODIPSearchCountLimit

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.511

Other
Single-valued attribute.

orclODIPSearchTimeLimit

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.512

Other
Single-valued attribute.

orclODIPServerCommitSize

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.515

Other
Single-valued attribute.

orclODIPServerConfigLocation

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.919

Other
Single-valued attribute.

orclODIPServerDebugLevel

Description
The number that corresponds to the debugging level for the Oracle Directory Integration Platform server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.516

Other
Single-valued attribute.

orclODIPServerRefreshIntvl

Description
The number of minutes between server refreshes for any changes in Oracle Directory Integration Platform profiles. If not specified, the default of 2 is used.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.514

Other
Single-valued attribute.

orclODIPServerSSLMode

Description
The number of the corresponding SSL mode. The default is 0. The modes are as follows:

- 0 — SSL is not used.

- 1 — SSL is used for encryption only, not for authentication.
- 2 — SSL is used for one-way authentication. With this mode you must also specify the complete path and file name of the server's Oracle Wallet.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.513

Other
Single-valued attribute.

orclODIPServerWalletLoc

Description
The complete path and file name of the Oracle Directory Integration Platform server's Oracle Wallet.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.517

Other
Single-valued attribute.

orclODIPSynchronizationErrors

Description
Messages explaining the errors if the last execution of the synchronization profile failed. This attribute is updated by Oracle Directory Integration Platform server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.64

orclODIPSynchronizationMode

Description
Direction of synchronization between Oracle Internet Directory and the connected directory. Allowed values are: IMPORT or EXPORT.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.2

Other
Single-valued attribute.

orclODIPSynchronizationStatus

Description
Status of the last execution of a synchronization profile: SUCCESS or FAILURE. Initially, this attribute has the value YET TO BE EXECUTED.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.63

Other
Single-valued attribute.

orclODIPSyncProfileLocation

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.915

Other
Single-valued attribute.

orclODIPSyncRetryCount

Description
Maximum number of times Oracle Directory Integration Platform server tries to run the third-party directory connector in the event of a failure. The default is 5.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.7

Other
Single-valued attribute.

orclOpAbandoned

Description
Specifies the number of abandoned LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.168

Other
Single-valued attribute.

orclOpCompleted

Description
Specifies the number of completed LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.166

Other
Single-valued attribute.

orclOpenConn

Description
Specifies the number of open connections to the Oracle Internet Directory server, including client LDAP connections and database connections.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.149

Other
Single-valued attribute.

orclOpFailed

Description
Specifies the number of failed LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.190

Other
Single-valued attribute.

orclOpInitiated

Description
Specifies the number of initiated LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.165

Other
Single-valued attribute.

orclOpLatency

Description
Stores operation latency.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.127

Other
Single-valued attribute.

orclOpPending

Description
Specifies the number of pending LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.167

Other
Single-valued attribute.

orclOpResult

Description
Stores the operation result.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.64

orclOpSucceeded

Description
Specifies the number of successful LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.189

Other
Single-valued attribute.

orclOpTimedOut

Description
Specifies the number of LDAP search operations that timed out.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.169

Other
Single-valued attribute.

orclORA28error

Description
Specifies the number of ORA-28 errors encountered by Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.182

Other
Single-valued attribute.

orclORA3113error

Description
Specifies the number of ORA-3113 errors encountered by Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.157

Other
Single-valued attribute.

orclORA3114error

Description
Specifies the number of ORA-3114 errors encountered by Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.158

Other
Single-valued attribute.

orclOracleHome

Description
The *ORACLE_HOME* location of an Oracle service.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
N/A

Object ID
2.16.840.1.113894.7.1.2

Other
Single-valued attribute.

orclOwnerGUID

Description
The global unique identifier of the user who owns an application or resource.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.358

orclPassword

Description
Identifies an Oracle-specific password for custom authentication schemes like O3Logon for the database server.

Syntax
1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule
caseExactMatch

Object ID
2.16.840.1.113894.7.1.13

orclPasswordAttribute

Description
Specifies the password value to access the resource.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.353

Other
Single-valued attribute.

orclPasswordHint

Description
Specifies the password hint to be displayed when users forget their password.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.314

Other
Single-valued attribute.

orclPasswordHintAnswer

Description
The answer related to the password hint question stored in orclPasswordHint.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.315

Other
Single-valued attribute.

> **Note:** `orclPasswordHintAnswer` is hashed using the `SHA-1` algorithm. The hexadecimal value of this is `Base64` encoded.
>
> Oracle Internet Directory hashes the value only if it is provided as plaintext. Prehashed values are not hashed again.

orclPasswordVerifier

Description
Attribute for storing a password to an Oracle component when that password is different from that used to authenticate the user to the directory, namely, userPassword. The value in this attribute is not synchronized with that in the userPassword attribute.

Like authPassword, this attribute is multivalued and can contain all the other verifiers that different applications use for this user's clear text password.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
2.16.840.1.113894.1.1.210

orclPilotMode

Description
Whether to BEGIN or END pilot mode for a replica.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.824

Other
Single-valued attribute.

orclPKCS12Hint

Description
Password hint for the user's PKCS12 private key store.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.11

orclPKIMatchingRule

Description
This is used to specify the matching rule for mapping a user's PKI certificate DN to the user's entry DN in Oracle Internet Directory. The following matching rule values are allowed:

- 0 - Exact match. The PKI certificate DN must match the user entry DN.
- 1 - Certificate search. Check to see if the user has a PKI certificate provisioned into Oracle Internet Directory.
- 2 - A combination of exact match and certificate search. If the exact match fails, then a certificate search is performed.
- 3 - Mapping rule only. Use a mapping rule to map user PKI certificate DNs to Oracle Internet Directory DNs.
- 4 - Try in order: 1 (mapping rule), 2 (certificate search), 3 (exact match).

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.703

Other
Single-valued attribute.

orclPKINextUpdate

Description
The universal time when the certificate revocation list (CRL) should be updated.

Syntax
1.3.6.1.4.1.1466.115.121.1.53 (UTC Time)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.2.1.300.1

orclPKIValMecAttr

Description
Contains the certificate validation mechanism supported. Currently, only validation with crls is supported, hence the value of this attribute will be CRL.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.2.1.300.2

orclPluginAttributeList

Description
A semicolon-separated attribute name list that controls whether the plug-in takes effect. If the target attribute is included in the list, the plug-in is invoked.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.563

Other
Single-valued attribute.

orclPluginCheckEntryExist

Description
If enabled, then the Plug-in will be invoked when the base entry does not exist. Allowed values are 0 (disabled) or 1 (enabled).

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.569

Other
Single-valued attribute.

orclPluginEnable

Description
Whether or not a plug-in is enabled or disabled. Allowed values are 0 (disabled) or 1 (enabled). The default is 0 (disabled).

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.554

Other
Single-valued attribute.

orclPluginEntryProperties

Description
An LDAP search filter that specifies entry criteria that will cause the plug-in to not be invoked. For example, if the following filter is used, the plug-in will not be invoked if the target entry has `objectclass` equal to `inetorgperson` and `sn` equal to `Cezanne`.

```
(&(objectclass=inetorgperson)(sn=Cezanne))
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.568

Other
Single-valued attribute.

orclPluginIsReplace

Description
For plug-ins that use WHEN timing only. 0 is disabled (default). 1 is enabled. This attribute can be set to enabled only if the orclPluginLDAPOperation attribute value is `ldapbind`, `ldapcompare`, or `ldapmodify`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.559

Other
Single-valued attribute.

orclPluginBinaryFlexfield

Description
Custom binary information (Java only)

Syntax
1.3.6.1.4.1.1466.115.121.1.5

Object ID
2.16.840.1.113894.1.1.574

Other
Single-valued attribute.

orclPluginFlexfield

Description
Custom text information (Java only). To indicate a subtype, specify `orclPluginFlexfield; subtypename`, for example, `orclPluginFlexfield; minPwdLength: 8`

Syntax
1.3.6.1.4.1.1466.115.121.1.15

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.573

Other
Single-Valued attribute.

orclPluginSecuredFlexfield

Description

Syntax
1.3.6.1.4.1.1466.115.121.1.15

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.577

Other
Single-Valued attribute.

orclPluginKind

Description
The kind of plug-in. PL/SQL is the only allowed value.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.562

Other
Single-valued attribute.

orclPluginLDAPOperation

Description
The LDAP operation that this plug-in supplements. Allowed values are:

- ldapcompare
- ldapmodify
- ldapbind
- ldapadd
- ldapdelete
- ldapsearch

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.557

Other
Single-valued attribute.

orclPluginName

Description
The plug-in package name.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.552

Other
Single-valued attribute.

orclPluginPort

Description
The port that the plug-in is using.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.566

Other
Single-valued attribute.

orclPluginRequestGroup

Description

A semicolon-separated group list that controls if the plug-in takes effect. You can use this group to specify who can actually invoke the plug-in. For example, if you specify `orclpluginrequestgroup:cn=security,cn=groups,dc=oracle,dc=com`, when you register the plug-in, then the plug-in will not be invoked unless the ldap request comes from the person who belongs to the group `cn=security,cn=groups,dc=oracle,dc=com`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.564

Other

Single-valued attribute.

orclPluginRequestNegGroup

Description

A semicolon-separated group list that controls if the plug-in takes effect. You can use this group to specify who cannot invoke the plug-in. For example, if you specify `orclpluginrequestneggroup: cn=security,cn=groups,dc=oracle,dc=com`, when you register the plug-in, then the plug-in will not be invoked if the ldap request comes from the person who belongs to the group `cn=security,cn=groups,dc=oracle,dc=com`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.571

Other

Single-valued attribute.

orclPluginResultCode

Description

An integer value to specify the LDAP result code. If this value is specified, then the plug-in will be invoked only if the ldap operation is in that result code scenario. This only applies if the value for the orclPluginTiming attribute is `POST`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.565

Other
Single-valued attribute.

orclPluginSASLCallBack

Description
Controls the type of bind used when the LDAP_PLUGIN package connects back to the same Oracle Internet Directory server.

- 1= SASL bind (default).
- 0= Simple bind.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.572

Other
Single-valued attribute.

orclPluginSearchNotFound

Description
This only applies if the value for the orclPluginTiming attribute is `PRE`. Brings in the external entries if the entry is not found in Oracle Internet Directory. Provides additional plug-in invocation checking and ensures that the plug-in will only be invoked when the entry is not present in Oracle Internet Directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.570

Other
Single-valued attribute.

orclPluginShareLibLocation

Description
File location of the program libraries for the plug-in. If this value is not present, then the Oracle Internet Directory server assumes the plug-in language is PL/SQL.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.556

Other
Single-valued attribute.

orclPluginSubscriberDNList

Description
A semicolon-separated DN list that controls if the plug-in takes effect. For example:

```
dc=COM,c=us;dc=us,dc=oracle,dc=com;dc=org,dc=us;o=IMC,c=US
```

If the target DN of an LDAP operation is included in the list, then the plug-in is invoked.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.561

Other
Single-valued attribute.

orclPluginTiming

Description
Specifies when the plug-in is to be invoked in relation to the LDAP operation it supplements. The following values are allowed:

- PRE

- WHEN
- POST

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.558

Other
Single-valued attribute.

orclPluginType

Description
Valid value is `operational` — Operational plug-ins augment existing LDAP operations. The work they perform depends on whether they execute before, after, or in addition to normal directory server operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.553

Other
Single-valued attribute.

orclPluginVersion

Description
The supported version number of the plug-in.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.555

Other
Single-valued attribute.

orclPrName

Description
Stores a process name.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.55

Other
Single-valued attribute.

orclProductVersion

Description
Identifies the product version.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.6

orclPrPassword

Description
Contains a password for the OID proxy user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.56

Other
Single-valued attribute.

orclPurgeBase

Description
The base DN in the directory information tree (DIT) where the garbage collection task is applied. This attribute value is reserved for each garbage collector and it must not be modified. Defaults to the RDN of the garbage collector configuration entry DN.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.805

Other
Single-valued attribute.

orclPurgeDebug

Description
Flag to enable (1) or disable (0) collection of debugging messages. Default value is 0.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.810

Other
Single-valued attribute.

orclPurgeEnable

Description
Flag to enable (1) or disable (0) this garbage collector. Default value is 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.808

Other
Single-valued attribute.

orclPurgeFileLoc

Description
Absolute file directory where the garbage collection log file is saved. Default value is . (period - the current directory).

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.812

Other
Single-valued attribute.

orclPurgeFileName

Description
The file name of the garbage collection log file. Default value is `oidgc001.log`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.811

Other
Single-valued attribute.

orclPurgeFilter

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.803

Other
Single-valued attribute.

orclPurgeInterval

Description
Time interval in hours that the garbage collection job is executed again. This can be measured from either the point in time specified in the orclPurgeStart attribute or from the last time it was run. Default value is 24.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.801

Other
Single-valued attribute.

orclPurgeNow

Description
Every time this attribute is added or modified to a garbage collection entry, then the submitted job is executed immediately.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.809

Other
Single-valued attribute.

orclPurgePackage

Description
Specifies the package name for purging directory objects.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.804

Other
Single-valued attribute.

orclPurgeSchedule

Description
Specifies the schedule for purging directory objects.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.24

Other
Single-valued attribute.

DSA operational attribute.

orclPurgeStart

Description
The time when the garbage collector starts to run. The format is `yyyymmddhhmmss`. Default value is 12:00 a.m. of the day Oracle Internet Directory is installed.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.813

Other
Single-valued attribute.

orclPurgeTargetAge

Description
This attribute enables time-based purging of change log records. Set this to the number of hours after which old change logs will be purged. Time-based purging respects the change status of replication, but not the change status of other consumers. When time-based purging is enabled, the change log garbage collector purges all change logs that are not needed by replication and that are at least the specified number of hours old.

The default behavior is change number-based purging, meaning this attribute is NULL or set to a value less than zero. Change number-based purging respects the change status of all change log consumers. That is, it does not purge change logs unless they have been consumed by all consumers. In addition, it does not purge change logs until they are 10 days old.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.800

Other
Single-valued attribute.

orclPurgeTranSize

Description
The number of objects to be purged in one commit transaction. The default value is 1000.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.802

Other
Single-valued attribute.

orclPwdAccountUnlock

Description
It allows a user with the appropriate admininstration rights and priviledges to unlock an already locked account. However, it doesn't necessarily imply that the user affected (that is, who's account was locked) can unlock it by changing this attribute.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.203

Other
Single-valued attribute.

orclPwdAllowHashCompare

Description
Whether or not to allow password validations by comparing the hash values of encrypted passwords. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.218

Other
Single-valued attribute.

orclPwdAlphaNumeric

Description
Number of numeric characters required in a password. The default value is 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.205

Other
Single-valued attribute.

orclPwdEncryptionEnable

Description
If the value is TRUE, then the user password is stored in reversible encrypted form. If the value is FALSE, then the user password is stored in plain text.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.215

Other
Single-valued attribute.

orclPwdIllegalValues

Description
Lists the common words and attribute types whose values cannot be used as a valid password. By default, all words are acceptable password values.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{1024} (Directory String, 1024 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.204

orclPwdIPAccountLockedTime

Description
The time when a user account was locked for a specific IP address.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.211

Other
Directory operational attribute.

Not user modifiable.

orclPwdIPFailureTime

Description
The time of a password failure.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.212

Other
Directory operational attribute.

Not user modifiable.

orclPwdIPLockout

Description
Whether or not to enable account lockouts for a specific IP address. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.200

Other
Single-valued attribute.

orclPwdIPLockoutDuration

Description
The number of seconds you want to enforce account lockout for a specific IP address. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.201

Other
Single-valued attribute.

orclPwdIPMaxFailure

Description
The maximum number of failed logins from a specific IP address after which the account is locked.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.202

Other
Single-valued attribute.

orclPwdPolicyEnable

Description
Whether to enable (TRUE) or disable (FALSE) the password policy.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.213

Other
Single-valued attribute.

orclPwdVerifierParams

Description
This attribute contains the values of different password verifier types, such as:

```
orclpwdverifierparams;authpassword:
orclpwdverifierparams;orclpasswordverifier:
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15{256} (Directory String, 256 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.209

orclQueueDepth

Description
Indicates the queue depth.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.144

Other
Single-valued attribute.

orclQueueLatency

Description
Defines the queue latency.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.145

Other
Single-valued attribute.

orclReadWaitThreads

Description
Specifies the number of Oracle Internet Directory server threads waiting to read from the network.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.142

Other
Single-valued attribute.

orclReplAgreements

Description
The DNs of the replication agreement entries.

Syntax
1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.105

orclReplicaDN

Description
For LDAP-based replication only. The DN of the consumer replica in the replication agreement.

Syntax
1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.817

Other
Single-valued attribute.

orclReplicaID

Description
Naming attribute for the replica subentry. Its value is unique to each directory server node that is initialized at installation. The value of this attribute, assigned during installation, is unique to each directory node, and matches that of the `orclreplicaID` attribute at the root DSE. You cannot modify this value.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.106

Other
Single-valued attribute.

orclReplicaSecondaryURI

Description
Contains the set of `ldapURI` formatted addresses that can be used if the orclReplicaURI values cannot be used.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseExactIA5Match

Object ID
2.16.840.1.113894.1.1.815

orclReplicaState

Description
Defines the state of the replica. Possible values are:

- 0 (boot strapping)
- 1 (online)
- 2 (offline)
- 3 (bootstrap in progress)
- 4 (bootstrap in progress, `cn=oraclecontext` bootstrap has completed)
- 5 (bootstrap completed, failure detected for one or more naming contexts)

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.818

Other
Single-valued attribute.

orclReplicationProtocol

Description
Defines the replication protocol for change propagation to replica. Values are:

- ODS_ASR_1.0 (Advanced Replication-based protocol)
- ODS_LDAP_1.0 (LDAP-based replication)

You cannot modify this attribute.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.29

Other
Single-valued attribute.

orclReplicaType

Description
Defines the type of replica such as read-only or read/write. Possible values are:

- 0 (Read/Write)
- 1 (Read-Only)

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.816

Other
Single-valued attribute.

orclReplicaURI

Description
Contains information in `ldapURI` format that can be used to open a connection to this replica.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseExactIA5Match

Object ID
2.16.840.1.113894.1.1.814

Other
Single-valued attribute.

orclReplicaVersion

Description
Oracle Internet Directory version of the replica.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.820

Other
Single-valued attribute.

orclResourceIdentifier

Description
Stores the resource identifier.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.348

orclResourceName

Description
Specifies the name of the resource for which the connection information is being maintained.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.350

orclResourceTypeName

Description
Specifies the name of the resource, for example, database, XMLPDS, JDBCPDS.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.351

orclResourceViewers

Description
Lists the users or groups of users who can view a Resource Access Descriptor.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.366

orclRevPwd

Description
Reversible encrypted value of the user password. This attribute is generated only if the attribute value of orclPwdEncryptionEnable in the password policy entry is set to 1. This attribute can be queried only by using the SSL one-way and two-way authentication mechanisms. This attribute cannot be queried over non-SSL sessions.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
2.16.840.1.113894.1.1.216

Other
Directory operational attribute.

Not user modifiable.

orclSAMAccountName

Description
Stores the value of Active Directory's `SAMAccountName` attribute. In Oracle Internet Directory, this attribute is defined as a directory string type. However, in Active Directory this attribute cannot accept any special or non-printable characters. If any entry is added in Oracle Internet Directory with this attribute, it can only contain a simple text string or synchronization from Oracle Internet Directory to Active Directory will fail.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.903

Other
Single-valued attribute.

orclSASLAuthenticationMode

Description
SASL authentication mode indicates different modes depending on the type of authentication required and the level of security, such as, auth-only, auth-int, or auth-conf.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.700

Other
Single-valued attribute.

orclSASLCipherChoice

Description
Contains the SASL cipher choice. when the authentication mode is auth-conf, the SASL cipher choices can be 3DES, DES, RC4, RC4-56, or RC4-40.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.702

orclSASLMechanism

Description
Indicates the different kinds of SASL mechanisms supported in the LDAP server. Currently, OID supports SASL-EXTERNAL and DIGEST-MD5.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.701

orclsDumpFlag

Description
Determines whether to generate or stack file (default value 0) or OS level core file (value 1) in case the OID server crashes.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.407

Other
Single-valued attribute.

orclSearchBaseDN

Description
Contains search base information to be used when performing the directory query for identity mapping.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.706

Other
Single-valued attribute.

orclSearchFilter

Description
Contains search filter information to be used when performing the directory query for identity mapping.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.705

Other
Single-valued attribute.

orclSearchScope

Description
Contains search scope information to be used when performing the directory query for identity mapping.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.707

Other
Single-valued attribute.

orclSecondaryUID

Description
Indicates the secondary UID of a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.360

orclSequence

Description
Specifies the sequence number for audit log entires.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.62

orclServerAvgMemGrowth

Description
Specifies the Oracle Internet Directory server process memory growth as a percentage.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.148

Other
Single-valued attribute.

orclServerMode

Description
Specifies if data can be written to the server. Valid values are:

- r (read-only)
- rw (read/write)
- rm (read-modify, that is, to read and modify, but not to add or delete)

The default value is `rw`.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.51

Other
Single-valued attribute.

orclServerProcs

Description
Number of server processes to start. The default for `configset0` is 1. You cannot use a negative value for this attribute.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.364

Other
Single-valued attribute.

orclServiceInstanceLocation

Description
Secifies the DN of an instance of a service.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseExactMatch

Object ID
2.16.840.1.113894.1.1.1102

Other
Single-valued attribute.

orclServiceMember

Description
Identifies all the service instances that are members of a logical service entity.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.1005

orclServiceSubscriptionLocation

Description
Specifies the DN where the list of users subscribed to a service is available.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseExactMatch

Object ID
2.16.840.1.113894.1.1.1100

Other
Single-valued attribute

orclServiceSubType

Description
Identifies the sub-types of a Service e.g. IMAP, SMTP are sub-type of an e-mail service.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1009

Other
Single-valued attribute

orclServiceType

Description
Identifies the type of Service e.g. Email, Calendar, and so forth.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.4

Other
Single-valued attribute

orclSID

Description
Stores the SID.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.5

Other
Single-valued attribute

orclSizeLimit

Description
Maximum number of entries to be returned by a search.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.10

Other
Single-valued attribute

orclSkewedAttribute

Description
Attribute that contains names of attributes which are skewed. A skewed attribute has very different search response times depending on its value. You can uniform the response times for searches for such an attribute by adding it as a value of the orclskewedattribute attribute.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.405

orclSkipRefInSQL

Description
Specifies whether to skip referral in SQL generated for searches. Its default value is 0. Set it to 1 if there are no referral entries in the directory; this will help optimizing search performance.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.410

Other
Single-valued attribute

orclSMSpec

Description
Represents a structural object class that includes common attributes for server manageability object classes.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.185

orclSQLexeFetchLatency

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.132

Other
Single-valued attribute

orclSQLGenReusedParsed

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.134

Other
Single-valued attribute

orclSSLAuthentication

Description
Type of SSL authentication to use for this instance of Oracle Internet Directory server. The default value of 1, specifies no SSL authentication. Different instances can have different values. One-way and two-way SSL authentication requires a wallet. You may use one of the following three values:

- 1 = Neither the client nor the server authenticates itself to the other. No certificates are sent or exchanged. If you selected the SSL Enabled check box on the Credentials tab, and choose this option, then only SSL encryption/decryption will be used.
- 32 = One-way authentication. Only the directory server authenticates itself to the client by sending its certificate to the client.
- 64 = Two-way authentication. Both client and server send certificates to each other.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.13

Other
Single-valued attribute

orclSSLCipherSuite

Description
A cipher suite is a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth. The following cipher suites are supported:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum.

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.19

orclSSLEnable

Description
Flag for enabling or disabling SSL. Use this flag when you use different instances of the same server for either SSL or non-SSL. Allowed values are:

- 0—for non-secure operation only
- 1—for SSL authentication only
- 2— for both non-secure operation and SSL authentication

  The default value is `0`.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.14

Other
Single-valued attribute

orclSSLPort

Description
The default SSL default port for the directory server. Default value is 636. When you run the directory in the secure mode, it listens at default port 636 and accepts only SSL-based TCP/IP connections. (When you run the directory in the normal mode, it listens at default port 389, accepting normal TCP/IP connections.) You might want to change this port when you add multiple LDAP server instances.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.17

Other
Single-valued attribute

orclSSLVersion

Description
SSL version. The default value is 3.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.18

Other
Single-valued attribute

orclSSLWalletURL

Description
Sets the location of the Oracle Wallet. You initially set this value when you create the wallet. If you elect to change the location of the Oracle Wallet, you must change this parameter. You must set the wallet location on both the client and the server. For example, on UNIX, you could set this parameter as follows:

```
file:/home/my_dir/my_wallet
```

On Microsoft Windows, you could set this parameter as follows:

```
file:C:\my_dir\my_wallet
```

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.15

Other
Single-valued attribute

orclStatsDN

Description
Specifies list of user DNs for which to track LDAP operations.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.187

orclStatsFlag

Description
Enable or disable the Oracle Internet Directory Server Manageability framework. To enable, set this to 1. To disable, set it to 0.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.197

Other
Single-valued attribute.

orclStatsLevel

Description
Level of statistics collection for users. There is only one valid value in this release, 1. Specifying this value collects the number of bind and compare operations against the directory and the user who performed each one.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.199

Other
Single-valued attribute.

orclStatsOp

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.188

Other
Single-valued attribute.

orclStatsPeriodicity

Description
Time interval in minutes for gathering server manageability statistics. The default value is 60.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.198

Other
Single-valued attribute.

orclStatus

Description
Depending on the context of the object that it is applied to, like a service, it indicates if the service is available or not.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.9.1.9

orclSUAccountLocked

Description
Determines whether a super user account is locked.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.192

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

orclSubscriberDisable

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.100

Other
Single-valued attribute.

orclSubscriberFullName

Description
Stores the full name of the configured realm.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.333

Other
Single-valued attribute.

orclSubscriberNickNameAttribute

Description
Stores a name of an attribute that holds the unique identifier of a realm.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.302

Other
Single-valued attribute.

orclSubscriberSearchBase

Description
Specifies the DIT node that contains all realms.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.301

orclSubscriberType

Description
Defines the type of realm created.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.331

Other
Single-valued attribute.

orclSuffix

Description
To have the directory server manage part of an LDAP directory, you can specify the highest level parent DNs in the server configuration. These DNs are called suffixes. The server can access all objects in the directory that are below the specified suffix in the directory hierarchy. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.6

Other
Single-valued attribute.

orclSuiteType

Description
Identifies the type of suite e.g ocs, ebiz, and so forth.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.1011

Other
Single-valued attribute.

orclSULoginFailureCount

Description
The number of failed login attempts for the directory super user.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.191

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

orclSUName

Description
The distinguished name of the directory super user account, for example, `cn=orcladmin`.

Syntax
1.3.6.1.4.1.1466.115.121.1.12

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.8

Other
Single-valued attribute.

orclSUPassword

Description
Oracle Internet Directory super user password.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.9

Other
Single-valued attribute.

orclSystemName

Description
Identifies the host name on which a particular instance of a service is running.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.3

Other
Single-valued attribute.

orclTcpConnToClose

Description
Specifies the number of clients for which the Oracle Internet Directory server will close TCP connections.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.153

Other
Single-valued attribute.

orclTcpConnToShutDown

Description
Specifies the number of clients for which the Oracle Internet Directory server will shut down TCP connections.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.152

Other
Single-valued attribute.

orclThreadSpawnFailed

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.154

Other
Single-valued attribute.

orclThreadsPerSupplier

Description
Specifies the number of threads per supplier for the Oracle directory replication server.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.31

Other
Single-valued attribute.

DSA operational attribute.

orclTimeLimit

Description
Maximum number of seconds allowed for a search to be completed. The default value is 3600.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.65

Other
Single-valued attribute.

orclTimeZone

Description
Specifies the time zone applicable for a user location.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.311

orclTLimitMode

Description
Defines the time limit mode.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.406

Other
Single-valued attribute.

orclTotFreePhyMem

Description
Stores the total amount of free system physical memory.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.146

Other
Single-valued attribute.

orclTraceDimesionLevel

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.174

Other
Single-valued attribute.

orclTraceFileLocation

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.176

Other
Single-valued attribute.

orclTraceFileSize

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.177

Other
Single-valued attribute.

orclTraceLevel

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.173

Other
Single-valued attribute.

orclTraceMode

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.175

Other
Single-valued attribute.

orclTrustedApplicationGroup

Description
Identifies the DN of the group that list all the applications that specific application trusts for Service to Service Authentication.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.368

orclUIAccessibilityMode

Description
Set to TRUE to display a user interface that is accessible to people with impaired vision.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
2.16.840.1.113894.1.1.367

Other
Single-valued attribute.

orclUniqueAttrName

Description
The name of an attribute that you want to be unique. Autoboot uniqueness means that each entry must have a unique value for this attribute type.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.500

Other
Single-valued attribute.

orclUniqueEnable

Description
Disables or enables attribute uniqueness constraints. Allowed values are 0 (disable) or 1 (enable). The default value is 0.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.508

Other
Single-valued attribute.

orclUniqueObjectClass

Description

Specifies an object class filter for an attribute uniqueness constraint entry. This means the attribute specified in orclUniqueAttrNamemust be unique in an instance of this object class.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.503

Other

Single-valued attribute.

orclUniqueScope

Description

The scope of the attribute uniqueness constrain in the DIT. Allowed values are:

- `base`—Searches the root entry only
- `onelevel`—Searches one level only
- `sub`—Searches the entire directory

The default value is `sub`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.501

Other

Single-valued attribute.

orclUniqueSubtree

Description

When multiple attribute uniqueness constraints have the same values in orclUniqueAttrName, orclUniqueScope and orclUniqueObjectClass, but different values in `orcluniquesubtree`, the union of subtree scopes specified by those attribute uniqueness constraints is checked.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.502

Other
Single-valued attribute.

orclUnsyncRevPwd

Description
This attribute stores a password that is not synchronized with the entry in the userpassword.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
2.16.840.1.113894.1.1.217

Other
Directory operational attribute.

Not user modifiable.

orclUpdateSchedule

Description
Replication update interval for new changes and those being retried. The value is in minutes.

Syntax
1.3.6.1.4.1.1466.115.121.1.27

Matching Rule
N/A

Object ID
2.16.840.1.113894.1.1.30

Other
Directory operational attribute.

Not user modifiable.

orclUpgradeInProgress

Description
Indicates whether rolling upgrade is in progress.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.104

Other
Single-valued attribute.

orclUserDN

Description
The distinguished name (DN) of the user who performed an operation.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.16.840.1.113894.1.1.61

orclUserIDAttribute

Description
Specifies the attribute to use as the user identifier value when accessing the resource.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.16.840.1.113894.1.1.352

Other
Single-valued attribute.

orclUserModifiable

Description
Specifies if the data is modifiable by the user that this resource access descriptor entry is created for.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
1.2.3.4.5.6.1.11

orclUserObjectClasses

Description
A list of the object classes that comprise a user entity.

Syntax
1.3.6.1.4.1.1466.115.121.1.15

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.329

orclUserPrincipalName

Description
The is the Kerberos user principal name for Microsoft Active Directory users.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.8.1.904

Other
Single-valued attribute.

orclVersion

Description
The release version of the Oracle Internet Directory server.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.7.1.1

Other
Single-valued attribute.

orclWirelessAccountNumber

Description
Stores the wireless account number of a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.365

Other
Single-valued attribute.

orclWorkflowNotificationPref

Description
Identifies workflow notification preferences for a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.313

orclWriteWaitThreads

Description
Specifies the number of Oracle Internet Directory server threads waiting to write to the network.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
2.16.840.1.113894.1.1.143

Other
Single-valued attribute.

owner

Description
Specifies the distinguished name (DN) of some object which has some responsibility for the associated object.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.5.4.32

pilotStartTime

Description
The time stamp of when pilot mode was started for a replica.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
2.16.840.1.113894.1.1.825

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

preferredServerList

Description

The IP addresses of the preferred servers that a directory user agent should use in a space separated list. The servers in this list are tried in order before those in the defaultServerList until a successful connection is made. This has no default value. At least one server must be specified in either `preferredServerList` or `defaultServerList`.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (Printable String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.2

Other

Single-valued attribute.

profileTTL

Description

The time to live before a client directory user agent (DUA) should re-read this configuration profile. The values for profileTTL can be zero, to indicate no expiration, or a positive integer combined with one of the following letters to indicate the unit of measure:

`d`: indicates days

`h`: indicates hours

`m`: indicates minutes

`s`: indicates seconds

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.11.1.3.1.1.7

Other

Single-valued attribute.

protocolInformation

Description
This attribute is used in conjunction with the `presentationAddress` attribute, to provide additional information to the Open System Interconnection (OSI) network service.

Syntax
1.3.6.1.4.1.1466.115.121.1.42 (Protocol Information)

Matching Rule
protocolInformationMatch

Object ID
2.5.4.48

pwdAccountLockedTime

Description
The time stamp of when a user's account was locked.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.17

Other
Single-valued attribute.

Directory operational attribute.

No user modification.

pwdAllowUserChange

Description
Reserved for future use.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.14

Other
Single-valued attribute.

pwdChangedTime

Description
The time stamp indicating when the user's current password was created or modified.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.16

Other
Single-valued attribute.

Directory operational attribute.

No user modification.

pwdCheckSyntax

Description
A value of 1 (default) means passwords are checked for syntax errors. A value of 0 means syntax checking is disabled.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.5

Other
Single-valued attribute.

pwdExpirationWarned

Description
The time stamp when the first password expiration warning was sent to the user.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.18

Other
Directory operational attribute.

No user modification.

pwdExpireWarning

Description
The number of seconds before a password expires that a warning should be sent to the user. The user will see the warning when they attempt to log on during the warning period. If the user does not modify the password before it expires, the user is locked out until the password is changed by the administrator. The default value is 0, which means no warnings are sent.

For this feature to work, the client application must support it.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.7

Other
Single-valued attribute.

pwdFailureCountInterval

Description
The number of seconds after which the password failure times are purged from the user entry. If this attribute is not present, or if it has a value of 0, then failure times are never purged. The default value is `0`.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.12

Other
Single-valued attribute.

pwdFailureTime

Description
The time stamp of consecutive failed login attempts by the user.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.19

Other
Directory operational attribute.

No user modification.

pwdGraceLoginLimit

Description
Maximum number of grace logins allowed after a password expires. The default value is 0 (no grace logins allowed). The recommended value is 3.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.8

Other
Single-valued attribute.

pwdGraceUseTime

Description
The time stamps of each grace login for a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule
generalizedTimeMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.21

Other
Directory operational attribute.

No user modification.

pwdHistory

Description
A history of a user's previous passwords. The number of passwords stored in the history is determined by the pwdInHistory attribute.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.20

Other
Single-valued attribute.

Directory operational attribute.

No user modification.

pwdInHistory

Description
Number of previous passwords to be stored in the password history (pwdHistory). If a user attempts to reuse one of the passwords stored in the history, then the password is rejected. The default value is 0 (no previous passwords stored in the history).

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.4

Other
Single-valued attribute.

pwdLockout

Description

Specification for whether users are locked out of the directory after the number of consecutive failed bind attempts specified by pwdMaxFailure. If the value of this policy attribute is TRUE, then users are locked out. If this attribute is not present, or if the value is FALSE, then users are not locked out and the value of pwdMaxFailure is ignored. By default, account lockout is enforced.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.9

Other

Single-valued attribute.

pwdLockoutDuration

Description

The number of seconds a user is locked out of the directory if both of the following are true:

- Account lockout is enabled.
- The user has been unable to bind successfully to the directory for at least the number of times specified by pwdMaxFailure.

You can set user lockout for a specific duration, or until the administrator resets the user's password. A default value of 0 (zero) means that the user is locked out forever. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.10

Other

Single-valued attribute.

pwdMaxAge

Description
The maximum number of seconds that a given password is valid. If this attribute is not present, or if the value is 0 (zero), then the password does not expire. By default, the passwords expire in 60 days.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.3

Other
Single-valued attribute.

pwdMaxFailure

Description
The number of consecutive failed bind attempts after which a user account is locked. If this attribute is not present, or if the value is 0 (zero), then the account is not locked due to failed bind attempts, and the value of the password lockout policy is ignored. The default is 4.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.11

Other
Single-valued attribute.

pwdMinAge

Description
This attribute holds the number of seconds that must elapse between modifications to the password. If this attribute is not present, 0 seconds is assumed.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.2

Other
Single-valued attribute.

pwdMinLength

Description
The minimum number of characters required in a password. The default is 5. The value for this attribute must be at least 1.

Syntax
1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule
integerMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.6

Other
Single-valued attribute.

pwdMustChange

Description
Indicator of whether users must change their passwords after the first login, or after the password is reset by the administrator. Enabling this option requires users to change their passwords even if user-defined passwords are disabled. By default, users need not change their passwords after reset. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.13

Other
Single-valued attribute.

pwdReset

Description
Indicator that the password has been reset and must be changed by the user on first authentication. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.22

Other
Single-valued attribute.

Directory operational attribute.

Not user modifiable.

pwdSafeModify

Description
Indicator of whether user must supply old password with new one when modifying password. By default, the old password is not required. Allowed values are TRUE or FALSE.

Syntax
1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule
booleanMatch

Object ID
1.3.6.1.4.1.42.2.27.8.1.15

Other
Single-valued attribute.

ref

Description
A named reference. Values placed in the attribute must conform to the specification given for the labeledURI attribute (RFC 2079).

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseExactIA5Match

Object ID
2.16.840.1.113730.3.1.34

Other
DSA operational attribute.

searchTimeLimit

Description
Maximum time in seconds that a POSIX directory user agent (DUA) should allow for a search to complete.

Syntax

Matching Rule

Object ID

seeAlso

Description
Specifies the distinguished names of other directory objects which may be other aspects (in some sense) of the same real world object.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.5.4.34

serverName

Description
The name of the server involved in an Oracle Directory Integration Platform change subscription.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
caseIgnoreMatch

Object ID
2.16.840.1.113894.1.1.34

serviceAuthenticationMethod

Description
The authentication method for the service.

Syntax
1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule
N/A

Object ID
1.3.6.1.4.1.11.1.3.1.1.15

serviceCredentialLevel

Description
The credential level to be used by a service. The default value for all services is NULL. The supported credential levels are `anonymous` or `proxy`.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
N/A

Object ID
1.3.6.1.4.1.11.1.3.1.1.13

serviceSearchDescriptor

Description
Defines how and where an LDAP naming service client should search for information for a particular service. Contains a service name, followed by one or more semicolon-separated base-scope-filters.

Syntax
1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule
caseExactIA5Match

Object ID
1.3.6.1.4.1.11.1.3.1.1.8

sn

Description
The surname or last name of a user.

Syntax
1.3.6.1.4.1.1466.115.121.1.15{32768} (Directory String, 32768 character maximum)

Matching Rule
caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID
2.5.4.4

uniqueMember

Description
The distinguished name for the member of a group.

Syntax
1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
2.5.4.50

userCertificate;binary

Description
The user's certificate.

Syntax
1.3.6.1.4.1.1466.115.121.1.8 (Certificate)

Matching Rule
octetStringMatch

Object ID
2.5.4.36

userPassword

Description
The password used to authenticate a user to the directory.

Syntax
1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule
octetStringMatch

Object ID
2.5.4.35

Other
Single-valued attribute.

userPKCS12

Description
PKCS#12 PFX PDU for exchange of personal identity information.

Syntax
1.3.6.1.4.1.1466.115.121.1.5 (Binary)

Matching Rule
N/A

Object ID
2.16.840.1.113730.3.1.216

x509issuer

Description
The DN of the certificate authority who issued the X.509 certificate revocation list.

Syntax
1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule
distinguishedNameMatch

Object ID
1.3.6.1.4.1.10126.1.5.3.4

Part III

Appendixes

This part contains the following appendix:

- Appendix A, "LDIF File Format"

A

LDIF File Format

This appendix provides some general information about creating LDAP Data Interchange Files (LDIF) that can be used by the Oracle Internet Directory command-line tools. LDIF files are specially formatted text files that can be used to exchange data between LDAP directory servers, such as Oracle Internet Directory.

This appendix contains the following topics:

General LDIF Formatting Rules

LDIF formats are defined by the Internet Engineering Task Force (IETF) in RFC 2849. Visit the IETF Web site at `http://www.ietf.org/rfc/rfc2849.txt` for more information about LDIF formatting rules. This section explains some general rules for formatting LDIF files.

Line Types and White Space

Each line in an LDIF file must be correctly formatted in order to be read by the Oracle Internet Directory command-line tools. White space and line breaks must be used carefully.

Each line in an LDIF file is terminated with a line feed, which is `<LF>` on UNIX or `<CR><LF>` on Windows. In LDIF you can have the following types of lines:

- **Directive Line** - Any line that does not begin with either a `SPACE` or `#` (hash). A directive line specifies either some type of data in an entry or an operation to perform.
- **Continuation Line** - A line that begins with a `SPACE` denotes that the characters following the space are part of the previous line.
- **Blank Line** - Blank lines are used to separate entries and are typically created with the `ENTER` key.
- **Comment Line** - A comment line begins with a `#` (hash). Comments are ignored by the Oracle Internet Directory command-line tools.
- **Separator Line** - A line that starts with a `-` (dash) character is used to end an operation. It denotes that the next line begins a new operation directive.

Unnecessary space characters in the LDIF input file, such as a space at the end of an attribute value, will cause the LDAP operations to fail.

Sequencing of Entries

The sequence of entries in your LDIF file must follow the Directory Information Tree (DIT) from the top down. Parent entries should be listed before their children entries. Any attributes or object classes used in an entry must exist in the schema or be added to the schema before they can be used. Separate entries with a blank line.

Binary Files

Reference binary files, such as photographs, with the absolute address of the file proceeded by a `\` (forward slash).

Non-Printing Characters in Attribute Values

Non-printing characters and tabs are represented in attribute values as base-64 encoding.

LDIF Format for Entries

The standard format for directory entries is as follows:

```
dn: distinguished_name
changetype: add|delete|modify|modrdn|moddn
attribute_type: attribute_value
...
objectClass: object_class_value
...
```

The dn Directive

The `dn` directive defines the **distinguished name (DN)** of an entry. It is assumed that all lines below a `dn` directive belong to that entry until you add a space in the LDIF file to denote a separate entry. The following example shows a `dn` directive line:

```
dn: cn=Mary Jones,ou=Sales,dc=company,dc=com
```

The changetype Directive

The `changetype` directive defines the operation you want to perform on the entry. The operations that you specify with the `changetype` directive are:

- `add` - See "LDIF Format for Adding Entries" on page A-3 for syntax and examples.
- `delete` - See "LDIF Format for Deleting Entries" on page A-3 for syntax and examples.
- `modify` - "LDIF Format for Modifying Entries" on page A-3 for syntax and examples.
- `modrdn` - See "LDIF Format for Modifying the RDN of an Entry" on page A-4 for syntax and examples.
- `moddn` - See "LDIF Format for Modifying the DN of an Entry" on page A-4 for syntax and examples.

If `changetype` directive is omitted, then an `add` operation is assumed if using **bulkload**, **ldapadd** or **ldapaddmt**. A `delete` operation is assumed if using **bulkdelete** or **ldapdelete**. All other operations must specify a `changetype:` directive.

The *attribute_type* Directive

The *attribute_type* directive is used to specify an attribute type name and value pair. The entry will have an *attribute_type* directive for each attribute in the entry. For example, here is an *attribute_type* directive for the attribute type named `cn` where the value is `Mary Smith`.

```
cn: Mary Smith
```

The objectClass Directive

The `objectClass` directive is used to specify the object class that is associated with the entry. If an entry uses multiple object classes, then it will have an `objectClass` directive for each object class used. For example, here are the object classes used to define a user entry.

```
objectClass: orclUserV2
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Note that if an object class has required attributes, you must supply a value for those attributes using *attribute_type* directives.

LDIF Format for Adding Entries

The following example shows a file entry for an employee. The first line contains the DN. The second line contains the `changetype: add` directive. The lines that follow begin with the name for an attribute type, followed by the value to be associated with that attribute. Note that the `photo` attribute value begins with a forward slash (`\`) to denote that it is a binary file reference. Each entry ends with lines defining the object classes for the entry. Use an empty line at the end of the entry as a separator.

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
changetype: add
cn: Suzie Smith
cn: SuzieS
sn: Smith
mail: ssmith@us.Acme.com
telephoneNumber: 69332
photo: \$ORACLE_HOME/empdir/photog/ssmith.jpg
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

LDIF Format for Deleting Entries

When deleting an entry, the LDIF file entry only needs the DN of the entry to be deleted and the `changetype: delete` directive. Use an empty line at the end of the entry as a separator.

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
changetype: delete
```

LDIF Format for Modifying Entries

When modifying an entry, you must supply the DN of the entry followed by the `changetype: modify` directive. Next you must specify the attributes you want to modify using one of the following directives:

- `add: attribute_type` - Specifies the name of an attribute type for which you want to add a value. The next line should then contain the *`attribute_type: value`* directive for the value you want to add. For example:

  ```
  add: work-phone
  work-phone: 510/506-7000
  ```

- `delete: attribute_type` - Specifies the name of an attribute type for which you want to delete the value. If the attribute is multi-valued, then you should also supply the *`attribute_type: value`* directive for the specific value you want to delete, otherwise all values for the attribute will be deleted. For example:

  ```
  delete: home-fax
  ```

- `replace: attribute_type` - Specifies the name of an attribute type for which you want to replace the existing value with a new value. The next line should then contain the *`attribute_type: value`* directive for the value you want to replace. For example:

  ```
  replace: home-phone
  home-phone: 415/697-8899
  ```

  If the attribute is multi-valued then all the current values are replaced with one or more attributes following this directive. If only a single value of a multi-valued attribute needs to be replaced use `delete` then `add`.

If you are making several modifications to an entry, then, between each modification you enter, add a line that contains a hyphen (-) only. For example:

```
dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: modify
add: work-phone
work-phone: 650/506-7000
work-phone: 650/506-7001
-
delete: home-fax
-
replace: home-phone
home-phone: 415/697-8899
```

LDIF Format for Modifying the RDN of an Entry

To modify the relative distinguished name (RDN) for an entry, you must supply the DN of the entry followed by the `changetype: modrdn` directive. Next you must specify the new RDN with a `newrdn:` directive, and you can optionally delete or keep the old entry by supplying a `deleteoldrdn:` directive. For example:

```
dn: cn=Sally Smith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: Sally Smith-Jones
# deletes old RDN entry
deleteoldrdn: 1
```

LDIF Format for Modifying the DN of an Entry

To modify the DN for an entry (move the entry to a new node in the DIT), you must supply the DN of the entry followed by the `changetype: moddn` directive. Next you must specify the new parent DN with a `newsuperior:` directive, and you can

optionally delete or keep the old entry by supplying a `deleteoldrdn:` directive. For example:

```
dn: cn=Sally Smith,ou=people,dc=example,dc=com
changetype: moddn
newsuperior: ou=expeople,dc=example,dc=com
# keeps old RDN entry
deleteoldrdn: 0
```

LDIF Format for Adding Schema Elements

Attribute types and object classes must be added to the Oracle Internet Directory schema before they can be used in entries.

Example: Adding an Attribute to the Schema

This example adds a new attribute to the schema called `myAttr`. The LDIF file for this operation is:

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5.6.7 NAME 'myAttr' DESC 'New attribute definition'
 EQUALITY caseIgnoreMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

On the first line, enter the DN specifying where this new attribute is to be located. All attributes and object classes are stored in `cn=subschemasubentry`.

The second and third lines show the proper format for adding a new attribute.

The last line is the attribute definition itself. The first part of this is the object identifier number: `1.2.3.4.5.6.7`. It must be unique among all other object classes and attributes. Next is the `NAME` of the attribute. In this case the attribute NAME is `myAttr`. It must be surrounded by single quotes. Next is a description of the attribute. Enter whatever description you want between single quotes. At the end of this attribute definition in this example are optional formatting rules to the attribute. In this case we are adding a matching rule of `EQUALITY caseIgnoreMatch` and a `SYNTAX` of `1.3.6.1.4.1.1466.115.121.1.15` (which is the object ID for the syntax of "Directory String").

When you define schema within an LDIF file, insert a white space between the opening parenthesis and the beginning of the text, and between the end of the text and the ending parenthesis.

Example: Adding an Object Class to the Schema

Before you add the object class, all of the attribute types that the object class uses must be in the schema. If there are new attribute types, then define those first in your LDIF file before defining your object class.

The following example adds a new object class named `myObjectClass` to the schema.

```
dn: cn=subschemasubentry
changetype: modify
add: objectClasses
objectClasses: ( 1.2.3.4.56789.1.0.200 NAME 'myObjectClass'
 SUP ( top ) STRUCTURAL
 MUST ( cn )
 MAY ( myAttr1 $  myAttr2 $ myAttr3 ) )
```

On the first line, enter the DN specifying where this new object class is to be located. All attributes and object classes are stored in `cn=subschemasubentry`.

The second and third lines show the proper format for adding a new object class.

The last line is the object class definition itself. The first part of this is the object identifier number: `1.2.3.4.56789.1.0.200`. It must be unique among all other object classes and attributes. Next is the `NAME` of the object class. In this case the object class name is `myObjectClass`. It must be surrounded by single quotes. Next is the superior (`SUP`) object classes, which in this case is `top`. `STRUCTURAL` denotes the type of object class. `MUST` and `MAY` denote the required and allowed attributes. Separate attribute names with a dollar sign (`$`).

When you define schema within an LDIF file, insert a white space between the opening parenthesis and the beginning of the text, and between the end of the text and the ending parenthesis. If using line breaks for formatting long lines, make sure to add a space at the beginning of a line to denote that it is a continuation of the previous line.

Example: Adding A New Object Class to an Entry

Before you can use a new object class and the attributes it contains, you must update the entry to use the new object class. The following example shows how to add a new object class to an entry. Note that you must define a value for all of the required attributes of the object class.

```
# Add a new AUXILIARY object class to an existing entry
dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
# the object class used for binding
objectclass: inetorgperson
# objectclass being added
objectclass: myObjectClass
# MUST attributes of new object class
myAttr1: some value
myAttr2: my value
myAttr3: a value
```

LDIF Format for Migrating Entries

This section describes how to properly format an LDIF file for use with the Oracle Internet Directory Migration Tool. The migration tool enables you to take LDIF entries output from other directories or applications and covert the data to use the attributes and values found in Oracle Internet Directory entries. You do this by inserting substitution variables for the data elements you want to convert.

See "ldifmigrator" on page 4-41 for more information about the Oracle Internet Directory Migration Tool.

Substitution Variables for Migration Input Files

Substitution variables are denoted in the LDIF file by the following syntax:

```
%s_variableName%
```

For example, let's say you have the following LDIF formatted entry that was exported from another application. The subtree where user entries are stored, the user nickname attribute, and the name of the user's organization are different in Oracle Internet Directory than in the original application. For those elements you want to convert, you would add substitution variables to the file as placeholders.

Example:

```
dn: cn=jdoe, %s_UserContainerDN%
sn: Doe
%s_UserNicknameAttribute%: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
ou: %s_UserOrganization%
```

When you run the Oracle Internet Directory Migration Tool against this file, it will find the variables and either replace then with the values you define on the command-line or look up the correct values in Oracle Internet Directory.

Predefined Substitution Variables

The Oracle Internet Directory Migration Tool recognizes several predefined substitution variables. If running the tool in lookup mode, the values for these variables can be looked up in Oracle Internet Directory. You can use these predefined variables or define variables of your own using the `%s_variableName%` syntax.

Table A–1 Predefined Substitution Variables

Variable Name	Meaning	How OID Migration Tool Determines the Value for This Variable
%s_UserContainerDN%	Distinguished name of the entry under which all users are supposed to be added.	This is assigned the value of the attribute: `orclCommonUserSearchBase` from the entry `cn=Common,cn=Products` under the realm- specific Oracle context.
%s_GroupContainerDN%	Distinguished name of the entry under which all public groups are supposed to be added.	This is assigned the value of the attribute: `orclCommonGroupSearchBase` from the entry `cn=Common,cn=Products` under the realm- specific Oracle context.
%s_UserNicknameAttribute%	The nickname attribute to be used for user entries in the identity management realm.	This is assigned the value of the attribute: `orclCommonNicknameAttribute` from the entry `cn=Common,cn=Products` under the realm- specific Oracle context.
%s_SubscriberDN%	Distinguished name of the LDAP entry corresponding to the identity management realm.	If a simple subscriber name is given, the migration tool will resolve it to a DN using the attribute `orclSubscriberSearchBase` and the `orclSubscriberNickNameAttr` from the entry `cn=Common,cn=Products` under the root Oracle context.

Table A–1 (Cont.) Predefined Substitution Variables

Variable Name	Meaning	How OID Migration Tool Determines the Value for This Variable
%s_SubscriberOracleContextDN%	Distinguished name of the realm-specific Oracle Context.	First the realm DN is computed as described earlier and then the string `cn=OracleContext` is pre-pended to it.
%s_RootOracleContextDN%	Distinguished name of the Root Oracle Context.	This is currently hard-coded to `cn=OracleContext`.
%s_CurrentUserDN%	Distinguished name of the User who is loading the LDIF file. This is sometimes required to bootstrap the creation of groups which require at least one member in them.	The migration tool expects this DN to be specified on the command line as part of the authentication information.

Reconcile Options for Migrated Entries

When migrating entries into Oracle Internet Directory from another application, it is possible that there may be conflicts. For example, a user entry may already be defined in Oracle Internet Directory, or have conflicting values with the migrated data. In this case, the reconcile option will control what LDIF `changetype` directives are performed. There are three modes for reconciliation of migrated data:

- **SAFE** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If any other directive besides the following are specified in the LDIF file, they will not be applied.

```
changetype:add

changetype:modify
      add: attribute_name (adds attribute only if it doesn't exist)
```

- **SAFE-EXTENDED** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If you try to add a new value for existing attributes, then it will add it to the existing set of values. If any other directive besides the following are specified in the LDIF file, they will not be applied.

```
changetype:add

changetype:modify
      add: attribute_name (appends values if attribute exists)
```

- **NORMAL** - This mode applies all directives as intended. The following directives are supported:

```
changetype:add

changetype:delete

changetype:modify
      add: attribute_name
      replace: attribute_name
      delete: attribute_name
```

Glossary

3DES

See **Triple Data Encryption Standard (3DES)**.

access control item (ACI)

Access control information represents the permissions that various entities or subjects have to perform operations on a given object in the directory. This information is stored in Oracle Internet Directory as user-modifiable operational **attribute**s, each of which is called an access control item (ACI). An ACI determines user access rights to directory data. It contains a set of rules for controlling access to entries (structural access items) and attributes (content access items). Access to both structural and content access items may be granted to one or more users or groups.

access control list (ACL)

A list of resources and the user names of people who are permitted access to those resources within a computer system. In Oracle Internet Directory, an ACL is a list of **access control item (ACI) attribute value**s that is associated with directory objects. The attribute values on that list represent the permissions that various directory user entities (or subjects) have on a given object.

access control policy point (ACP)

A directory entry that contains access control policy information that applies downward to all entries at lower positions in the **directory information tree (DIT)**. This information affects the entry itself and all entries below it. In Oracle Internet Directory, you can create ACPs to apply an access control policy throughout a **subtree** of your directory.

account lockout

A security feature that locks a user account if repeated failed logon attempts occur within a specified amount of time, based on security policy settings. Account lockout occurs in OracleAS Single Sign-On when a user submits an account and password combination from any number of workstations more times than is permitted by Oracle Internet Directory. The default lockout period is 24 hours.

ACI

See **access control item (ACI)**.

ACL

See **access control list (ACL)**.

ACP

See **access control policy point (ACP)**.

administrative area

A **subtree** on a directory server whose entries are under the control of a single administrative authority. The designated administrator controls each **entry** in that administrative area, as well as the directory **schema**, **access control list (ACL)**, and **attribute**s for those entries.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a **symmetric cryptography** algorithm that is intended to replace **Data Encryption Standard (DES)**. AES is a Federal Information Processing Standard (FIPS) for the encryption of commercial and government data.

advanced replication

See **Oracle Database Advanced Replication**.

advanced symmetric replication (ASR)

See **Oracle Database Advanced Replication**.

AES

See **Advanced Encryption Standard (AES)**.

anonymous authentication

The process by which a directory authenticates a user without requiring a user name and password combination. Each anonymous user then exercises the privileges specified for anonymous users.

API

See **application programming interface (API)**.

application programming interface (API)

A series of software routines and development tools that comprise an interface between a computer application and lower-level services and functions (such as the operating system, device drivers, and other software applications). APIs serve as building blocks for programmers putting together software applications. For example, LDAP-enabled clients access Oracle Internet Directory information through programmatic calls available in the LDAP API.

application service provider

Application Service Providers (ASPs) are third-party entities that manage and distribute software-based services and solutions to customers across a wide area network from a central data center. In essence, ASPs are a way for companies to outsource some or almost all aspects of their information technology needs.

artifact profile

An **authentication** mechanism which transmits data using a compact reference to an **assertion**, called an artifact, instead of sending the full assertion. This **profile** accomodates browsers which handle a limited number of characters.

ASN.1

Abstract Syntax Notation One (ASN.1) is an International Telecommunication Union (ITU) notation used to define the syntax of information data. ASN.1 is used to describe

structured information, typically information that is to be conveyed across some communications medium. It is widely used in the specification of Internet protocols.

ASR

See **Oracle Database Advanced Replication**.

assertion

An assertion is a statement used by providers in security domains to exchange information about a subject seeking access to a resource. Identity providers, as well as service providers, exchange assertions about identities to make **authentication** and **authorization** decisions, and to determine and enforce security policies protecting the resource.

asymmetric algorithm

A **cryptographic algorithm** that uses different **key**s for **encryption** and **decryption**.

See also: **public key cryptography**.

asymmetric cryptography

See **public key cryptography**.

attribute

Directory attributes hold a specific data element such as a name, phone number, or job title. Each directory **entry** is comprised of a set of attributes, each of which belongs to an **object class**. Moreover, each attribute has both a *type*, which describes the kind of information in the attribute, and a *value*, which contains the actual data.

attribute configuration file

In an Oracle Directory Integration Platform environment, a file that specifies attributes of interest in a connected directory.

attribute type

Attribute types specify information about a data element, such as the data type, maximum length, and whether it is single-valued or multivalued. The attribute type provides the real-world meaning for a value, and specifies the rules for creating and storing specific pieces of data, such as a name or an e-mail address.

attribute uniqueness

An Oracle Internet Directory feature that ensures that no two specified **attribute**s have the same value. It enables applications synchronizing with the enterprise directory to use attributes as unique keys.

attribute value

Attribute values are the actual data contained within an **attribute** for a particular **entry**. For example, for the attribute type `email`, an attribute value might be `sally.jones@oracle.com`.

authentication

The process of verifying the identity claimed by an entity based on its credentials. Authentication of a user is generally based on something the user knows or has (for example, a password or a certificate).

Authentication of an electronic message involves the use of some kind of system (such as **public key cryptography**) to ensure that a file or message which claims to originate

from a given individual or company actually does, and a check based on the contents of a message to ensure that it was not modified in transit.

authentication level

An OracleAS Single Sign-On parameter that enables you to specify a particular authentication behavior for an application. You can link this parameter with a specific **authentication plugin**.

authentication plugin

An implementation of a specific authentication method. OracleAS Single Sign-On has Java plugins for password authentication, digital certificates, Windows native authentication, and third-party access management.

authorization

The process of granting or denying access to a service or network resource. Most security systems are based on a two step process. The first stage is authentication, in which a user proves his or her identity. The second stage is authorization, in which a user is allowed to access various resources based on his or her identity and the defined **authorization policy**.

authorization policy

Authorization policy describes how access to a protected resource is governed. Policy maps identities and objects to collections of rights according to some system model. For example, a particular authorization policy might state that users can access a sales report only if they belong to the sales group.

basic authentication

An **authentication** protocol supported by most browsers in which a Web server authenticates an entity with an encoded user name and password passed via data transmissions. Basic authentication is sometimes called plaintext authentication because the base-64 encoding can be decoded by anyone with a freely available decoding utility. Note that encoding is not the same as **encryption**.

Basic Encoding Rules (BER)

Basic Encoding Rules (BER) are the standard rules for encoding data units set forth in **ASN.1**. BER is sometimes incorrectly paired with ASN.1, which applies only to the abstract syntax description language, not the encoding technique.

BER

See **Basic Encoding Rules (BER)**.

binding

In networking, binding is the establishment of a logical connection between communicating entities.

In the case of Oracle Internet Directory, binding refers to the process of authenticating to the directory.

The formal set of rules for carrying a **SOAP** message within or on top of another protocol (underlying protocol) for the purpose of exchange is also called a binding.

block cipher

Block ciphers are a type of **symmetric algorithm**. A block cipher encrypts a message by breaking it down into fixed-size blocks (often 64 bits) and encrypting each block with a key. Some well known block ciphers include **Blowfish**, **DES**, and **AES**.

See also: **stream cipher**.

Blowfish

Blowfish is a **symmetric cryptography** algorithm developed by Bruce Schneier in 1993 as a faster replacement for **DES**. It is a **block cipher** using 64-bit blocks and keys of up to 448 bits.

CA

See **Certificate Authority (CA)**.

CA certificate

A **Certificate Authority (CA)** signs all certificates that it issues with its **private key**. The corresponding Certificate Authority's **public key** is itself contained within a certificate, called a CA Certificate (also referred to as a root certificate). A browser must contain the CA Certificate in its list of trusted root certificates in order to trust messages signed by the CA's private key.

cache

Generally refers to an amount of quickly accessible memory in your computer. However, on the Web it more commonly refers to where the browser stores downloaded files and graphics on the user's computer.

CBC

See **cipher block chaining (CBC)**.

central directory

In an Oracle Directory Integration Platform environment, the directory that acts as the central repository. In an Oracle Directory Integration Platform environment, Oracle Internet Directory is the central directory.

certificate

A certificate is a specially formatted data structure that associates a **public key** with the identity of its owner. A certificate is issued by a **Certificate Authority (CA)**. It contains the name, serial number, expiration dates, and public key of a particular entity. The certificate is digitally signed by the issuing CA so that a recipient can verify that the certificate is real. Most digital certificates conform to the **X.509** standard.

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted third party that issues, renews, and revokes digital **certificate**s. The CA essentially vouches for a entity's identity, and may delegate the verification of an applicant to a **Registration Authority (RA)**. Some well known Certificate Authorities (CAs) include Digital Signature Trust, Thawte, and VeriSign.

certificate chain

An ordered list of certificates containing one or more pairs of a user **certificate** and its associated **CA certificate**.

certificate management protocol (CMP)

Certificate Management Protocol (CMP) handles all relevant aspects of certificate creation and management. CMP supports interactions between **public key infrastructure (PKI)**) components, such as the **Certificate Authority (CA)**, **Registration Authority (RA)**, and the user or application that is issued a certificate.

certificate request message format (CRMF)

Certificate Request Message Format (CRMF) is a format used for messages related to the life-cycle management of **X.509** certificates, as described in the **RFC** 2511 specification.

certificate revocation list (CRL)

A Certificate Revocation List (CRL) is a list of digital **certificate**s which have been revoked by the **Certificate Authority (CA)** that issued them.

change logs

A database that records changes made to a directory server.

cipher

See **cryptographic algorithm**.

cipher block chaining (CBC)

Cipher block chaining (CBC) is a mode of operation for a **block cipher**. CBC uses what is known as an initialization vector (IV) of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block of ciphertext to depend on all the preceding ciphertext blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous ciphertext block.

cipher suite

In **Secure Sockets Layer (SSL)**, a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth.

ciphertext

Ciphertext is the result of applying a **cryptographic algorithm** to readable data (plaintext) in order to render the data unreadable by all entities except those in possession of the appropriate **key**.

circle of trust

A trust relationship among a set of identity providers and service providers that allows a **principal** to use a single federated identity and **single sign-on (SSO)** when conducting business transactions with providers within that set.

Businesses federate or affiliate together into circles of trust based on Liberty-enabled technology and on operational agreements that define trust relationships between the businesses.

See also: **federated identity management (FIM)**, **Liberty Alliance**.

claim

A claim is a declaration made by an entity (for example, a name, identity, key, group, and so on).

client SSL certificates

A type of **certificate** used to identify a client machine to a server through **Secure Sockets Layer (SSL)** (client authentication).

cluster

A collection of interconnected usable whole computers that is used as a single computing resource. Hardware clusters provide high availability and scalability.

CMP

See **certificate management protocol (CMP)**.

CMS

See **Cryptographic Message Syntax (CMS)**.

code signing certificates

A type of **certificate** used to identify the entity who signed a Java program, Java Script, or other signed file.

cold backup

In Oracle Internet Directory, this refers to the procedure of adding a new **directory system agent (DSA)** node to an existing replicating system by using the database copy procedure.

concurrency

The ability to handle multiple requests simultaneously. Threads and processes are examples of concurrency mechanisms.

concurrent clients

The total number of clients that have established a session with Oracle Internet Directory.

concurrent operations

The number of operations that are being executed on Oracle Internet Directory from all of the **concurrent clients**. Note that this is not necessarily the same as the concurrent clients, because some of the clients may be keeping their sessions idle.

confidentiality

In cryptography, confidentiality (also known as privacy) is the ability to prevent unauthorized entities from reading data. This is typically achieved through **encryption**.

configset

See **configuration set entry**.

configuration set entry

An Oracle Internet Directory entry holding the configuration parameters for a specific instance of the directory server. Multiple configuration set entries can be stored and referenced at runtime. The configuration set entries are maintained in the subtree specified by the `subConfigsubEntry` attribute of the **directory-specific entry (DSE)**, which itself resides in the associated **directory information base (DIB)** against which the servers are started.

connect descriptor

A specially formatted description of the destination for a network connection. A connect descriptor contains destination service and network route information.

The destination service is indicated by using its service name for the Oracle Database or its Oracle System Identifier (SID) for Oracle release 8.0 or version 7 databases. The

network route provides, at a minimum, the location of the listener through use of a network address.

connected directory

In an Oracle Directory Integration Platform environment, an information repository requiring full synchronization of data between Oracle Internet Directory and itself—for example, an Oracle human resources database.

consumer

A directory server that is the destination of replication updates. Sometimes called a slave.

contention

Competition for resources.

context prefix

The **distinguished name (DN)** of the root of a **naming context**.

CRL

See **certificate revocation list (CRL)**.

CRMF

See **certificate request message format (CRMF)**.

cryptographic algorithm

A cryptographic algorithm is a defined sequence of processes to convert readable data (plaintext) to unreadable data (ciphertext) and vice versa. These conversions require some secret knowledge, normally contained in a **key**. Examples of cryptographic algorithms include **DES**, **AES**, **Blowfish**, and **RSA**.

Cryptographic Message Syntax (CMS)

Cryptographic Message Syntax (CMS) is a syntax defined in **RFC** 3369 for signing, digesting, authenticating, and encrypting digital messages.

cryptography

The process of protecting information by transforming it into an unreadable format. The information is encrypted using a **key**, which makes the data unreadable, and is then decrypted later when the information needs to be used again. See also **public key cryptography** and **symmetric cryptography**.

dads.conf

A configuration file for Oracle HTTP Server that is used to configure a **database access descriptor (DAD)**.

DAS

See **Oracle Delegated Administration Services**. (DAS).

Data Encryption Standard (DES)

Data Encryption Standard (DES) is a widely used **symmetric cryptography** algorithm developed in 1974 by IBM. It applies a 56-bit key to each 64-bit block of data. DES and 3DES are typically used as encryption algorithms by **S/MIME**.

data integrity

The guarantee that the contents of the message received were not altered from the contents of the original message sent.

See also: **integrity**.

database access descriptor (DAD)

Database connection information for a particular Oracle Application Server component, such as the OracleAS Single Sign-On schema.

decryption

The process of converting the contents of an encrypted message (ciphertext) back into its original readable format (plaintext).

default identity management realm

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such hosted environments, the enterprise performing the hosting is called the default identity management realm, and the enterprises that are hosted are each associated with their own identity management realm in the **directory information tree (DIT)**.

default knowledge reference

A **knowledge reference** that is returned when the base object is not in the directory, and the operation is performed in a **naming context** not held locally by the server. A default knowledge reference typically sends the user to a server that has more knowledge about the directory partitioning arrangement.

default realm location

An attribute in the **root Oracle Context** that identifies the root of the **default identity management realm**.

defederation

The act of unlinking a user's account from an **identity provider** or **service provider**.

Delegated Administration Services

See **Oracle Delegated Administration Services**.

delegated administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory. Other administrators—called delegated administrators—may exercise roles in specific identity management realms, or for specific applications.

DER

See **Distinguished Encoding Rules (DER)**.

DES

See **Data Encryption Standard (DES)**.

DIB

See **directory information base (DIB)**.

Diffie-Hellman

Diffie-Hellman (DH) is a public key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. First published in 1976, it was the first workable public key cryptographic system.

See also: **symmetric algorithm**.

digest

See **message digest**.

digital certificate

See **certificate**.

digital signature

A digital signature is the result of a two-step process applied to a given block of data. First, a **hash function** is applied to the data to obtain a result. Second, that result is encrypted using the signer's **private key**. Digital signatures can be used to ensure integrity, message authentication, and non-repudiation of data. Examples of digital signature algorithms include **DSA**, **RSA**, and **ECDSA**.

Digital Signature Algorithm (DSA)

The Digital Signature Algorithm (DSA) is an **asymmetric algorithm** that is used as part of the Digital Signature Standard (DSS). It cannot be used for encryption, only for digital signatures. The algorithm produces a pair of large numbers that enable the authentication of the signatory, and consequently, the integrity of the data attached. DSA is used both in generating and verifying digital signatures.

See also: **Elliptic Curve Digital Signature Algorithm (ECDSA)**.

directory

See **Oracle Internet Directory**, **Lightweight Directory Access Protocol (LDAP)**, and **X.500**.

directory information base (DIB)

The complete set of all information held in the directory. The DIB consists of entries that are related to each other hierarchically in a **directory information tree (DIT)**.

directory information tree (DIT)

A hierarchical tree-like structure consisting of the **DN**s of the entries.

Directory Integration Platform server

In an Oracle Directory Integration Platform environment, the server that drives the synchronization of data between Oracle Internet Directory and a **connected directory**.

directory integration profile

In an Oracle Directory Integration Platform environment, an entry in Oracle Internet Directory that describes how Oracle Directory Integration Platform communicates with external systems and what is communicated.

Directory Manager

See **Oracle Directory Manager**.

directory naming context

See **naming context**.

directory provisioning profile

A special kind of **directory integration profile** that describes the nature of provisioning-related notifications that Oracle Directory Integration Platform sends to the directory-enabled applications.

directory replication group (DRG)

The directory servers participating in a **replication agreement**.

directory server instance

A discrete invocation of a directory server. Different invocations of a directory server, each started with the same or different configuration set entries and startup flags, are said to be different directory server instances.

directory synchronization profile

A special kind of **directory integration profile** that describes how synchronization is carried out between Oracle Internet Directory and an external system.

directory system agent (DSA)

The **X.500** term for a directory server.

directory-specific entry (DSE)

An entry specific to a directory server. Different directory servers may hold the same **directory information tree (DIT)** name, but have different contents—that is, the contents can be specific to the directory holding it. A DSE is an entry with contents specific to the directory server holding it.

directory user agent (DUA)

The software that accesses a directory service on behalf of the directory user. The directory user may be a person or another software element.

DIS

See **Directory Integration Platform server**.

Distinguished Encoding Rules (DER)

Distinguished Encoding Rules (DER) are a set of rules for encoding **ASN.1** objects in byte-sequences. DER is a special case of **Basic Encoding Rules (BER)**.

distinguished name (DN)

A **X.500** distinguished name (DN) is a unique name for a node in a directory tree. A DN is used to provide a unique name for a person or any other directory entry. A DN is a concatenation of selected **attribute**s from each node in the tree along the path from the root node to the named entry's node. For example, in LDAP notation, the DN for a person named John Smith working at Oracle's US office would be: "cn=John Smith, ou=People, o=Oracle, c=us".

DIT

See **directory information tree (DIT)**.

DN

See **distinguished name (DN)**.

Document Type Definition (DTD)

A Document Type Definition (DTD) is a document that specifies constraints on the tags and tag sequences that are valid for a given **XML** document. DTDs follow the rules of Simple Generalized Markup Language (SGML), the parent language of XML.

domain

A domain includes the Web site and applications that enable a **principal** to utilize resources. A federated site acts as an **identity provider** (also known as the source domain), a **service provider** (also known as the destination domain), or both.

domain component attribute

The domain component (dc) attribute can be used in constructing a **distinguished name (DN)** from a domain name. For example, using a domain name such as "oracle.com", one could construct a DN beginning with "dc=oracle, dc=com", and then use this DN as the root of its subtree of directory information.

DRG

See **directory replication group (DRG)**.

DSA

See **Digital Signature Algorithm (DSA)** or **directory system agent (DSA)**.

DSE

See **directory-specific entry (DSE)**.

DTD

See **Document Type Definition (DTD)**.

ECC

See **Elliptic Curve Cryptography (ECC)**.

ECDSA

See **Elliptic Curve Digital Signature Algorithm (ECDSA)**.

EJB

See **Enterprise Java Bean (EJB)**.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is an alternative to the **RSA** encryption system which is based on the difficulty of solving elliptic curve discrete logarithm problems rather than on factoring large numbers. Developed and marketed by Certicom, ECC is especially suitable for environments, such as wireless devices and PC cards, where computational power is limited and high speed is required. For any given key size (measured in bits) ECC provides more security (is harder to decrypt without the key) than RSA.

Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analog of the **Digital Signature Algorithm (DSA)** standard. The advantages of ECDSA compared to RSA-like schemes are shorter key lengths and faster signing and decryption. For example, a 160 (210) bit ECC key is expected to give the same security as a 1024 (2048) bit RSA key, and the advantage increases as level of security is raised.

encryption

Encryption is the process of converting plaintext to ciphertext by applying a **cryptographic algorithm**.

encryption certificate

An encryption certificate is a **certificate** containing a **public key** that is used to encrypt electronic messages, files, documents, or data transmission, or to establish or exchange a session key for these same purposes.

end-to-end security

This is a property of message-level security that is established when a message traverses multiple applications within and between business entities and is secure over its full route through and between the business entities.

Enterprise Java Bean (EJB)

Enterprise JavaBeans (EJBs) are a Java API developed by Sun Microsystems that defines a component architecture for multi-tier client/server systems. Because EJB systems are written in Java, they are platform independent. Being object oriented, they can be implemented into existing systems with little or no recompiling and configuring.

Enterprise Manager

See **Oracle Enterprise Manager**.

entry

An entry is a unique record in a directory that describes an object, such as a person. An entry consists of **attribute**s and their associated **attribute value**s, as dictated by the **object class** that describes that entry object. All entries in an LDAP directory structure are uniquely identified through their **distinguished name (DN)**.

export agent

In an Oracle Directory Integration Platform environment, an agent that exports data out of Oracle Internet Directory.

export data file

In an Oracle Directory Integration Platform environment, the file that contains data exported by an **export agent**.

export file

See **export data file**.

external agent

A directory integration agent that is independent of Oracle Directory Integration Platform server. Oracle Directory Integration Platform server does not provide scheduling, mapping, or error handling services for it. An external agent is typically used when a third party metadirectory solution is integrated with Oracle Directory Integration Platform.

external application

Applications that do not delegate authentication to the OracleAS Single Sign-On server. Instead, they display HTML login forms that ask for application user names and passwords. At the first login, users can choose to have the OracleAS Single

Sign-On server retrieve these credentials for them. Thereafter, they are logged in to these applications transparently.

failover

The process of failure recognition and recovery. In an Oracle Application Server Cold Failover Cluster (Identity Management), an application running on one cluster node is transparently migrated to another cluster node. During this migration, clients accessing the service on the cluster see a momentary outage and may need to reconnect once the failover is complete.

fan-out replication

Also called a point-to-point replication, a type of replication in which a supplier replicates directly to a consumer. That consumer can then replicate to one or more other consumers. The replication can be either full or partial.

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) are standards for information processing issued by the US government Department of Commerce's National Institute of Standards and Technology (NIST).

federated identity management (FIM)

The agreements, standards, and technologies that make identity and entitlements portable across autonomous domains. FIM makes it possible for an authenticated user to be recognized and take part in personalized services across multiple domains. It avoids pitfalls of centralized storage of personal information, while allowing users to link identity information between different accounts. Federated identity requires two key components: trust and standards. The trust model of federated identity management is based on **circle of trust**. The standards are defined by the **Liberty Alliance** Project.

federation

See **identity federation**.

filter

A filter is an expression that defines the entries to be returned from a request or search on a directory. Filters are typically expressed as DNs, for example: `cn=susie smith,o=acme,c=us`.

FIM

See **federated identity management (FIM)**.

FIPS

See **Federal Information Processing Standards (FIPS)**.

forced authentication

The act of forcing a user to reauthenticate if he or she has been idle for a preconfigured amount of time. Oracle Application Server Single Sign-On enables you to specify a global user inactivity timeout. This feature is intended for installations that have sensitive applications.

GET

An authentication method whereby login credentials are submitted as part of the login URL.

global administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory.

global logout

The process by which a principal, conducting transactions with a given set of Identity Providers and Service Providers using a single federated identity, is logged out by all peer providers in the circle of trust including the provider that asserted the principal's identity. The logout process can be initiated by the principal or by a logout request from a peer provider.

global unique identifier (GUID)

An identifier generated by the system and inserted into an entry when the entry is added to the directory. In a multimaster replicated environment, the GUID, not the DN, uniquely identifies an entry. The GUID of an entry cannot be modified by a user.

global user inactivity timeout

An optional feature of Oracle Application Server Single Sign-On that forces users to reauthenticate if they have been idle for a preconfigured amount of time. The global user inactivity timeout is much shorter than the single sign-out session timeout.

globalization support

Multilanguage support for graphical user interfaces. Oracle Application Server Single Sign-On supports 29 languages.

globally unique user ID

A numeric string that uniquely identifies a user. A person may change or add user names, passwords, and distinguished names, but her globally unique user ID always remains the same.

grace login

A login occurring within the specified period before password expiration.

group search base

In the Oracle Internet Directory default **directory information tree (DIT)**, the node in the identity management realm under which all the groups can be found.

guest user

One who is not an anonymous user, and, at the same time, does not have a specific user entry.

GUID

See **global unique identifier (GUID)**.

handshake

A protocol two computers use to initiate a communication session.

hash

A number generated from a string of text with an algorithm. The hash value is substantially smaller than the text itself. Hash numbers are used for security and for faster access to data.

See also: **hash function**.

hash function

In cryptography, a hash function or one-way hash function is an algorithm that produces a given value when applied to a given block of data. The result of a hash function can be used to ensure the integrity of a given block of data. For a hash function to be considered secure, it must be very difficult, given a known data block and a known result, to produce another data block that produces the same result.

Hashed Message Authentication Code (HMAC)

Hashed Message Authentication Code (HMAC) is a hash function technique used to create a secret hash function output. This strengthens existing hash functions such as MD5 and SHA. It is used in transport layer security (TLS).

HMAC

See **Hashed Message Authentication Code (HMAC)**.

HTTP

The Hyper Text Transfer Protocol (HTTP) is the protocol used between a Web browser and a server to request a document and transfer its contents. The specification is maintained and developed by the World Wide Web Consortium.

HTTP Redirect Profile

A **federation** profile which indicates that the requested resource resides under a different URL.

HTTP Server

See **Oracle HTTP Server**.

httpd.conf

The file used to configure **Oracle HTTP Server**.

iASAdmins

The administrative group responsible for user and group management functions in Oracle Application Server. The OracleAS Single Sign-On administrator is a member of the group iASAdmins.

identity federation

The linking of two or more accounts a **principal** may hold with one or more identity providers or service providers within a given **circle of trust**.

When users federate the otherwise isolated accounts they have with businesses, known as their local identities, they create a relationship between two entities, an association comprising any number of service providers and identity providers.

See also: **identity provider**, **service provider**.

identity management

The process by which the complete security lifecycle for network entities is managed in an organization. It typically refers to the management of an organization's application users, where steps in the security life cycle include account creation, suspension, privilege modification, and account deletion. The network entities managed may also include devices, processes, applications, or anything else that needs to interact in a networked environment. Entities managed by an identity management

process may also include users outside of the organization, for example customers, trading partners, or Web services.

identity management infrastructure database

The database that contains data for OracleAS Single Sign-On and Oracle Internet Directory.

identity management realm

A collection of identities, all of which are governed by the same administrative policies. In an enterprise, all employees having access to the intranet may belong to one realm, while all external users who access the public applications of the enterprise may belong to another realm. An identity management realm is represented in the directory by a specific **entry** with a special **object class** associated with it.

identity management realm-specific Oracle Context

An Oracle Context contained in each identity management realm. It stores the following information:

- User naming policy of the identity management realm—that is, how users are named and located.
- Mandatory authentication attributes.
- Location of groups in the identity management realm.
- Privilege assignments for the identity management realm—for example: who has privileges to add more users to the realm.
- Application specific data for that realm including authorizations.

identity provider

One of the three primary roles defined in the **identity federation** protocols supported by Oracle Identity Federation. The other primary roles are **service provider** and **principal**. The identity provider is responsible for managing and authenticating a set of identities within a given **circle of trust**.

A service provider, in turn, provides services or goods to a principal based on the identity provider's authentication of a principal's identity.

Identity providers are service providers offering business incentives so that other service providers affiliate with them. An identity provider typically authenticates and asserts a principal's identity.

import agent

In an Oracle Directory Integration Platform environment, an agent that imports data into Oracle Internet Directory.

import data file

In an Oracle Directory Integration Platform environment, the file containing the data imported by an **import agent**.

infrastructure tier

The Oracle Application Server components responsible for identity management. These components are OracleAS Single Sign-On, Oracle Delegated Administration Services, and Oracle Internet Directory.

inherit

When an **object class** has been derived from another class, it also derives, or inherits, many of the characteristics of that other class. Similarly, an attribute subtype inherits the characteristics of its supertype.

instance

See **directory server instance**.

integrity

In cryptography, integrity is the ability to detect if data has been modified by entities that are not authorized to modify it.

Internet Directory

See **Oracle Internet Directory**.

Internet Engineering Task Force (IETF)

The principal body engaged in the development of new Internet standard specifications. It is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Internet Message Access Protocol (IMAP)

A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders, also called mailboxes, in a way that is functionally equivalent to local mailboxes.

J2EE

See **Java 2 Platform, Enterprise Edition (J2EE)**.

Java 2 Platform, Enterprise Edition (J2EE)

Java 2 Platform, Enterprise Edition (J2EE) is an environment for developing and deploying enterprise applications, defined by Sun Microsystems Inc. The J2EE platform consists of a set of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multitiered, Web-based applications.

Java Server Page (JSP)

JavaServer Pages (JSP), a server-side technology, are an extension to the Java servlet technology that was developed by Sun Microsystems. JSPs have dynamic scripting capability that works in tandem with HTML code, separating the page logic from the static elements (the design and display of the page). Embedded in the HTML page, the Java source code and its extensions help make the HTML more functional, being used in dynamic database queries, for example.

JSP

See **Java Server Page (JSP)**.

key

A key is a data structure that contains some secret knowledge necessary to successfully encrypt or decrypt a given block of data. The larger the key, the harder it is to crack a block of encrypted data. For example, a 256-bit key is more secure than a 128-bit key.

key pair

A **public key** and its associated **private key**.

See also: **public/private key pair**.

knowledge reference

The access information (name and address) for a remote **directory system agent (DSA)** and the name of the **directory information tree (DIT)** subtree that the remote DSA holds. Knowledge references are also called referrals.

latency

The time a client has to wait for a given directory operation to complete. Latency can be defined as wasted time. In networking discussions, latency is defined as the travel time of a packet from source to destination.

LDAP

See **Lightweight Directory Access Protocol (LDAP)**.

LDAP connection cache

To improve throughput, the OracleAS Single Sign-On server caches and then reuses connections to Oracle Internet Directory.

LDAP Data Interchange Format (LDIF)

A common, text-based format for exchanging directory data between systems. The set of standards for formatting an input file for any of the LDAP command-line utilities.

LDIF

See **LDAP Data Interchange Format (LDIF)**.

legacy application

Older application that cannot be modified to delegate authentication to the OracleAS Single Sign-On server. Also known as an **external application**.

Liberty Alliance

The Liberty Alliance Project is a consortium of companies, non-profits, and non-government organizations around the globe. It is committed to developing an open standard for **federated identity management (FIM)** and identity-based Web services supporting current and emerging network devices.

Liberty ID-FF

Liberty Identity Federation Framework (Liberty ID-FF) provides an architecture for Web-based **single sign-on (SSO)** with federated identities.

Lightweight Directory Access Protocol (LDAP)

A set of protocols for accessing information in directories. LDAP supports TCP/IP, which is necessary for any type of Internet access. Its framework of design conventions supports industry-standard directory products, such as Oracle Internet Directory. Because it is a simpler version of the **X.500** standard, LDAP is sometimes called X.500 light.

load balancer

Hardware devices and software that balance connection requests between two or more servers, either due to heavy load or failover. BigIP, Alteon, or Local Director are all

popular hardware devices. Oracle Application Server Web Cache is an example of load balancing software.

logical host

In an Oracle Application Server Cold Failover Cluster (Identity Management), one or more disk groups and pairs of host names and IP addresses. It is mapped to a physical host in the cluster. This physical host impersonates the host name and IP address of the logical host.

MAC

See **message authentication code (MAC)**.

man-in-the-middle

A security attack characterized by the third-party, surreptitious interception of a message. The third-party, the *man-in-the-middle*, decrypts the message, re-encrypts it (with or without alteration of the original message), and retransmits it to the originally-intended recipient—all without the knowledge of the legitimate sender and receiver. This type of security attack works only in the absence of **authentication**.

mapping rules file

In an Oracle Directory Integration Platform environment, the file that specifies mappings between Oracle Internet Directory attributes and those in a **connected directory**.

master definition site (MDS)

In replication, a master definition site is the Oracle Internet Directory database from which the administrator runs the configuration scripts.

master site

In replication, a master site is any site other than the **master definition site (MDS)** that participates in LDAP replication.

matching rule

In a search or compare operation, determines equality between the attribute value sought and the attribute value stored. For example, matching rules associated with the `telephoneNumber` attribute could cause "(650) 123-4567" to be matched with either "(650) 123-4567" or "6501234567" or both. When you create an **attribute**, you associate a matching rule with it.

MD2

Message Digest Two (MD2) is a message digest **hash function**. The algorithm processes input text and creates a 128-bit **message digest** which is unique to the message and can be used to verify data integrity. MD2 was developed by Ron Rivest for RSA Security and is intended to be used in systems with limited memory, such as smart cards.

MD4

Message Digest Four (MD4) is similar to **MD2** but designed specifically for fast processing in software.

MD5

Message Digest Five (MD5) is a message digest **hash function**. The algorithm processes input text and creates a 128-bit **message digest** which is unique to the message and can be used to verify data integrity. MD5 was developed by Ron Rivest

after potential weaknesses were reported in **MD4**. MD5 is similar to MD4 but slower because more manipulation is made to the original data.

MDS

See **master definition site (MDS)**.

message authentication

The process of verifying that a particular message came from a particular entity.

See also: **authentication**.

message authentication code (MAC)

The Message Authentication Code (MAC) is a result of a two-step process applied to a given block of data. First, the result of a **hash function** is obtained. Second, that result is encrypted using a **secret key**. The MAC can be used to authenticate the source of a given block of data.

message digest

The result of a **hash function**.

See also: **hash**.

metadirectory

A directory solution that shares information between all enterprise directories, integrating them into one virtual directory. It centralizes administration, thereby reducing administrative costs. It synchronizes data between directories, thereby ensuring that it is consistent and up-to-date across the enterprise.

middle tier

That portion of a OracleAS Single Sign-On instance that consists of the Oracle HTTP Server and OC4J. The OracleAS Single Sign-On middle tier is situated between the identity management infrastructure database and the client.

mod_osso

A module on the Oracle HTTP Server that enables applications protected by OracleAS Single Sign-On to accept HTTP headers in lieu of a user name and password once the user has logged into the OracleAS Single Sign-On server. The values for these headers are stored in the **mod_osso cookie**.

mod_osso cookie

User data stored on the HTTP server. The cookie is created when a user authenticates. When the same user requests another application, the Web server uses the information in the mod_osso cookie to log the user in to the application. This feature speeds server response time.

mod_proxy

A module on the Oracle HTTP Server that makes it possible to use **mod_osso** to enable single sign-on to legacy, or **external application**s.

MTS

See **shared server**.

multimaster replication

Also called peer-to-peer or *n*-way replication, a type of replication that enables multiple sites, acting as equals, to manage groups of replicated data. In a multimaster replication environment, each node is both a supplier and a consumer node, and the entire directory is replicated on each node.

name identifier profile

A **federation** profile which allows a provider to inform it's peers when assigning or updating a name identifier for one of their common users.

naming attribute

The attribute used to compose the RDN of a new user entry created through Oracle Delegated Administration Services or Oracle Internet Directory Java APIs. The default value for this is `cn`.

naming context

A subtree that resides entirely on one server. It must be contiguous, that is, it must begin at an entry that serves as the top of the subtree, and extend downward to either leaf entries or **knowledge reference**s (also called referrals) to subordinate naming contexts. It can range in size from a single entry to the entire **directory information tree (DIT)**.

native agent

In an Oracle Directory Integration Platform environment, an agent that runs under the control of the **Directory Integration Platform server**. It is in contrast to an **external agent**.

net service name

A simple name for a service that resolves to a connect descriptor. Users initiate a connect request by passing a user name and password along with a net service name in a connect string for the service to which they wish to connect, for example:

```
CONNECT username/password@net_service_name
```

Depending on your needs, net service names can be stored in a variety of places, including:

- Local configuration file, `tnsnames.ora`, on each client
- Directory server
- Oracle Names server
- External naming service, such as NDS, NIS or CDS

Net Services

See **Oracle Net Services**.

nickname attribute

The attribute used to uniquely identify a user in the entire directory. The default value for this is `uid`. Applications use this to resolve a simple user name to the complete distinguished name. The user nickname attribute cannot be multi-valued—that is, a given user cannot have multiple nicknames stored under the same attribute name.

non-repudiation

In cryptography, the ability to prove that a given **digital signature** was produced with a given entity's **private key**, and that a message was sent untampered at a given point in time.

OASIS

Organization for the Advancement of Structured Information Standards. OASIS is a worldwide not-for-profit consortium that drives the development, convergence and adoption of e-business standards.

object class

In LDAP, object classes are used to group information. Typically an object class models a real-world object such as a person or a server. Each directory entry belongs to one or more object classes. The object class determines the attributes that make up an entry. One object class can be derived from another, thereby inheriting some of the characteristics of the other class.

OC4J

See **Oracle Containers for J2EE (OC4J)**.

OCA

See **Oracle Certificate Authority**.

OCI

See **Oracle Call Interface (OCI)**.

OCSP

See **Online Certificate Status Protocol (OCSP)**.

OEM

See **Oracle Enterprise Manager**.

OID

See **Oracle Internet Directory**.

OID Control Utility

A command-line tool for issuing run-server and stop-server commands. The commands are interpreted and executed by the **OID Monitor** process.

OID Database Password Utility

The utility used to change the password with which Oracle Internet Directory connects to an Oracle Database.

OID Monitor

The Oracle Internet Directory component that initiates, monitors, and terminates the Oracle Internet Directory Server processes. It also controls the replication server if one is installed, and Oracle Directory Integration Platform Server.

Online Certificate Status Protocol (OCSP)

Online Certificate Status Protocol (OCSP) is one of two common schemes for checking the validity of digital certificates. The other, older method, which OCSP has superseded in some scenarios, is **certificate revocation list (CRL)**. OCSP is specified in **RFC** 2560.

one-way function

A function that is easy to compute in one direction but quite difficult to reverse compute, that is, to compute in the opposite direction.

one-way hash function

A **one-way function** that takes a variable sized input and creates a fixed size output.

See also: **hash function**.

Oracle Application Server Single Sign-On

OracleAS Single Sign-On consists of program logic that enables you to log in securely to applications such as expense reports, mail, and benefits. These applications take two forms: **partner application**s and **external application**s. In both cases, you gain access to several applications by authenticating only once.

Oracle Call Interface (OCI)

An application programming interface (API) that enables you to create applications that use the native procedures or function calls of a third-generation language to access an Oracle Database server and control all phases of SQL statement execution.

Oracle Certificate Authority

Oracle Application Server Certificate Authority is a **Certificate Authority (CA)** for use within your Oracle Application Server environment. OracleAS Certificate Authority uses Oracle Internet Directory as the storage repository for certificates. OracleAS Certificate Authority integration with OracleAS Single Sign-On and Oracle Internet Directory provides seamless certificate provisioning mechanisms for applications relying on them. A user provisioned in Oracle Internet Directory and authenticated in OracleAS Single Sign-On can choose to request a digital certificate from OracleAS Certificate Authority.

Oracle CMS

Oracle CMS implements the IETF **Cryptographic Message Syntax (CMS)** protocol. CMS defines data protection schemes that allow for secure message envelopes.

Oracle Containers for J2EE (OC4J)

A lightweight, scalable container for **Java 2 Platform, Enterprise Edition (J2EE)**.

Oracle Context

See **identity management realm-specific Oracle Context** and **root Oracle Context**.

Oracle Crypto

Oracle Crypto is a pure Java library that provides core cryptography algorithms.

Oracle Database Advanced Replication

A feature in the Oracle Database that enables database tables to be kept synchronized across two Oracle databases.

Oracle Delegated Administration Services

A set of individual, pre-defined services—called Oracle Delegated Administration Services units—for performing directory operations on behalf of a user. Oracle Internet Directory Self-Service Console makes it easier to develop and deploy administration solutions for both Oracle and third-party applications that use Oracle Internet Directory.

Oracle Directory Integration Platform

A collection of interfaces and services for integrating multiple directories by using Oracle Internet Directory and several associated plug-ins and connectors. A feature of Oracle Internet Directory that enables an enterprise to use an external user repository to authenticate to Oracle products.

Oracle Directory Integration Platform Server

In an Oracle Directory Integration Platform environment, a daemon process that monitors Oracle Internet Directory for change events and takes action based on the information present in the **directory integration profile**.

Oracle Directory Integration Platform

A component of **Oracle Internet Directory**. It is a framework developed to integrate applications around a central LDAP directory like Oracle Internet Directory.

Oracle Directory Manager

A Java-based tool with a graphical user interface for administering Oracle Internet Directory.

Oracle Enterprise Manager

A separate Oracle product that combines a graphical console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products.

Oracle HTTP Server

Software that processes Web transactions that use the Hypertext Transfer Protocol (HTTP). Oracle uses HTTP software developed by the Apache Group.

Oracle Identity Management

An infrastructure enabling deployments to manage centrally and securely all enterprise identities and their access to various applications in the enterprise.

Oracle Internet Directory

A general purpose directory service that enables retrieval of information about dispersed users and network resources. It combines **Lightweight Directory Access Protocol (LDAP)** Version 3 with the high performance, scalability, robustness, and availability of the Oracle Database.

Oracle Liberty SDK

Oracle Liberty SDK implements the **Liberty Alliance** Project specifications enabling federated single sign-on between third-party Liberty-compliant applications.

Oracle Net Services

The foundation of the Oracle family of networking products, allowing services and their client applications to reside on different computers and communicate. The main function of Oracle Net Services is to establish network sessions and transfer data between a client application and a server. Oracle Net Services is located on each computer in the network. Once a network session is established, Oracle Net Services acts as a data courier for the client and the server.

Oracle PKI certificate usages

Defines Oracle application types that a **certificate** supports.

Oracle PKI SDK

Oracle PKI SDK implements the security protocols that are necessary within **public key infrastructure (PKI)** implementations.

Oracle SAML

Oracle SAML provides a framework for the exchange of security credentials among disparate systems and applications in an XML-based format as outlined in the **OASIS** specification for the **Security Assertions Markup Language (SAML)**.

Oracle Security Engine

Oracle Security Engine extends Oracle Crypto by offering X.509 based certificate management functions. Oracle Security Engine is a superset of Oracle Crypto.

Oracle S/MIME

Oracle S/MIME implements the **Secure/Multipurpose Internet Mail Extension (S/MIME)** specifications from the **Internet Engineering Task Force (IETF)** for secure e-mail.

Oracle Wallet Manager

A Java-based application that security administrators use to manage public-key security credentials on clients and servers.

See also: *Oracle Advanced Security Administrator's Guide*.

Oracle Web Services Security

Oracle Web Services Security provides a framework for authentication and authorization using existing security technologies as outlined in the **OASIS** specification for Web Services Security.

Oracle XML Security

Oracle XML Security implements the W3C specifications for XML Encryption and XML Signature.

OracleAS Portal

An OracleAS Single Sign-On **partner application** that provides a mechanism for integrating files, images, applications, and Web sites. The External Applications portlet provides access to external applications.

other information repository

In an Oracle Directory Integration Platform environment, in which Oracle Internet Directory serves as the **central directory**, any information repository except Oracle Internet Directory.

OWM

See **Oracle Wallet Manager**.

partition

A unique, non-overlapping directory naming context that is stored on one directory server.

partner application

An Oracle Application Server application or non-Oracle application that delegates the authentication function to the OracleAS Single Sign-On server. This type of application spares users from reauthenticating by accepting **mod_osso** headers.

peer-to-peer replication

Also called multimaster replication or *n*-way replication. A type of replication that enables multiple sites, acting as equals, to manage groups of replicated data. In such a replication environment, each node is both a supplier and a consumer node, and the entire directory is replicated on each node.

PKCS#1

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS#1 provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes; ASN.1 syntax for representing keys and for identifying the schemes.

PKCS#5

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS#5 provides recommendations for the implementation of password-based cryptography.

PKCS#7

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #7 describes general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

PKCS#8

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #8 describes syntax for private key information, including a private key for some public key algorithms and a set of attributes. The standard also describes syntax for encrypted private keys.

PKCS#10

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #10 describes syntax for a request for certification of a public key, a name, and possibly a set of attributes.

PKCS#12

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #12 describes a transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions. Systems (such as browsers or operating systems) that support this standard allow a user to import, export, and exercise a single set of personal identity information—typically in a format called a **wallet**.

PKI

See **public key infrastructure (PKI)**.

plaintext

Plaintext is readable data prior to a transformation to ciphertext using encryption, or readable data that is the result of a transformation from ciphertext using decryption.

point-to-point replication

Also called fan-out replication is a type of replication in which a supplier replicates directly to a consumer. That consumer can then replicate to one or more other consumers. The replication can be either full or partial.

policy precedence

In Oracle Application Server Certificate Authority (OCA), policies are applied to incoming requests in the order that they are displayed on the main policy page. When the OCA policy processor module parses policies, those that appear toward the top of the policy list are applied to requests first. Those that appear toward the bottom of the list are applied last and take precedence over the others. Only enabled policies are applied to incoming requests.

policy.properties

A multipurpose configuration file for Oracle Application Server Single Sign-On that contains basic parameters required by the single sign-on server. Also used to configure advanced features of OracleAS Single Sign-On, such as multilevel authentication.

POSIX

Portable Operating System Interface for UNIX. A set of programming interface standards governing how to write application source code so that the applications are portable between operating systems. A series of standards being developed by the **Internet Engineering Task Force (IETF)**.

POST Profile

An **authentication** method whereby login credentials are submitted within the body of the login form.

predicates

In Oracle Application Server Certificate Authority (OCA), a policy predicate is a logical expression that can be applied to a policy to limit how it is applied to incoming certificate requests or revocations. For example, the following predicate expression specifies that the policy in which it appears can have a different effect for requests or revocations from clients with DNs that include "ou=sales,o=acme,c=us":

```
Type=="client" AND DN=="ou=sales,o=acme,c=us"
```

principal

One of the three primary roles defined in the **identity federation** protocols supported by Oracle Identity Federation. The other roles are **identity provider** and **service provider**.

A principal is any entity capable of using a service and capable of acquiring a federated identity. Typically, a principal is a person or user, or a system entity whose identity can be authenticated.

primary node

In an Oracle Application Server Cold Failover Cluster (Identity Management), the cluster node on which the application runs at any given time.

See also: **secondary node**.

private key

A private key is the secret key in a **public/private key pair** used in **public key cryptography**. An entity uses its private key to decrypt data that has been encrypted with its **public key**. The entity can also use its private key to create **digital signature**s. The security of data encrypted with the entity's public key as well as signatures created by the private key depends on the private key remaining secret.

private key cryptography

See **symmetric cryptography**.

profile

See **directory integration profile**.

Project Liberty

See **Liberty Alliance**.

provisioned applications

Applications in an environment where user and group information is centralized in Oracle Internet Directory. These applications are typically interested in changes to that information in Oracle Internet Directory.

provisioning

The process of providing users with access to applications and other resources that may be available in an enterprise environment.

provisioning agent

An application or process that translates Oracle-specific provisioning events to external or third-party application-specific events.

provisioning integration profile

A special kind of **directory integration profile** that describes the nature of provisioning-related notifications that Oracle Directory Integration Platform sends to the directory-enabled applications.

proxy server

A server between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server. In OracleAS Single Sign-On, proxies are used for load balancing and as an extra layer of security.

See also: **load balancer**.

proxy user

A kind of user typically employed in an environment with a middle tier such as a firewall. In such an environment, the end user authenticates to the middle tier. The middle tier then logs into the directory on the end user's behalf. A proxy user has the privilege to switch identities and, once it has logged into the directory, switches to the end user's identity. It then performs operations on the end user's behalf, using the authorization appropriate to that particular end user.

public key

A public key is the non-secret key in a **public/private key pair** used in **public key cryptography**. A public key allows entities to encrypt data that can only then be decrypted with the public key's owner using the corresponding **private key**. A public key can also be used to verify digital signatures created with the corresponding private key.

public key certificate

See **certificate**.

public key cryptography

Public key cryptography (also known as asymmetric cryptography) uses two keys, one public and the other private. These keys are called a key pair. The private key must be kept secret, while the public key can be transmitted to any party. The private key and the public key are mathematically related. A message that is signed by a private key can be verified by the corresponding public key. Similarly, a message encrypted by the public key can be decrypted by the private key. This method ensures privacy because only the owner of the private key can decrypt the message.

public key encryption

The process in which the sender of a message encrypts the message with the public key of the recipient. Upon delivery, the message is decrypted by the recipient using the recipient's private key.

public key infrastructure (PKI)

A public key infrastructure (PKI) is a system that manages the issuing, distribution, and authentication of **public key**s and **private key**s. A PKI typically comprises the following components:

- A **Certificate Authority (CA)** that is responsible for generating, issuing, publishing and revoking digital certificates.
- A **Registration Authority (RA)** that is responsible for verifying the information supplied in requests for certificates made to the CA.
- A directory service where a **certificate** or **certificate revocation list (CRL)** gets published by the CA and where they can be retrieved by relying third parties.
- Relying third parties that use the certificates issued by the CA and the **public key**s contained therein to verify **digital signature**s and encrypt data.

public/private key pair

A mathematically related set of two numbers where one is called the private key and the other is called the public key. Public keys are typically made widely available, while private keys are available only to their owners. Data encrypted with a public key can only be decrypted with its associated private key and vice versa. Data encrypted with a public key cannot be decrypted with the same public key.

RC2

Rivest Cipher Two (RC2) is a 64-bit **block cipher** developed by Ronald Rivest for RSA Security, and was designed as a replacement for **Data Encryption Standard (DES)**.

RC4

Rivest Cipher Four (RC4) is a **stream cipher** developed by Ronald Rivest for RSA Security. RC4 allows variable key lengths up to 1024 bits. RC4 is most commonly used to secure data communications by encrypting traffic between Web sites that use the **Secure Sockets Layer (SSL)** protocol.

RDN

See **relative distinguished name (RDN)**.

readable data

Data prior to a transformation to ciphertext via encryption or data that is the result of a transformation from ciphertext via decryption.

realm

See **identity management realm**.

realm search base

An attribute in the **root Oracle Context** that identifies the entry in the **directory information tree (DIT)** that contains all **identity management realm**s. This attribute is used when mapping a simple realm name to the corresponding entry in the directory.

referral

Information that a directory server provides to a client and which points to other servers the client must contact to find the information it is requesting.

See also: **knowledge reference**.

Registration Authority (RA)

The Registration Authority (RA) is responsible for verifying and enrolling users before a certificate is issued by a **Certificate Authority (CA)**. The RA may assign each applicant a relative distinguished value or name for the new certificate applied. The RA does not sign or issue certificates.

registry entry

An entry containing runtime information associated with invocations of Oracle Internet Directory servers, called a **directory server instance**. Registry entries are stored in the directory itself, and remain there until the corresponding directory server instance stops.

relational database

A structured collection of data that stores data in tables consisting of one or more rows, each containing the same set of columns. Oracle makes it very easy to link the data in multiple tables. This is what makes Oracle a relational database management system, or RDBMS. It stores data in two or more tables and enables you to define relationships between the tables. The link is based on one or more fields common to both tables.

relative distinguished name (RDN)

The local, most granular level entry name. It has no other qualifying entry names that would serve to uniquely address the entry. In the example, `cn=Smith,o=acme,c=US`, the RDN is `cn=Smith`.

remote master site (RMS)

In a replicated environment, any site, other than the **master definition site (MDS)**, that participates in **Oracle Database Advanced Replication**.

replica

Each copy of a **naming context** that is contained within a single server.

replication agreement

A special directory entry that represents the replication relationship among the directory servers in a **directory replication group (DRG)**.

response time

The time between the submission of a request and the completion of the response.

RFC

The Internet Request For Comments (or RFC) documents are the written definitions of the protocols and policies of the Internet. The Internet Engineering Task Force (IETF) facilitates the discussion, development, and establishment of new standards. A standard is published using the RFC acronym and a reference number. For example, the official standard for e-mail is RFC 822.

root CA

In a hierarchical **public key infrastructure (PKI)**, the root **Certificate Authority (CA)** is the CA whose **public key** serves as the most trusted datum for a security domain.

root directory specific entry (DSE)

An entry storing operational information about the directory. The information is stored in a number of attributes.

root DSE

See **root directory specific entry (DSE)**.

root Oracle Context

In the Oracle Identity Management infrastructure, the root Oracle Context is an entry in Oracle Internet Directory containing a pointer to the default identity management realm in the infrastructure. It also contains information on how to locate an identity management realm given a simple name of the realm.

RSA

RSA is a **public key cryptography** algorithm named after its inventors (Rivest, Shamir, and Adelman). The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Netscape and Microsoft, and many other products.

RSAES-OAEP

The RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) is a public key encryption scheme combining the **RSA** algorithm with the OAEP method. Optimal Asymmetric Encryption Padding (OAEP) is a method for encoding messages developed by Mihir Bellare and Phil Rogaway.

S/MIME

See **Secure/Multipurpose Internet Mail Extension (S/MIME)**.

SAML

See **Security Assertions Markup Language (SAML)**.

SASL

See **Simple Authentication and Security Layer (SASL)**.

scalability

The ability of a system to provide throughput in proportion to, and limited only by, available hardware resources.

schema

The collection of **attribute**s, **object class**es, and their corresponding **matching rule**s.

secondary node

In an Oracle Application Server Cold Failover Cluster (Identity Management), the cluster node to which an application is moved during a failover.

See also: **primary node**.

secret key

A secret key is the **key** used in a **symmetric algorithm**. Since a secret key is used for both encryption and decryption, it must be shared between parties that are transmitting ciphertext to one another but must be kept secret from all unauthorized entities.

secret key cryptography

See **symmetric cryptography**.

Secure Hash Algorithm (SHA)

Secure Hash Algorithm (SHA) is a **hash function** algorithm that produces a 160-bit **message digest** based upon the input. The algorithm is used in the Digital Signature Standard (DSS). With the introduction of the Advanced Encryption Standard (AES) which offers three key sizes: 128, 192 and 256 bits, there has been a need for a companion hash algorithm with a similar level of security. The newer SHA-256, SHA-284 and SHA-512 hash algorithms comply with these enhanced requirements.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a protocol designed by Netscape Communications to enable encrypted, authenticated communications across networks (such as the Internet). SSL uses the **public key encryption** system from RSA, which also includes the use of a digital certificate. SSL provides three elements of secure communications: **confidentiality**, **authentication**, and **integrity**.

SSL has evolved into **Transport Layer Security (TLS)**. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL.

Secure/Multipurpose Internet Mail Extension (S/MIME)

Secure/Multipurpose Internet Mail Extension (S/MIME) is an Internet Engineering Task Force (IETF) standard for securing MIME data through the use of **digital signature**s and **encryption**.

Security Assertions Markup Language (SAML)

An **XML**-based framework which defines mechanisms for exchanging security information about a subject by making assertions about the subject that are used to make access control decisions. SAML enables the exchange of **authentication** and **authorization** information between identity providers and service providers who otherwise may not be able to interoperate.

SAML 2.0 is a major revision of the standard which updates SAML 1.1 and combines input from both Shibboleth and **Liberty ID-FF** specifications. A key aspect of SAML 2.0 is the ability for two sites to establish and maintain an identifier for a user, with that user's cooperation. Additional features include privacy mechanisms and support for **global logout**.

security token

In the Liberty protocol, refers to a set of security information that represents and substantiates a claim.

server certificate

A **certificate** that attests to the identity of an organization that uses a secure Web server to serve data. A server certificate must be associated with a **public/private key pair** issued by a mutually trusted **Certificate Authority (CA)**. Server certificates are required for secure communications between a browser and a Web server.

service provider

One of the three primary roles defined in the **identity federation** protocols supported by Oracle Identity Federation. The other roles are **identity provider** and **principal**.

A service provider, which is the relying party in SAML, provides services or goods to a principal while relying on an identity provider to authenticate the principal's identity.

service time

The time between the initiation of a request and the completion of the response to the request.

session key

A **secret key** that is used for the duration of one message or communication session.

SGA

See **System Global Area (SGA)**.

SHA

See **Secure Hash Algorithm (SHA)**.

shared server

A server that is configured to allow many user processes to share very few server processes, so the number of users that can be supported is increased. With shared server configuration, many user processes connect to a dispatcher. The dispatcher directs multiple incoming network session requests to a common queue. An idle shared server process from a shared pool of server processes picks up a request from the queue. This means a small pool of server processes can server a large amount of clients. Contrast with dedicated server.

sibling

An entry that has the same parent as one or more other entries.

Signed Public Key And Challenge (SPKAC)

Signed Public Key And Challenge (SPKAC) is a proprietary protocol used by the Netscape Navigator browser to request certificates.

simple authentication

The process by which the client identifies itself to the server by means of a DN and a password which are not encrypted when sent over the network. In the simple authentication option, the server verifies that the DN and password sent by the client match the DN and password stored in the directory.

Simple Authentication and Security Layer (SASL)

Simple Authentication and Security Layer (SASL) is a method for adding **authentication** and **authorization** capabilities to application protocols. SASL provides a security layer between the protocol and the connection, so that users can be authenticated to a server. A security layer can also be negotiated to protect subsequent protocol interactions.

Simple Object Access Protocol (SOAP)

Simple Object Access Protocol (SOAP) is an **XML**-based protocol that defines a framework for exchanging messages between systems over the Internet. A common protocol for Web Services, SOAP is used with transport protocols such as HTTP and FTP. A SOAP message consists of three parts — an envelope that describes the message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.

single key-pair wallet

A **PKCS#12**-format wallet that contains a single user **certificate** and its associated **private key**. The **public key** is imbedded in the certificate.

single sign-off

The process by which you terminate an OracleAS Single Sign-On session and log out of all active partner applications simultaneously. You can do this by logging out of the application that you are working in.

single sign-on (SSO)

In a federated environment, single sign-on enables users to sign on once with a member of a federated group of identity providers and service providers, and later use resources available from members witout needing to sign on again.

single sign-on SDK

Legacy APIs to enable OracleAS Single Sign-On partner applications for single sign-on. The SDK consists of PL/SQL and Java APIs as well as sample code that demonstrates how these APIs are implemented. This SDK is now deprecated and **mod_osso** is used instead.

single sign-on server

Program logic that enables users to log in securely to single sign-on applications such as expense reports, mail, and benefits.

SLAPD

Standalone LDAP daemon. An LDAP directory server service that is responsible for most functions of a directory except replication.

slave

See **consumer**.

smart knowledge reference

A **knowledge reference** that is returned when the knowledge reference entry is in the scope of the search. It points the user to the server that stores the requested information.

SOAP

See **Simple Object Access Protocol (SOAP)**.

specific administrative area

Administrative areas control:

- Subschema administration
- Access control administration

- Collective attribute administration

A *specific* administrative area controls one of these aspects of administration. A specific administrative area is part of an autonomous administrative area.

SPKAC

See **Signed Public Key And Challenge (SPKAC)**.

sponsor node

In replication, the node that is used to provide initial data to a new node.

SSL

See **Secure Sockets Layer (SSL)**.

SSO

See **single sign-on (SSO)**.

stream cipher

Stream ciphers are a type of **symmetric algorithm**. A stream cipher encrypts in small units, often a bit or a byte at a time, and implements some form of feedback mechanism so that the key is constantly changing. **RC4** is an example of a stream cipher.

See also: **block cipher**.

subACLSubentry

A specific type of **subentry** that contains **access control list (ACL)** information.

subclass

An object class derived from another object class. The object class from which it is derived is called its **superclass**.

subentry

A type of entry containing information applicable to a group of entries in a subtree. The information can be of these types:

- Access control policy points
- Schema rules
- Collective attributes

Subentries are located immediately below the root of an administrative area.

subordinate CA

In a hierarchical **public key infrastructure (PKI)**, the subordinate **Certificate Authority (CA)** is a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.

subordinate reference

A **knowledge reference** pointing downward in the **directory information tree (DIT)** to a **naming context** that starts immediately below an entry

subschema DN

The list of **directory information tree (DIT)** areas having independent **schema** definitions.

subSchemaSubentry

A specific type of **subentry** containing **schema** information.

subtree

A section of a directory hierarchy, which is also called a **directory information tree (DIT)**. The subtree typically starts at a particular directory node and includes all subdirectories and objects below that node in the directory hierarchy.

subtype

An attribute with one or more options, in contrast to that same attribute without the options. For example, a `commonName` (`cn`) attribute with American English as an option is a subtype of the `commonName` (`cn`) attribute without that option. Conversely, the `commonName` (`cn`) attribute without an option is the **supertype** of the same attribute with an option.

success URL

When using Oracle Application Server Single Sign-On, the URL to the routine responsible for establishing the session and session cookies for an application.

super user

A special directory administrator who typically has full access to directory information.

superclass

The **object class** from which another object class is derived. For example, the object class `person` is the superclass of the object class `organizationalPerson`. The latter, namely, `organizationalPerson`, is a **subclass** of `person` and inherits the attributes contained in `person`.

superior reference

A **knowledge reference** pointing upward to a **directory system agent (DSA)** that holds a naming context higher in the **directory information tree (DIT)** than all the naming contexts held by the referencing DSA.

supertype

An attribute without options, in contrast to the same attribute with one or more options. For example, the `commonName` (`cn`) attribute without an option is the supertype of the same attribute with an option. Conversely, a `commonName` (`cn`) attribute with American English as an option is a **subtype** of the `commonName` (`cn`) attribute without that option.

supplier

In replication, the server that holds the master copy of the **naming context**. It supplies updates from the master copy to the **consumer** server.

symmetric algorithm

A symmetric algorithm is a cryptographic algorithm that uses the same key for encryption and decryption. There are essentially two types of symmetric (or secret key) algorithms — **stream cipher**s and **block cipher**s.

symmetric cryptography

Symmetric cryptography (or shared secret cryptography) systems use the same key to encipher and decipher data. The problem with symmetric cryptography is ensuring a

secure method by which the sender and recipient can agree on the secret key. If a third party were to intercept the secret key in transit, they could then use it to decipher anything it was used to encipher. Symmetric cryptography is usually faster than asymmetric cryptography, and is often used when large quantities of data need to be exchanged. **DES**, **RC2**, and **RC4** are examples of symmetric cryptography algorithms.

symmetric key

See **secret key**.

System Global Area (SGA)

A group of shared memory structures that contain data and control information for one Oracle database instance. If multiple users are concurrently connected to the same instance, the data in the instance SGA is shared among the users. Consequently, the SGA is sometimes referred to as the "shared global area." The combination of the background processes and memory buffers is called an Oracle instance.

system operational attribute

An attribute holding information that pertains to the operation of the directory itself. Some operational information is specified by the directory to control the server, for example, the time stamp for an entry. Other operational information, such as access information, is defined by administrators and is used by the directory program in its processing.

think time

The time the user is not engaged in actual use of the processor.

third-party access management system

Non-Oracle single sign-on system that can be modified to use OracleAS Single Sign-On to gain access to Oracle Application Server applications.

throughput

The number of requests processed byOracle Internet Directory for each unit of time. This is typically represented as "operations per second."

Time Stamp Protocol (TSP)

Time Stamp Protocol (TSP), as specified in RFC 3161, defines the participating entities, the message formats, and the transport protocol involved in time stamping a digital message. In a TSP system, a trusted third-party Time Stamp Authority (TSA) issues time stamps for messages.

TLS

See **Transport Layer Security (TLS)**.

Transport Layer Security (TLS)

A protocol providing communications privacy over the Internet. The protocol enables client/server applications to communicate in a way that prevents eavesdropping, tampering, or message forgery.

Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) is based on the **Data Encryption Standard (DES)** algorithm developed by IBM in 1974, and was adopted as a national standard in 1977. 3DES uses three 64-bit long keys (overall key length is 192 bits, although actual key length is 56 bits). Data is encrypted with the first key, decrypted with the second

key, and finally encrypted again with the third key. This makes 3DES three times slower than standard DES but also three times more secure.

trusted certificate

A third party identity that is qualified with a level of trust. The trust is used when an identity is being validated as the entity it claims to be. Typically, trusted certificates come from a **Certificate Authority (CA)** you trust to issue user certificates.

trustpoint

See **trusted certificate**.

TSP

See **Time Stamp Protocol (TSP)**.

Unicode

A type of universal character set, a collection of 64K characters encoded in a 16-bit space. It encodes nearly every character in just about every existing character set standard, covering most written scripts used in the world. It is owned and defined by Unicode Inc. Unicode is canonical encoding which means its value can be passed around in different locales. But it does not guarantee a round-trip conversion between it and every Oracle character set without information loss.

UNIX Crypt

The UNIX encryption algorithm.

URI

Uniform Resource Identifier (URI). A way to identify any point of content on the Web, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the Web page address, which is a particular form or subset of URI called a **URL**.

URL

Uniform Resource Locator (URL). The address of a file accessible on the Internet. The file can be a text file, HTML page, image file, a program, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of the file location on the computer.

URLC token

The OracleAS Single Sign-On code that passes authenticated user information to the **partner application**. The partner application uses this information to construct the session cookie.

user name mapping module

A OracleAS Single Sign-On Java module that maps a user **certificate** to the user's nickname. The nickname is then passed to an authentication module, which uses this nickname to retrieve the user's certificate from the directory.

user search base

In the Oracle Internet Directory default **directory information tree (DIT)**, the node in the identity management realm under which all the users are placed.

UTC (Coordinated Universal Time)

The standard time common to every place in the world. Formerly and still widely called Greenwich Mean Time (GMT) and also World Time, UTC nominally reflects the mean solar time along the Earth's prime meridian. UTC is indicated by a z at the end of the value, for example, 200011281010z.

UTF-8

A variable-width 8-bit encoding of **Unicode** that uses sequences of 1, 2, 3, or 4 bytes for each character. Characters from 0-127 (the 7-bit ASCII characters) are encoded with one byte, characters from 128-2047 require two bytes, characters from 2048-65535 require three bytes, and characters beyond 65535 require four bytes. The Oracle character set name for this is AL32UTF8 (for the Unicode 3.1 standard).

UTF-16

16-bit encoding of **Unicode**.The Latin-1 characters are the first 256 code points in this standard.

verification

Verification is the process of ensuring that a given **digital signature** is valid, given the **public key** that corresponds to the **private key** purported to create the signature and the data block to which the signature purportedly applies.

virtual host

A single physical Web server machine that is hosting one or more Web sites or domains, or a server that is acting as a proxy to other machines (accepts incoming requests and reroutes them to the appropriate server).

In the case of OracleAS Single Sign-On, virtual hosts are used for load balancing between two or more OracleAS Single Sign-On servers. They also provide an extra layer of security.

virtual host name

In an Oracle Application Server Cold Failover Cluster (Identity Management), the host name corresponding to a particular virtual IP address.

virtual IP address

In an Oracle Application Server Cold Failover Cluster (Identity Management), each physical node has its own physical IP address and physical host name. To present a single system image to the outside world, the cluster uses a dynamic IP address that can be moved to any physical node in the cluster. This is called the virtual IP address.

wait time

The time between the submission of the request and initiation of the response.

wallet

An abstraction used to store and manage security credentials for an individual entity. It implements the storage and retrieval of credentials for use with various cryptographic services. A wallet resource locator (WRL) provides all the necessary information to locate the wallet.

Wallet Manager

See **Oracle Wallet Manager**.

Web service

A Web service is application or business logic that is accessible using standard Internet protocols, such as **HTTP**, **XML**, and **SOAP**. Web Services combine the best aspects of component-based development and the World Wide Web. Like components, Web Services represent black-box functionality that can be used and reused without regard to how the service is implemented.

Web Services Description Language (WSDL)

Web Services Description Language (WSDL) is the standard format for describing a Web service using **XML**. A WSDL definition describes how to access a Web service and what operations it will perform.

WSDL

See **Web Services Description Language (WSDL)**.

WS-Federation

Web Services Federation Language (WS-Federation) is a specification developed by Microsoft, IBM, BEA, VeriSign, and RSA Security. It defines mechanisms to allow **federation** between entities using different or like mechanisms by allowing and brokering trust of identities, attributes, and authentication between participating **Web service**s.

See also: **Liberty Alliance**.

X.500

X.500 is a standard from the International Telecommunication Union (ITU) that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city.

X.509

X.509 is the most widely used standard for defining digital certificates. A standard from the International Telecommunication Union (ITU), for hierarchical directories with authentication services, used in many **public key infrastructure (PKI)** implementations.

XML

Extensible Markup Language (XML) is a specification developed by the World Wide Web Consortium (W3C). XML is a pared-down version of Standard Generalized Mark-Up Language (SGML), designed especially for Web documents. XML is a metalanguage (a way to define tag sets) that allows developers to define their own customized markup language for many classes of documents.

XML canonicalization (C14N)

This is a process by which two logically equivalent XML documents can be resolved to the same physical representation. This has significance for digital signatures because a signature can only verify against the same physical representation of the data against which it was originally computed. For more information, see the W3C's XML Canonicalization specification.

Index

Numerics

A

B

C

D

E

G

H

I

L

M

N

O

P

R

S

T

U

W